Citrix Virtual Apps and Desktops 7 2402 LTSR

Contents

Citrix Virtual Apps and Desktops 7 2402 Long Term Service Release (LTSR)

June 27, 2024

> **Important :**
>
> La stratégie de cycle de vie du produit des versions Current Releases (CR) et Long Term Service Releases (LTSR) est décrite dans Étapes du cycle de vie.

Citrix Virtual Apps and Desktops fournit une solution de virtualisation pour la mise à disposition d'applications et de bureaux sur n'importe quel périphérique, sur n'importe quel réseau, tout en améliorant la sécurité des données, en réduisant les coûts et en renforçant la productivité.

Le programme LTSR (Long Term Service Release, version de service à long terme) pour Citrix Virtual Apps and Desktops offre une stabilité et une assistance à long terme pour les versions de Citrix Virtual Apps and Desktops.

La mise à jour cumulative 4 (CU4) est la dernière mise à jour vers la version 2203 LTSR. Les LTSR sont également disponibles pour Citrix Virtual Apps and Desktops 1912.

- Pour plus d'informations sur les cas d'utilisation, voir https://www.citrix.com/products/citrix-virtual-apps-and-desktops/.
- Pour en savoir plus sur les composants et les technologies disponibles dans les déploiements Citrix Virtual Apps and Desktops, reportez-vous à la section Vue d'ensemble technique.

Versions précédentes

La documentation des autres versions actuellement disponibles se trouve dans Citrix Virtual Apps and Desktops.

Pour les versions antérieures, la documentation est archivée dans l'ancienne documentation.

Citrix Virtual Apps and Desktops dans Citrix Cloud

L'offre Citrix Cloud Virtual Apps and Desktops est Citrix DaaS. Pour de plus amples informations, consultez Citrix DaaS.

Liens utiles

- Citrix Supportability Pack

- FAQ sur LTSR
- Options de maintenance Citrix Virtual Apps and Desktops
- Dates de cycle de vie des produits
- Programme LTSR pour l'application Citrix Workspace

Citrix Virtual Apps and Desktops 7 2402 LTSR

June 28, 2024

À propos de la version

Le programme LTSR (Long Term Service Release, version de service à long terme) pour Citrix Virtual Apps and Desktops offre une stabilité et une assistance à long terme pour les versions de Citrix Virtual Apps and Desktops.

Les LTSR sont également disponibles pour Citrix Virtual Apps and Desktops 2203 et 1912.

Cette version de Citrix Virtual Apps and Desktops comprend les nouvelles versions des VDA Windows et les nouvelles versions de plusieurs composants principaux. Vous pouvez :

- **Installer ou mettre à niveau un site** : utilisez le fichier ISO de cette version pour installer ou mettre à niveau les composants principaux et les VDA. L'installation ou la mise à niveau vers la version la plus récente vous permet d'utiliser les fonctionnalités les plus récentes.
- **Installer ou mettre à niveau des VDA dans un site existant :** si vous disposez déjà d'un déploiement, et que vous n'êtes pas prêt à mettre à niveau les composants principaux, vous pouvez toujours utiliser plusieurs des dernières fonctionnalités HDX en installant (ou en effectuant une mise à niveau vers) un nouveau VDA. Mettre à niveau les VDA uniquement peut être utile lorsque vous voulez tester les améliorations dans un environnement de non production.

  Après la mise à niveau de vos VDA vers cette version, vous n'avez pas besoin de mettre à jour le niveau fonctionnel du catalogue de machines. Pour de plus amples informations, consultez la section Versions VDA et niveaux fonctionnels.

Pour obtenir des instructions d'installation et de mise à niveau :

- Si vous créez un nouveau site, suivez la séquence sous Installer et configurer.
- Si vous mettez un site à niveau, consultez la section Mettre un déploiement à niveau.

Citrix Virtual Apps and Desktops 7 2402 LTSR

Secure HDX (Technical Preview)

Vous pouvez désormais utiliser Secure HDX, qui est une solution de cryptage au niveau de l'application (ALE) qui empêche tout élément de réseau sur le chemin du trafic de pouvoir inspecter le trafic HDX. Pour plus d'informations, consultez Secure HDX.

Nouvelle stratégie HDX Graphics - Autoriser le verrouillage de l'écran de Windows

Avec la nouvelle stratégie **Autoriser le verrouillage de l'écran de Windows** dans HDX Graphics, vous avez désormais la possibilité de modifier les délais d'affichage de Windows dans une session Citrix Virtual Desktop sur le système d'exploitation du poste de travail selon vos besoins.
Pour plus d'informations, consultez la section Autoriser le verrouillage de l'écran de Windows.

Nouvelle stratégie Mode tolérance de pertes pour l'audio

Le mode tolérance de pertes pour l'audio est désormais disponible pour permettre la diffusion audio via la stratégie de mode tolérance de pertes.
Pour plus d'informations, consultez la section Mode de tolérance de pertes pour l'audio.

Fichiers binaires tiers signés

Les fichiers binaires distribués par Citrix sont désormais signés. Les fichiers binaires signés indiquent qu'ils sont validés soit par des certificats générés par Citrix, soit par des certificats tiers authentiques.
Pour plus d'informations, consultez la section Installer des VDA.

Journaux système améliorés pour la redirection de contenu du navigateur

Grâce aux améliorations apportées aux journaux système, la redirection de contenu du navigateur permet désormais aux administrateurs de surveiller l'état des fonctionnalités. Pour plus d'informations, consultez l'article How to troubleshoot browser content redirection.

Amélioration de la configuration de redirection de contenu bidirectionnelle

Auparavant, la configuration de la redirection de contenu bidirectionnelle impliquait la gestion de trois stratégies distinctes : Autoriser la redirection bidirectionnelle du contenu, Autoriser la redirection des URL vers le VDA et Autoriser la redirection des URL vers le client. Ces stratégies nécessitent

des configurations à la fois côté serveur et côté client (configurées via des stratégies de groupe). À partir de cette version, nous avons regroupé les trois stratégies en une seule stratégie unifiée. Cela non seulement simplifie et améliore le processus de configuration, mais élimine également la nécessité de configurations côté client.
Pour plus d'informations, reportez-vous à la section Configuration de la redirection bidirectionnelle du contenu.

Réducteur HDX

Vous pouvez configurer la version de l'algorithme de compression HDX, ou Reducer, que vous souhaitez utiliser dans l'hôte de session.
Pour plus d'informations, consultez la section HDX Reducer.

Nouveau paramètre de registre HDX pour configurer le délai d'expiration EDT

Vous pouvez désormais configurer le délai d'expiration EDT en configurant le registre. Pour plus d'informations, consultez la section Configurer le délai d'expiration EDT.

Optimisation Microsoft Teams - Entrée de registre sur liste verte

À partir de Citrix Virtual Apps and Desktops 2402, vous n'avez plus besoin de configurer manuellement l'entrée de registre `msedgewebview2.exe`, car elle est désormais mise sur liste verte par défaut.

Pour de plus amples informations, consultez la documentation de Microsoft.

Prise en charge de la liste verte de canaux virtuels pour les variables d'environnement

Vous pouvez désormais utiliser des variables d'environnement système dans le chemin des processus sécurisés. Pour plus d'informations, consultez Utilisation de variables d'environnement système.

Citrix Secure Private Access pour les applications locales

Secure Private Access pour applications locales, prise en charge de ZTNA et autres améliorations

La solution Citrix Secure Private Access locale améliore la posture globale de sécurité et de conformité d'une organisation en permettant de fournir facilement un accès réseau Zero Trust aux applications basées sur un navigateur (applications Web internes et applications SaaS) en utilisant une instance

locale de StoreFront comme portail d'accès unifié aux applications Web et SaaS, ainsi qu'aux applications et bureaux virtuels intégrés à Citrix Workspace. La solution Citrix Secure Private Access locale est une solution ZTNA (Zero Trust Network Access) gérée par le client qui fournit un accès sans VPN aux applications Web et SaaS internes avec les éléments suivants, ainsi qu'une expérience utilisateur fluide pour l'utilisateur final :

- Principe du moindre privilège
- Authentification unique (SSO)
- Authentification multifacteur
- Évaluation de la posture de périphérique
- Contrôles de sécurité au niveau des applications
- Fonctionnalités App Protection

Pour plus d'informations, consultez Citrix Secure Private Access pour les applications locales - Disponibilité générale.

Virtual Delivery Agents (VDA) 2402 LTSR

Possibilité d'installer, de mettre à niveau ou de désinstaller l'application Citrix Workspace pendant l'installation, la mise à niveau ou la désinstallation du VDA

Cette fonctionnalité vous permet de choisir d'installer, de mettre à niveau ou de désinstaller l'application Citrix Workspace lors de l'installation, de la mise à niveau ou de la désinstallation d'un VDA dans les scénarios suivants :

- Lors de l'installation d'un VDA, vous pouvez choisir d'installer l'application Citrix Workspace. Par défaut, l'application Citrix Workspace n'est pas installée lors de l'installation du VDA.
- Lors d'une mise à niveau du VDA, si l'application Citrix Workspace n'est pas déjà installée dans le VDA, vous pouvez choisir d'installer l'application Citrix Workspace.
- Lors d'une mise à niveau du VDA, si la version de l'application Citrix Workspace peut être mise à niveau, l'option de mise à niveau de l'application Citrix Workspace s'affiche.
- Lors de la désinstallation d'un VDA, vous pouvez choisir de ne pas désinstaller l'application Citrix Workspace. Par défaut, l'application Citrix Workspace est désinstallée lors de la désinstallation du VDA. Pour plus d'informations, consultez les sections Sélection les composants à installer et l'emplacement d'installation et Options de ligne de commande pour l'installation d'un VDA.

Prise en charge de WebSocket pour les VDA

Citrix Virtual Apps and Desktops vous permet désormais d'utiliser la technologie WebSocket via Citrix Brokering Protocol (CBP) pour faciliter la communication entre les VDA et les Delivery Controller. Cette

fonctionnalité requiert uniquement le port TLS 443 pour la communication entre le VDA et le Delivery Controller.

Pour plus d'informations, consultez la section Communication WebSocket entre VDA et Delivery Controller.

Prise en charge des mises à jour des VDA à partir d'un partage de fichiers local auquel les VDA ont accès (Technical Preview)

Vous pouvez désormais prendre en charge les mises à jour du VDA à partir d'un partage de fichiers local et spécifier l'emplacement du programme d'installation du VDA via les commandes PowerShell. Pour plus d'informations, consultez la section Prise en charge des mises à jour du VDA via un partage de fichiers local.

Studio Web

Prise en charge du provisioning des machines virtuelles VMware à l'aide de profils de machine

Lorsque vous provisionnez des machines virtuelles VMware à l'aide de Machine Creation Services (MCS), vous pouvez désormais sélectionner un modèle existant comme profil de machine, afin que les machines virtuelles du catalogue héritent des paramètres du modèle sélectionné.

Les paramètres hérités incluent :

- Balises placées sur le modèle
- Attributs personnalisés
- Stratégies de stockage vSAN
- Version du matériel virtuel
- vSphere Virtual TPM (vTPM)
- Nombre d'UC et de cœurs par socket
- Nombre de cartes d'interface réseau

Pour plus d'informations, consultez l'article Créer des catalogues de machines.

Gestion des images préparées à l'aide du nœud Images

Le nœud **Images** est désormais disponible dans Web Studio. Il vous permet de préparer une image MCS (image préparée) à partir d'une seule image source et de la déployer sur différents catalogues de machines MCS. Ce nœud facilite la gestion complète du cycle de vie des images, en vous permettant de créer des définitions, des versions et des catalogues d'images.

Les images préparées à l'aide de ce nœud ne peuvent être utilisées que dans les environnements Azure et VMware. Pour des informations détaillées sur la gestion des images, consultez la section Gestion des images (Technical Preview).

Vous pouvez également créer des catalogues contenant des images préparées à l'aide du nœud **Catalogues de machines**. Pour plus d'informations, consultez l'article Créer des catalogues de machines.

Stratégies liées

Nouvelles validations de stratégies. Des validations de stratégie supplémentaires sont ajoutées. Par conséquent, l'activation de stratégies ou la mise à niveau sur place peuvent entraîner la perte de données de stratégie si des paramètres de stratégie non valides sont présents. Si vous créez ou modifiez les stratégies à l'aide d'une méthode autre que Web Studio, Citrix vous recommande d'utiliser la dernière version du SDK et du composant logiciel enfichable. Pour plus d'informations, veuillez consulter l'article CTX676686.

Fonctionnalités obsolètes

Les fonctionnalités et paramètres suivants sont désormais obsolètes dans Web Studio :

- Environnements Azure :

  Le provisioning de machines virtuelles à l'aide d'une image principale provenant d'une autre région est obsolète. Nous vous recommandons d'utiliser Azure Compute Gallery pour répliquer l'image principale dans la région où les machines virtuelles seront créées.

- Environnements AWS :

  L'option **Appliquer les propriétés du modèle de machine aux machines virtuelles** sur la page **Configuration d'un catalogue de machines > Modèle de machine** est obsolète. Nous vous recommandons plutôt d'utiliser des profils de machine pour spécifier les propriétés des machines virtuelles.

- Tous les environnements d'hyperviseurs et de services de cloud :

  La configuration du cache en écriture différée avec uniquement un cache disque et aucun cache mémoire est obsolète. Nous vous recommandons de définir la taille du cache mémoire sur une valeur supérieure à zéro.

Citrix Director

Intégration de Secure Private Access à Director (Technical Preview)

L'intégration de Secure Private Access à Director permet à l'administrateur du service d'assistance ou à l'administrateur complet de surveiller et de dépanner toutes les sessions Secure Private Access dans Director. Pour prendre en charge cette fonctionnalité, vous devez utiliser la version 2402 ou versions ultérieures de Director, de Secure Private Access, de l'application Citrix Workspace et du VDA.

Les actions disponibles incluent l'affichage des détails des éléments suivants :

- Sessions actives Secure Private Access pour un utilisateur dans la fenêtre contextuelle **Sélectionner une session** > onglet **Sessions** > **Applications Web et SaaS**
- Échecs des énumérations Secure Private Access ou énumérations bloquées et échecs de lancement d'application dans la fenêtre contextuelle **Sélectionner une session** > onglet **Accès refusé**
- Affichage des détails des sessions et des applications pour les lancements d'application actifs et ayant échoué
- Affichage des détails de session et d'application pour les échecs des énumérations et les énumérations bloquées

Pour plus d'informations, consultez la page Intégration de Secure Private Access à Director (Technical Preview).

Amélioration du panneau Indicateurs de performance

Le panneau **Indicateurs de performance** offre une visualisation améliorée des mesures en temps réel. Lorsque vous cliquez sur l'onglet **Performances des sessions**, vous pouvez voir les données en temps réel, ainsi que les données des 15 dernières minutes sans attendre le temps de chargement de la page. Cette amélioration contribue à réduire le temps moyen de résolution en permettant aux administrateurs de corréler les mesures de performance de plusieurs composants dans une seule vue. Pour plus d'informations, consultez la section Indicateurs de performance.

Prise en charge de la nouvelle version de Microsoft Teams

Citrix Director prend désormais en charge Microsoft Teams 2.1 ou la version antérieure.

Machine Creation Services (MCS)

Gestion des images (Technical Preview)

Grâce à la fonctionnalité de gestion des images, MCS sépare la phase de mastering du workflow global de provisioning.

Vous pouvez préparer une image MCS (image préparée) à partir d'une seule image source et l'utiliser dans plusieurs catalogues de machines MCS différents. Cette implémentation réduit considérablement les coûts en stockage et en temps, et simplifie le déploiement des machines virtuelles et le processus de mise à jour des images.

Les avantages de cette fonctionnalité de gestion d'images sont les suivants :

- Générez des images préparées à l'avance sans créer de catalogue.
- Réutilisez les images préparées dans plusieurs scénarios, tels que la création et la mise à jour d'un catalogue.
- Réduisez considérablement le temps de création ou de mise à jour du catalogue.

Pour des informations détaillées sur la gestion des images, consultez la section Gestion des images (Technical Preview).

Vérifier la présence de plusieurs cartes d'interface réseau dans VMware

Dans les environnements VMware, nous avons introduit plusieurs vérifications préalables lorsque l'unité d'hébergement et le modèle de profil de machine disposent de plusieurs réseaux, et que le paramètre `-NetworkMapping` est utilisé dans les commandes `New-ProvScheme` et `Set-ProvScheme`. Pour plus d'informations sur la liste des vérifications préalables pour plusieurs cartes d'interface réseau, consultez la section Vérifier la présence de plusieurs cartes d'interface réseau.

Prise en charge de la création de machines virtuelles Windows 11 dans GCP

Vous pouvez désormais créer des machines virtuelles Windows 11 dans GCP. Si vous installez Windows 11 sur l'image principale, vous devez activer vTPM pendant le processus de création de l'image principale. Vous devez également activer vTPM sur la source du profil de la machine (machine virtuelle ou modèle d'instance).

Cette fonctionnalité s'applique aux éléments suivants :

- Catalogues de machines MCS persistants et non persistants
- Groupe de nœuds à locataire unique uniquement

Pour plus d'informations sur la création de machines virtuelles Windows 11 sur le nœud à locataire unique, consultez Créer des machines virtuelles Windows 11 sur le nœud à locataire unique.

Prise en charge de la création de catalogues Citrix Provisioning à l'aide des commandes MCS PowerShell dans VMware

Vous pouvez désormais créer des catalogues Citrix Provisioning à l'aide des commandes MCS PowerShell dans VMware.

Cette implémentation vous offre les avantages suivants :

- Une API unifiée unique pour gérer à la fois les catalogues MCS et Citrix Provisioning.
- Bénéficiez de nouvelles fonctionnalités pour les catalogues Citrix Provisioning, telles qu'une solution de gestion des identités, le provisioning à la demande, etc.

Pour plus d'informations, consultez la section Créer des catalogues Citrix Provisioning dans Citrix Studio.

Profile Management

Pour plus d'informations sur les nouvelles fonctionnalités, consultez l'article Nouveautés dans sa documentation.

Linux VDA

Pour plus d'informations sur les nouvelles fonctionnalités, consultez l'article Nouveautés dans sa documentation.

Enregistrement de session

Pour plus d'informations sur les nouvelles fonctionnalités, consultez l'article Nouveautés dans sa documentation.

Workspace Environment Management

Pour plus d'informations sur les nouvelles fonctionnalités, consultez l'article Nouveautés dans sa documentation.

Citrix Provisioning

Pour plus d'informations sur les nouvelles fonctionnalités, consultez l'article Nouveautés dans sa documentation.

Service d'authentification fédérée

Pour plus d'informations sur les nouvelles fonctionnalités, consultez l'article Nouveautés dans sa documentation.

Composants de base de la version initiale 2402 LTSR

Composant de référence de 2402	Version indiquée dans Programmes et fonctionnalités	documentation
VDA mono-session	2402.0.4000.4310	VDA mono-session
VDA multi-session	2402.0.4000.4310	VDA multi-session
Delivery Controller	7.41.100.229	Delivery Controller
Citrix Studio	7.41.100.251	Citrix Studio
Citrix Director	7.33.4000.26	Citrix Director
Gestion de stratégie de groupe Citrix	7.41.100.115	Gestion de stratégie de groupe Citrix
Extension de stratégie de groupe côté client Citrix	7.41.100.115	
Citrix StoreFront	2402.0.100.64	Citrix StoreFront
Citrix Provisioning	7.41.100	Citrix Provisioning
Serveur d'impression universelle	7.33.4000.11	Serveur d'impression universelle
Enregistrement de session	24.2.100.35	Enregistrement de session
Linux VDA	24.02.0.93	Linux Virtual Delivery Agent
Profile Management	24.2.100.52	Profile Management
Service d'authentification fédérée de Citrix	10.17.100.90	Service d'authentification fédérée (FAS) de Citrix
Redirection de contenu du navigateur	15.32.4000.12	Redirection de contenu du navigateur
Citrix Probe Agent 2402	7.41.100.78	Télécharger

Composants compatibles avec la version initiale 2402 LTSR

Les composants suivants, dans les versions indiquées ci-dessous, sont compatibles avec les environnements LTSR. Ils ne bénéficient pas des avantages du programme LTSR (cycle de vie prolongé et mises à jour cumulatives contenant uniquement des corrections). Citrix peut vous demander de mettre à niveau vers une version plus récente de ces composants dans vos environnements 2402.

Composants et fonctionnalités compatibles	Version indiquée dans Programmes et fonctionnalités	documentation
HDX RealTime Optimization Pack	2.9.600	HDX RealTime Optimization Pack
Serveur de licences	11.17.2.0_BUILD_47000	Serveur de licences
Couche de personnalisation de l'utilisateur	23.9.1	Couche de personnalisation de l'utilisateur
Lecteur Web d'enregistrement de session	22.3.4000.4	Lecteur Web d'enregistrement de session
Optimisation pour Microsoft Teams	15.32.3000.9	Optimisation pour Microsoft Teams
Workspace Environment Management	2402.1.100.1	Workspace Environment Management

Exclusions notables de la version initiale 2402 LTSR

Les fonctionnalités, plates-formes et composants suivants ne bénéficient pas des avantages et des étapes de cycle de vie de 2402. Plus précisément, le cycle de vie prolongé et les mises à jour cumulatives contenant uniquement des corrections sont exclus. Les mises à jour des fonctionnalités et composants exclus sont disponibles au travers des versions régulières.

Composants et fonctionnalités exclus
AppDisks
AppDNA
Pack d'administration Citrix SCOM
Framehawk
Personal vDisk

Composants et fonctionnalités exclus
Intégration de StoreFront Citrix Online

Plates-formes Windows exclues *
Windows 2008 32 bits (pour le serveur d'impression universelle)

* Citrix se réserve le droit de mettre à jour la prise en charge des plates-formes en fonction des étapes du cycle de vie des fournisseurs tiers.

Problèmes résolus

June 27, 2024

Citrix Virtual Apps and Desktops 7 2402 LTSR inclut les problèmes résolus suivants :

General

- Lorsque le nom du périphérique audio comporte plus de 200 caractères, le périphérique peut ne pas être redirigé vers la session virtuelle. [HDX-58341]
- Pour la redirection de la webcam, le client RDP vers le second saut n'est pas pris en charge. [HDX-55630]
- Lorsque vous analysez une image au cours d'une session de bureau avec l'environnement configuré conformément à la description donnée ci-dessous, il est possible que l'image ne soit pas analysée. Ce problème est intermittent.
  - Installation du pilote du scanner et de l'application d'imagerie.
  - Stratégie de direction USB activée sur DDC.
  - Configuration de l'environnement :
    - DDC : Win2K19 + 7.33CU4
    - VDA : Win2K19/Win2k16 + 7.40.0.191
    - Client : Win10x64 22H2 + application Citrix Workspace 24.1.0.597

  [HDX-58888]

- Le lancement d'une deuxième application transparente échoue si le protocole SSL est activé et que la fiabilité de session est désactivée. Si une application transparente est lancée, le lancement ultérieur d'une autre application transparente sur le même serveur doit être effectué dans la session existante (partage de session), tandis que le client a tendance à lancer l'application dans une nouvelle session, ce qui entraîne l'envoi d'une demande de validation inattendue au broker. [HDX-52439].
- Si vous utilisez un son mono pour des flux audio stéréo, il se peut que vous n'entendiez qu'un seul canal audio dans un écouteur au lieu de recevoir les deux canaux dans les deux oreilles. [HDX-56344]

Delivery Controller

- Les mises à jour de la table `MonitorData.ResourceUtilization` de la base de données de surveillance sont retardées. [CVADHELP-22724]
- Lorsque vous utilisez un VDA version 2203 CU3 avec Windows 10, le programme d'installation du VDA n'héberge pas le port WCF personnalisé si le proxy Rendezvous est configuré. [CVADHELP-24199]

Director

- Lorsque vous utilisez un VDA de bureau multisession ou mono-session dans **Multi Forest Site**, la fonction de recherche centrée sur l'utilisateur ne fonctionne pas. [CVADHELP-23174]

Graphiques

- Pour Windows 11 version 22H2, lorsque vous déplacez une fenêtre de Windows Media Player au cours d'une session, seule la moitié inférieure de la vidéo s'affiche. Pour contourner ce problème, sélectionnez : Paramètres > Système > Multitâche > Ancrer les fenêtres > Afficher les mises en page d'ancrage lorsque je fais glisser une fenêtre vers le haut de mon écran. [HDX-42092]
- Lorsque vous utilisez Citrix Virtual Apps and Desktops 2203, il est possible que vous observiez un écran noir lors de la reconnexion aux sessions déconnectées. [CVADHELP-23615]

Stratégie

- Après la mise à niveau de Citrix Virtual Apps and Desktops de la version 1912 LTSR CU3 vers la version CU4 ou CU5, il se peut que les VDA ne s'enregistrent pas auprès de Delivery Controller et ils ne restent pas enregistrés. [CVADHELP-19834]

- `CSEngine.exe` consomme plus de mémoire que prévu sur le VDA. [CVADHELP-20908, CVADHELP-19916]

Studio

- Les administrateurs personnalisés qui ne disposent pas de l'étendue « Tous » ne peuvent pas modifier ou supprimer les stratégies de l'ensemble de stratégies par défaut. Pour contourner ce problème, ajoutez une étendue à la stratégie par défaut à laquelle l'administrateur personnalisé peut accéder. [GP-1569]
- Lorsque vous utilisez *Citrix Studio* et *Web Studio* dans votre déploiement, vous pouvez rencontrer les problèmes suivants : si vous créez un dossier d'applications dans *Citrix Studio*, mais que vous n'y ajoutez aucune application, ce dossier vide n'apparaît pas dans *Web Studio*. [STUD-27526]
- Lors de la création d'une connexion d'hébergement à Azure à l'aide de Web Studio, si vous cliquez sur **Créer un principal de service** sur la page **Détails de la connexion** et que vous cliquez sur **Suivant**, vous risquez de recevoir une erreur. Pour résoudre le problème, autorisez les cookies tiers dans le navigateur. [STUD-24463]
- Lorsque vous ajoutez l'adresse du serveur StoreFront via Citrix Studio et que vous l'affectez à un groupe de mise à disposition, le magasin est désactivé par défaut.
  [CVADHELP-24862]

Serveur d'impression universelle

Impression

- Lorsque vous utilisez un VDA version 1912 CU5 et un système d'exploitation 2012 R2, plusieurs tâches d'impression du serveur d'impression Citrix UPS de production échouent avec le message d'erreur suivant :
  `CCgpStream::Open: WaitForMultipleObjects time out. InternalUpcRemoteOpenSt`
  `: Failed to Open Stream. Abort Job.`
  [CVADHELP-22354]
- Lorsque vous utilisez la version 2212 ou 2305 d'UPS dans Citrix Virtual Apps and Desktops version 2212 ou 2305 avec un VDA Windows 10, les imprimantes utilisant CUPS affichent le message suivant :
  `Access Denied, cannot connect message`
  [CVADHELP-23644]

VDA pour OS mono-session

- Lorsque vous utilisez le VDA Windows, vous risquez de rencontrer une erreur de mappage du clavier lorsque vous passez du clavier japonais au clavier coréen. [HDX-59307]
- Les valeurs `SaveRsopToFile`, `SaveRsopToMemory` et `SaveRsopToRegistry` de la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy` risquent de ne pas être restaurées. [CVADHELP-23184]
- Après la mise à niveau d'un VDA vers la version 2203, l'application Skype Entreprise peut ne plus répondre sur l'écran de démarrage. [CVADHELP-21021]
- `CSEngine.exe` consomme plus de mémoire que prévu sur le VDA. [CVADHELP-19916]
- Un blocage dans l'agent Broker empêche les machines de se réenregistrer lors d'un changement d'adresse IP DNS. [CVADHELP-18952]
- Ce correctif introduit l'option de ligne de commande `/no_pending_reboot_check` qui empêche de vérifier si un redémarrage est en attente depuis une installation précédente de Windows sur la machine lors de l'installation ou de la mise à niveau des composants principaux. [CVADHELP-21686]
- Le processus `WebSocketService.exe` ne démarre pas après le redémarrage d'un VDA. [CVADHELP-24771]
- Lorsque vous utilisez un VDA version LTSR 2203 CU 4.1, il peut effectuer une vérification des bogues et envoyer le message suivant à tout moment, au début ou au cours d'une session.

  ```
  Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED": Tdica.sys
  ```

[CVADHELP-24891]

- Lorsque vous utilisez une machine, le lancement de la session utilisateur échoue par intermittence. [CVADHELP-23922]
- Lors de la reconnexion d'une session ICA, la fenêtre de discussion d'une application de messagerie tierce peut apparaître automatiquement au premier plan. [CVADHELP-24000]
- Le processus `Wfshell.exe` peut se bloquer lorsque vous copiez et collez des fichiers depuis un poste de travail local dans la session Citrix pour VDA LTSR 2203. [CVADHELP-24146]
- Lorsque vous utilisez un VDA Windows 10 version 2308, le processus `ctxappvservice.exe` peut se bloquer. [CVADHELP-24575]
- La copie du contenu d'une application Microsoft Visio ou Visio publiée sur un bureau vers une application sur la machine utilisateur peut échouer. [CVADHELP-23647]
- WebSocketService (service WebSocker de redirection vidéo HTML5) peut se bloquer. [CVADHELP-23917]

- Une application définie sur la moitié gauche du moniteur gauche n'apparaît pas correctement au centre de l'écran une fois que vous vous êtes reconnecté lorsque vous utilisez Virtual Apps and Desktops 2203 LTSR, l'application Citrix Workspace 2203 LTSR CU3 (2303 ou 2205) et le VDA 2203 LTSR avec Windows 11 22h2. [CVADHELP-23878]

VDA pour OS multi-session

- Le processus `WebSocketService.exe` peut consommer plus de mémoire que prévu sur les VDA. [CVADHELP-23870]
- `CSEngine.exe` consomme plus de mémoire que prévu sur le VDA. [CVADHELP-19916]
- Un blocage dans l'agent Broker empêche les machines de se réenregistrer lors d'un changement d'adresse IP DNS. [CVADHELP-18952]
- Le processus `WebSocketService.exe` ne démarre pas après le redémarrage d'un VDA. [CVADHELP-24771]
- Lorsque vous utilisez un VDA version LTSR 2203 CU 4.1, il peut effectuer une vérification des bogues et envoyer le message suivant à tout moment, au début ou au cours d'une session. `Error "StopCode: SYSTEM THREAD EXCEPTION NOT HANDLED": Tdica.sys` [CVADHELP-24891]
- Certains processus de l'application Citrix Workspace peuvent ne pas se fermer comme prévu lorsqu'ils s'exécutent dans une session d'application publiée. [CVADHELP-24225]
- Avec la version LTSR 2203 CU3 de VDA Server 2019, le processus `WmiPrvSE.exe` se bloque. [CVADHELP-24436]
- Le processus `Wfshell.exe` peut se bloquer lorsque vous copiez et collez des fichiers depuis un poste de travail local dans la session Citrix pour VDA LTSR 2203. [CVADHELP-24146]
- Le processus Terminal Services peut se bloquer après la reconnexion ACR. [CVADHELP-24364]
- Dans Windows Server 2022, si l'application ou le système d'exploitation déplace un curseur de souris vers une position dédiée, vous ne pourrez pas déplacer le curseur de souris tant que l'application ou le système d'exploitation ne l'aura pas déplacé à un autre endroit. [CVADHELP-24444]
- La boîte de dialogue **Message d'avertissement : délai d'inactivité dépassé** ne s'affiche pas dans la session ICA sur le VDA OS 2022, bien que la durée limite d'**inactivité de session** soit effective. [CVADHELP-24646]
- La copie du contenu d'une application Microsoft Visio ou Visio publiée sur un bureau vers une application sur la machine utilisateur peut échouer. [CVADHELP-23647]

Profile Management

- La documentation Profile Management 2402 LTSR fournit des informations spécifiques sur les mises à jour de cette version.

Linux VDA

- La documentation Linux VDA 2402 LTSR fournit des informations spécifiques sur les mises à jour de cette version.

Enregistrement de session

- La documentation Enregistrement de session 2402 LTSR fournit des informations spécifiques sur les mises à jour de cette version.

Workspace Environment Management

- La documentation Workspace Environment Management 2402 LTSR fournit des informations spécifiques sur les mises à jour de cette version.

Citrix Provisioning

- La documentation Citrix Provisioning 2402 LTSR fournit des informations spécifiques sur les mises à jour de cette version.

Service d'authentification fédérée

- La documentation du Service d'authentification fédérée 2402 LTSR fournit des informations spécifiques sur les mises à jour apportées à cette version.

Problèmes connus

June 27, 2024

Citrix Virtual Apps and Desktops 7 2402 LTSR inclut les problèmes connus suivants :

Remarques

- Si un problème connu a une solution, celle-ci est fournie après la description du problème.
- L'avertissement suivant s'applique à toute solution qui suggère de modifier une entrée de registre :

  > **Avertissement :**
  >
  > Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

General

- Si vous lancez la barre d'applications, puis ouvrez le menu Centre de connexion dans l'application Citrix Workspace pour Windows, la barre d'applications n'apparaît pas sous le serveur qui l'héberge. [HDX-27504]
- Si vous utilisez l'application Citrix Workspace pour Windows et que vous lancez la barre d'applications en position verticale, la barre couvre le menu Démarrer ou la barre d'état d'horloge système. [HDX-27505]
- La zone de liste peut ne pas s'afficher correctement lorsqu'un utilisateur sélectionne une zone de liste qui est déjà active sur l'hôte. Pour contourner le problème, sélectionnez un autre élément d'interface utilisateur, puis sélectionnez la zone de liste. [HDX-21671]
- Citrix Desktop Service peut ne pas démarrer après avoir effectué une mise à niveau du système d'exploitation sur place de Windows 10 vers Windows 11. Pour résoudre le problème, redémarrez l'ordinateur. [HDX-58399]
- Les paramètres de **limites de session** des VDA multisession sont refusés sur les hôtes de session exécutant Windows Server 2022, Windows 10 Enterprise multisession et Windows 11 Enterprise multisession.
  Pour contourner ce problème, vous pouvez configurer les **limites de temps de session RDS** via l'objet de stratégie de groupe. [HDX-47001]
- La boîte de dialogue de sécurité Windows associée à FIDO2 ne s'affichera pas devant la fenêtre de session ICA si vous exécutez l'application avec des privilèges d'administrateur. Selon la conception du système d'exploitation, la boîte de dialogue de Windows Security sera masquée derrière la fenêtre de session ICA si elle s'exécute en tant que processus avec élévation de privilège. [HDX-26794]

- Le copier-coller du presse-papiers peut échouer pour les données supérieures à 100 Mo entre le client et la session ICA. Les copies tampon volumineuses ne sont pas prises en charge. [HDX-59028]
- Bien qu'un point de restauration soit créé, un VDA ne peut pas être restauré en cas d'échec de l'installation d'un VDA sur la plate-forme multisession Windows 10 ou Windows 11. L'installation du VDA a été initiée via l'interface utilisateur ou la ligne de commandes. [HDX-58915]
- Le système d'exploitation multisession Windows 10 ou Windows 11 ne prend pas en charge la restauration du système Windows. Par conséquent, l'option permettant de créer un point de restauration n'est pas disponible dans l'interface utilisateur. Les options de ligne de commandes `/EnableRestore` ou `/EnableRestoreCleanup` sont ignorées et le message « **Désactivation de la restauration du système** comme non prise en charge actuellement sur le système d'exploitation multisession Windows 10/11 » est enregistré. [HDX-58915]
- Citrix signe à la fois les fichiers binaires générés par Citrix et les fichiers binaires tiers. Cela signifie que les fichiers binaires sont authentifiés par Citrix. Les versions des fichiers binaires tiers restent les mêmes, car elles ont été obtenues auprès de tiers. Si un fichier binaire est déjà installé, une mise à niveau du VDA n'installe pas les fichiers binaires, car les versions correspondent. Pour éviter cette limitation, procédez comme suit :

  1. Incluez les fichiers binaires dans une **liste verte**. Il n'est donc plus nécessaire de signer les fichiers binaires.
  2. Désinstallez l'ancien VDA et installez le nouveau VDA. Cela ressemble à une nouvelle installation de VDA et les versions signées sont appliquées.

  [HDX-62302]
- Dans certains scénarios, lorsque vous utilisez le filtre de stratégie d'adresse IP du client, l'adresse IP utilisée pour évaluer la stratégie est incorrecte. [HDX-62375]
- Lorsque vous utilisez le transfert de domaine amélioré pour l'authentification unique, l'authentification unique dans la session peut échouer si la machine cliente ou l'hôte de la session exécute Windows 11. [HDX-62973]

Stratégies

- Si vous effectuez une mise à niveau à partir d'une version antérieure de Citrix Virtual Apps and Desktops vers la version 2311 ou 2402 LTSR, les données de stratégie risquent d'être perdues si des valeurs de données non valides sont définies dans les paramètres de stratégie. Pour en savoir plus sur le problème et les solutions de contournement associées, consultez CTX666304. [GP-1671]

Graphiques

- Si vous démarrez un aperçu vidéo à l'aide d'une application webcam 64 bits sur la compression Theora, la session peut se bloquer. [HDX-21443]
- Vous remarquerez peut-être que des webcams supplémentaires sont connectées au bureau distant dans l'application Skype pour ordinateur de bureau. L'aperçu de ces webcams supplémentaires est bloqué et peut afficher un écran noir pour des raisons de sécurité. Vous pouvez ignorer les webcams supplémentaires et continuer à utiliser la webcam pour le point de terminaison. [HDX-58807]
- H265 444 sur Intel et certains GPU NVIDIA peuvent entraîner l'affichage d'artefacts pendant la session. Pour les problèmes liés aux GPU Intel, il existe une solution temporaire pour redimensionner la session ou basculer en mode plein écran. [PMCS-41084]

Machine Creation Services

- Dans un environnement VMware hébergé sur AWS, la création du catalogue de machines MCS échoue si le vTPM est activé sur l'image principale. Ce problème concerne toutes les versions de Citrix Virtual Apps and Desktops. Pour obtenir de l'assistance VMware, consultez la section Obtenir de l'assistance. [PMCS-37603]
- Lors de la mise à niveau d'un site à plusieurs composants Delivery Controller à partir de certaines versions LTSR antérieures à la version 2402 (y compris les versions 2302, 2305, 2308, 2311) avec la version 2402 LTSR, les actions d'alimentation sur une machine virtuelle peuvent échouer si le site n'est que partiellement mis à niveau. Pour plus d'informations, consultez l'article CTX666299.

Impression

- Les imprimantes du serveur d'impression universelle sélectionnées dans le bureau virtuel n'apparaissent pas dans la fenêtre **Périphériques et imprimantes** du Panneau de configuration. Toutefois, lorsque les utilisateurs travaillent dans les applications, ils peuvent utiliser ces imprimantes. Ce problème se produit uniquement sous Windows 10. Pour plus d'informations, consultez la section CTX213540. [HDX-5043, 335153]
- L'imprimante par défaut peut ne pas être marquée correctement dans la fenêtre d'impression. Ce problème n'affecte pas les travaux d'impression envoyés à l'imprimante par défaut. [HDX-12755]
- Certaines tâches d'impression provenant d'imprimantes réseau à équilibrage de charge peuvent échouer lorsque les connexions SSL aux serveurs d'impression universels sont activées.

Cela se produit lorsque les tâches d'impression sont lancées rapidement les unes après les autres. [HDX-58316]

Problèmes tiers

- Chrome prend en charge l'automatisation de l'interface utilisateur uniquement pour les barres d'outils, les onglets, les menus et les boutons autour d'une page Web. En raison de ce problème de Chrome, la fonction d'affichage automatique du clavier peut ne pas fonctionner dans un navigateur Chrome sur les périphériques tactiles. Pour contourner le problème, exécutez `chrome --force-renderer-accessibility` ou ouvrez un nouvel onglet du navigateur, tapez `chrome://accessibility` et activez la prise en charge de **l'API d'accessibilité native** pour des pages spécifiques ou toutes les pages. En outre, lorsque vous publiez une application transparente, vous pouvez publier Chrome à l'aide du commutateur `--force-renderer-accessibility`. [HDX-20858]
- Un écran noir peut s'afficher lors du lancement d'une session si FSLogix 2201 HF1 est installé sur l'hôte de la session. Pour résoudre ce problème, vous devez mettre à niveau FSLogix vers une version plus récente. [HDX-46159]

Profile Management

- La documentation Profile Management 2402 LTSR fournit des informations spécifiques sur les mises à jour de cette version.

Linux VDA

- La documentation Linux VDA 2402 LTSR fournit des informations spécifiques sur les mises à jour de cette version.

Enregistrement de session

- La documentation Enregistrement de session 2402 LTSR fournit des informations spécifiques sur les mises à jour de cette version.

Workspace Environment Management

- La documentation Workspace Environment Management 2402 LTSR fournit des informations spécifiques sur les mises à jour de cette version.

Citrix Provisioning

- La documentation Citrix Provisioning 2402 LTSR fournit des informations spécifiques sur les mises à jour de cette version.

Service d'authentification fédérée

- La documentation du Service d'authentification fédérée 2402 LTSR fournit des informations spécifiques sur les mises à jour apportées à cette version.

Fin de prise en charge

June 27, 2024

Les annonces de cet article visent à vous avertir à l'avance des plates-formes, des produits Citrix et des fonctionnalités qui vont disparaître pour que vous puissiez prendre les décisions appropriées. Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand les retirer. Les annonces peuvent être modifiées dans les versions ultérieures et peuvent ne pas contenir chaque fonctionnalité amenée à disparaître. Pour obtenir des informations sur la prise en charge du cycle de vie d'un produit, consultez l'article Politique relative au cycle de vie du support produit Citrix. Pour plus d'informations sur l'option de maintenance LTSR (Long Term Service Release), reportez-vous à la section https://support.citrix.com/article/CTX205549.

Fins de prise en charge et retraits

Le tableau suivant indique les plates-formes, les produits Citrix et les fonctionnalités qui sont obsolètes ou ont été retirés. Les dates en **caractères gras** indiquent les modifications apportées dans cette version.

Fins de prise en charge

La fin de prise en charge signifie que nous avons l'intention de supprimer la fonctionnalité ou la capacité d'une prochaine version. La fonctionnalité ou la capacité continuera de fonctionner et sera entièrement prise en charge jusqu'à sa suppression officielle. Cette notification de fin de prise en charge peut s'étendre sur quelques mois, voire plusieurs années. Une fois supprimée, la fonctionnalité ou la capacité ne fonctionnera plus. Cet avis a pour but de vous laisser suffisamment de temps pour planifier et mettre à jour votre code avant la suppression de la fonctionnalité ou de la capacité. Nous suggérons des solutions alternatives pour les éléments obsolètes dans la mesure du possible.

Élément	Abandon annoncé dans la version	Solution alternative
Rendezvous V1	2402	Utilisez Rendezvous V2.
Secure ICA	2402	-
Prise en charge des VDA sur Windows Server 2016	2402	Effectuez une mise à niveau vers les versions les plus récentes de Windows Server.
Prise en charge de Delivery Controller, Web Studio, Citrix Director, Citrix License Server, Citrix StoreFront, Server VDI pour un système d'exploitation mono-session, un VDA pour un système d'exploitation multisession, une forêt et un domaine Active Directory, et un serveur d'impression universelle sur Windows Server 2016	2402	Mettez à niveau vers la version la plus récente de Windows Server.
Prise en charge de Microsoft SQL Server versions 2016 et 2017 pour les bases de données de configuration de site, de journalisation de la configuration et de surveillance	2402	Mettez à niveau vers la version la plus récente de Windows SQL Server.
Prise en charge de la configuration du cache en écriture différée pour inclure uniquement un cache disque et aucun cache mémoire	2402	Utilisez l'option de configuration de la taille du cache mémoire et allouez une taille différente de zéro.
Prise en charge des catalogues Azure créés avant la fonctionnalité de provisioning à la demande (catalogues « d'ancienne génération »)	2402	Recréez les machines virtuelles du catalogue Azure d'ancienne génération. Les catalogues sont provisionnés à la demande, ce qui permet de réduire les coûts de stockage.

Élément	Abandon annoncé dans la version	Solution alternative
Stratégie **Fréquence d'images minimum cible**	2311	Utilisez l'**indicateur d'état graphique** pour modifier le taux de trame minimum cible.
Support pour Citrix Connector 3.1 pour System Center Configuration Manager	2311	Effectuez manuellement la mise à jour de l'image ou de l'application.
Prise en charge de l'utilisation d'une image principale dans une région différente de celle dans laquelle le catalogue est créé	2311	Utilisez Azure Compute Gallery pour répliquer l'image principale dans la région souhaitée.
Réglage de la limite de mémoire de l'écran graphique HDX	2311	La quantité minimale de mémoire requise est allouée pour s'assurer que la disposition d'affichage du client est parfaitement adaptée.
Prise en charge du mode progressif dans HDX Graphics	2311	Utilisez Thinwire. Voir Mode progressif.
Prise en charge de la redirection de contenu de navigateur dans Internet Explorer 11	2311	Utilisez la redirection du contenu du navigateur basée sur Google Chrome.
Suppression de la prise en charge du travailleur de volume AWS	2311	Utiliser le chargement et le téléchargement directs sur disque. Voir Chargement et téléchargement directs sur disque.
Prise en charge de SQL Server 2016 dans Broker	2308	Utilisez les dernières versions. Pour plus d'informations, veuillez consulter la section Configuration système requise.
Prise en charge de XenApp 5.x dans Director	2308	—
Prise en charge de XenApp 6.x dans Director	2308	—

Élément	Abandon annoncé dans la version	Solution alternative
Pack SCOM pour les alertes dans Director	2308	—
Prise en charge du plug-in dans Director	2308	—
Prise en charge du format WebRTC SDP (Plan B)	2308	Mettez à niveau l'application Citrix Workspace vers une version prise en charge.
Prise en charge du mode fenêtre unique dans Optimisation Microsoft Teams	2308	Mettez à niveau l'application Citrix Workspace vers une version prenant en charge le mode multi-fenêtres. Pour plus d'informations, consultez Tableau des fonctionnalités et versions prises en charge.
Prise en charge de `AwsCaptureInstanceProperties` utilisé dans les environnements AWS	2308	Utilisez un profil de machine. Reportez-vous à la section Créer un catalogue à l'aide d'un profil de machine.
Commande PowerShell `Schedule-ProvVMUpdate`	2305	Utilisez `Set-ProvVMUpdateTimeWindow`.
Commande PowerShell `Request-ProvVMUpdate`	2305	Utilisez `Set-ProvVMUpdateTimeWindow` avec les paramètres `-StartsNow` et `-DurationInMinutes -1`.
Commande PowerShell `Cancel-ProvVMUpdate`	2305	Utilisez `Clear-ProvVMUpdateTimeWindow`.
Paramètre `DedicatedTenancy` utilisé dans la commande `New-ProvScheme`	2303	Utilisez le paramètre `TenancyType`.
Serveur de licences VPX	2206	—

Élément	Abandon annoncé dans la version	Solution alternative
Disque non géré pour provisionner des machines virtuelles dans les environnements Azure.	2206	Utiliser des disques gérés
Redirection hôte vers client (URL)	2203	Redirection bidirectionnelle du contenu
Prise en charge de quatre commandes spécifiques à AWS : `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` et `Grant-HypSecurityGroupIngress` utilisées dans un environnement cloud et local.	2203	—
Citrix Files pour Windows et Citrix Files pour Outlook à partir du métainstaller du VDA.	2203	Utilisez les programmes d'installation autonomes.
Composant de l'agent WEM à partir du métainstaller du VDA.	2203	—
Option de veille sur le réseau local intégrée à SCCM pour Remote PC Access.	2012	Utilisez la fonction autonome de veille sur le réseau local.

Élément	Abandon annoncé dans la version	Solution alternative
Packs d'administration Citrix SCOM pour XenApp et XenDesktop, Provisioning Services et StoreFront. Pour connaître les versions de produits qui peuvent être surveillées, consultez la documentation Citrix SCOM Management Packs.	1912	Utilisez Director pour surveiller et gérer votre déploiement. Pour plus d'informations sur la fin de vie de SCOM et les alternatives, consultez https://support.citrix.com/article/CTX266943.
SDK Mobilité / SDK Mobile (dans Citrix Labs)	7.16	Remplacé par les paramètres de stratégie d'expérience mobile et les expériences natives pour les bureaux / applications hébergés.

Retraits

Les éléments retirés sont retirés, ou ne sont plus pris en charge, dans le service Citrix Virtual Apps and Desktops.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Application Citrix Workspace pour Windows 1912	—	2402	Utilisez les dernières versions.
Plein écran + Optimisation du texte HDX Graphics	2311	2311	
Prise en charge de la capture par tampon de trame NVIDIA (NVFBC) avec HDX 3D Pro	2308	2311	Utilisez l'API de duplication de bureau (DDAPI).

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Prise en charge VDA du paramètre de stratégie « Installation automatique de pilotes d'imprimante fournis avec Windows ».	7.16	2311	Aucun. Paramètre de stratégie pris en charge avec les VDA sur les systèmes d'exploitation antérieurs uniquement (Windows 7, Windows Server 2012 R2 et versions antérieures).
Encodage matériel GPU NVIDIA (NVENC) avec : vGPU 11 et versions antérieures, et version de pilote 466.77 et antérieure.	2305	2305	Utilisez les pilotes NVIDIA actuellement pris en charge : vGPU 13 ou version ultérieure, version 471.41 ou ultérieure.
Citrix Supportability Tools (Supportability-Tool_x64 .msi) provenant du méta-installateur VDA.	—	2212	—
Citrix License Administration Console (incluse pour la dernière fois dans le serveur de licences Windows 11.16.3 build 30000 et supprimée dans le serveur de licences Windows v11.16.6 build 31000).	2003	2006	Utilisez la console Citrix Licensing Manager.
Prise en charge de la carte graphique Citrix Indirect Display Driver (IDD) sous Windows 10 version 1709 et antérieure.	2003	2003	Utilisez des VDA Citrix Virtual Apps and Desktops 7 1912 LTSR.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Codage matériel avec les GPU NVIDIA (NVENC) à l'aide de pilotes d'affichage GRID 9 ou antérieurs.	2003	2003	Utilisez des pilotes d'affichage GRID 10 avec les VDA Citrix Virtual Apps and Desktops 7 2003 ou version ultérieure, ou utilisez des VDA Citrix Virtual Apps and Desktops 7 1912 LTSR.
Fonction de réinitialisation du mot de passe (SSPR).	2003	2006	—
Prise en charge des versions de Microsoft .NET Framework antérieures à la version 4.8 pour les VDA et les composants principaux du serveur. Inclut Delivery Controller, Studio, Director et StoreFront.	1912	2003	Mettez à niveau vers .NET Framework version 4.8.
VDA sur Windows Server 2012 R2.	1912	2003	Installez les VDA sur un système d'exploitation pris en charge.
Composant de migration d'application AppDNA de Citrix Virtual Apps and Desktops Premium.	1909	2003	—
Installation de Studio sur des machines 32 bits (x86).	1909	2003	Installez sur un système d'exploitation x64 pris en charge.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Prise en charge du hook Excel dans les applications transparentes. Utilisé pour créer des icônes de barre des tâches distinctes pour chaque classeur Microsoft Excel 2010.	1909	1909	—
Composants de serveur principaux sur Windows Server 2012 R2 (y compris Service Packs). Comprend : Delivery Controller, Studio et Director.	1906	2003	Installez sur un système d'exploitation pris en charge plus récent.
Prise en charge de la configuration du site, de la journalisation de la configuration et des bases de données de surveillance sur Microsoft SQL Server versions 2008 R2, 2012 et 2014 (y compris tous les Service Packs et éditions).	1906	2003	Installez des bases de données sur une version Microsoft SQL Server prise en charge.
Prise en charge des VDA sous Windows 10 sur les plates-formes x86.	1906	1909*	Installez des VDA sur un système d'exploitation x64 pris en charge. *Cette fonctionnalité est toujours prise en charge dans Citrix Virtual Apps and Desktops 7 1912 LTSR.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Suppression de Citrix Smart Tools Agent du support d'installation de Citrix Virtual Apps and Desktops.	1903	1906	—
Suppression des options de Delivery Controller pour les produits en fin de vie suivants dans StoreFront : VDI-in-a-Box et XenMobile (9.0 ou version antérieure).	1903	1903	—
Prise en charge du VDA Linux sur Red Hat Enterprise Linux/CentOS 7.5.	1903	1903	Installez le VDA Linux sur une version ultérieure de Red Hat Enterprise Linux.
Prise en charge de StoreFront pour les protocoles TLS 1.0 et TLS 1.1 entre Citrix Virtual Apps and Desktops (anciennement XenApp et XenDesktop) et Citrix Receiver, et Workspace Hub.	7.17	2203	Mettez à niveau les Citrix Receiver vers une application Citrix Workspace qui prend en charge le protocole TLS 1.2. Pour plus d'informations sur l'application Citrix Workspace, voir https://docs.citrix.com/fr-fr/citrix-workspace-app.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Prise en charge VDA du paramètre de stratégie « Installation automatique de pilotes d'imprimante fournis avec Windows ».	7.16	2311	Aucun. Paramètre de stratégie pris en charge avec les VDA sur les systèmes d'exploitation antérieurs uniquement (Windows 7, Windows Server 2012 R2 et versions antérieures).
Prise en charge de StoreFront pour l'accès utilisateur aux bureaux sur les sites Desktop Appliance	1811	1912	Utilisez Desktop Lock pour les cas d'utilisation n'appartenant pas à un domaine.
Prise en charge de la technologie d'affichage à distance Framehawk	1811	1903	Utilisez Thinwire avec le transport adaptatif activé.
Prise en charge de Citrix Smart Scale dans toutes les versions de Citrix Virtual Apps and Desktops (et XenApp et XenDesktop). Cette fonctionnalité atteindra sa fin de vie le 31 mai 2019.	1808	1906	Pensez à utiliser Citrix Virtual Apps and Desktops Service sur Citrix Cloud pour améliorer la fonctionnalité de gestion de l'alimentation.
Prise en charge des versions 4.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 et 4.7 de Microsoft .NET Framework par Citrix StoreFront, les VDA Citrix, Citrix Studio, Citrix Director et Citrix Delivery Controller.	7.18	1808	Mettez à niveau vers .NET Framework version 4.7.1 ou ultérieure. (Le programme d'installation installe automatiquement .NET Framework 4.7.1 s'il n'est pas déjà installé.)

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Prise en charge du VDA Linux sur Red Hat Enterprise Linux 7.3.	7.18	1808	Installez le VDA Linux sur une version ultérieure de Red Hat Enterprise Linux.
Prise en charge pour le VDA Linux sur SUSE Linux Enterprise Server 11 Service Pack 4.	7.16	7.16	Installez le VDA Linux sur une version SUSE prise en charge.
Prise en charge du pilote Citrix WDDM sur les VDA.	7.16	7.16	Le pilote Citrix WDDM n'est plus installé avec les VDA.
VDA sur Windows 10 version 1511 (seuil 2) et versions antérieures des systèmes d'exploitation mono-session Windows, y compris Windows 8.x et Windows 7 (voir https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/).	7.15 LTSR (et 7.12)	7.16	Installez les VDA avec OS mono-session sur Windows 10 version minimale 1607 (Redstone 1) ou des canaux semi-annuels (ciblés) plus récents. Si vous utilisez 1607 LTSB, nous vous recommandons un VDA 7.15. Voir CTX224843.
VDA sur Windows Server 2008 R2 et Windows Server 2012 (y compris Service Packs)	7.15 LTSR (et 7.12)	7.16	Installez les VDA sur un système d'exploitation pris en charge.
Desktop Composition Redirection (anciennement appelé DirectX Command Remoting) (DCR)	7.15 LTSR	7.16	Utilisez Thinwire.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Expérience classique Citrix Receiver pour Web (interface utilisateur avec « bulles vertes »)	7.15 LTSR (et StoreFront 3.12)	1903	Expérience unifiée Citrix Receiver pour Web
Composants principaux sur Windows Server 2008 R2 et Windows Server 2012 (y compris Service Packs). Inclut : Delivery Controller, Studio, Director, StoreFront, Serveur de licences et Universal Print Server.	7.15 LTSR	7.18	Installez les composants sur un système d'exploitation pris en charge.
Fonction de réinitialisation des mots de passe en libre-service (SSPR) sur Windows Server 2012 et Windows Server 2008 R2 (y compris Service Packs)	7.15 LTSR	7.18	Installez sur un système d'exploitation pris en charge plus récent.
Studio sur Windows 7, Windows 8, et Windows 8.1 (y compris Service Packs).	7.15 LTSR	7.18	Installez Studio sur un système d'exploitation pris en charge.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Redirection Flash	7.15 LTSR	1912	Créez le contenu vidéo en tant que vidéo HTML5. Utilisez la redirection vidéo HTML5 pour le contenu géré et la redirection du contenu du navigateur pour les sites Web publics. Pour de plus amples informations, consultez la rubrique Fin de la vie de la redirection Flash Redirection.
Intégration de Citrix Online (produit Goto) avec StoreFront.	7.14 (et StoreFront 3.11)	StoreFront 3.12	—
Le compte utilisateur CtxAppVCOMAdmin qui était créé lors de l'installation du VDA et ajouté au groupe Administrateurs locaux sur la machine du VDA n'est plus créé. Le mécanisme de « COM » sous-jacent a également été supprimé.	7.14	7.14	Le service Windows CtxAppVService exécute la même fonction. Il est automatiquement installé et configuré et ne requiert aucune intervention de l'utilisateur.
Prise en charge du composant Serveur d'impression universelle, UpsServer, sur Windows Server 2008 32 bits	7.14	7.14	Installez sur un système d'exploitation pris en charge plus récent.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
StoreFront et Receiver pour Web sur Internet Explorer 8	7.13	7.13	—
Option d'installation de ligne de commande VDA /no_appv pour empêcher l'installation des composants Citrix App-V	7.13	7.13	Utilisez l'option d'installation de ligne de commande /exclude "Citrix Personalization for App-V - VDA".
Le programme d'installation du produit entier n'installe plus le composant logiciel enfichable Citrix.Common.Commands sur les nouvelles installations et le supprime automatiquement lors de la mise à niveau des installations existantes.	7.13	7.13	Certaines commandes PowerShell fournies par le composant logiciel enfichable Citrix.Common.Commands sont toujours disponibles dans le SDK XenApp 6.5.
Fonctionnalité partielle permettant de manipuler les données d'icônes qui était fournie par les applets de commande *-CtxIcon.	7.13	7.13	Maintenant fournie par les applets de commande *-BrokerIcon dans le service Broker.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Mode Thinwire d'ancienne génération	7.12	7.16	Utilisez Thinwire. Si vous utilisez le mode Thinwire d'ancienne génération sur Windows Server 2008 R2, migrez vers Windows Server 2012 R2 ou Windows Server 2016 et utilisez Thinwire.
Mises à niveau sur place depuis StoreFront 2.0, 2.1, 2.5 et 2.5.2.	7.13	7.16	Mettez à niveau à partir d'une de ces versions vers une version ultérieure prise en charge puis vers XenApp et XenDesktop 7.16.
Mises à niveau sur place depuis XenDesktop 5.6 ou 5.6 FP1	7.12	7.16	Migrez votre déploiement XenDesktop 5.6 ou 5.6 FP1 vers la version actuelle de XenDesktop. Pour ce faire, effectuez d'abord une mise à niveau vers XenDesktop 7.6 LTSR (avec la dernière CU), puis effectuez la mise à niveau vers la dernière version de Citrix Virtual Desktops (anciennement XenDesktop) ou la version LTSR.

Élément	Abandon annoncé dans la version	Supprimé dans la version	Solution alternative
Installation de Delivery Controller, Director, StoreFront ou Serveur de licences sur des machines 32 bits (x86).	7.12	7.16	Installez sur un système d'exploitation x64 pris en charge.
Location de connexion	7.12	7.16	Utilisez le Cache d'hôte local.
XenDesktop 5.6 utilisé sur Windows XP. Les installations de VDA sur Windows XP ne sont pas prises en charge.	7.12	7.16	Installez les VDA sur un système d'exploitation pris en charge.
Prise en charge des connexions CloudPlatform	7.12	2003	Utilisez un autre hyperviseur ou service de cloud pris en charge.
Prise en charge des connexions Azure Classic (également appelé Azure Service Management)	7.12	2003	Vous pouvez utiliser le service Virtual Apps and Desktops sur Citrix Cloud.
Fonctionnalité AppDisks (et l'intégration d'AppDNA dans Studio qui la prend en charge)	7.13	2003	Utilisez Citrix App Layering.
Fonctionnalité Personal vDisk	7.15	2006†	Utilisez la technologie de couches utilisateur Citrix App Layering ou la Couche de personnalisation des utilisateurs de Citrix.

† Dans Citrix Virtual Apps and Desktops 7 2003, le pilote Personal vDisk a été supprimé du programme d'installation du VDA. Dans Citrix Virtual Apps and Desktops 7 2006, le workflow du pilote Personal

vDisk a été supprimé de Studio.

Configuration système requise

June 27, 2024

Introduction

La configuration système requise détaillée dans ce document est valide lors de la publication de cette version du produit. Des mises à jour sont effectuées périodiquement. La configuration système requise des composants non couverts dans ce document (telles que systèmes hôte, application Citrix Workspace et Citrix Provisioning) est décrite dans leur documentation respective.

Consultez Préparer l'installation avant de procéder à l'installation.

Sauf spécification contraire, le programme d'installation du composant déploie automatiquement les composants logiciels requis (tels que les packs .NET et C++) si les versions requises ne sont pas détectées sur la machine. Le support d'installation Citrix contient également certains de ces logiciels requis.

Le support d'installation contient plusieurs composants tiers. Avant d'utiliser le logiciel Citrix, recherchez des mises à jour de sécurité à partir des composants tiers et installez-les.

Pour plus d'informations, consultez l'article du centre de connaissances CTX119253.

Les composants et les fonctionnalités qui peuvent être installés sur des serveurs Windows, ne peuvent pas être installés sur des serveurs Nano Server, sauf indication contraire. Server Core est pris en charge uniquement par les Delivery Controller et Director.

Configuration matérielle requise

Les valeurs RAM et d'espace disque s'ajoutent à la configuration requise pour l'image du produit, le système d'exploitation et d'autres logiciels sur la machine. Vos performances varient en fonction de votre configuration. La configuration comprend les fonctionnalités que vous utilisez, ainsi que le nombre d'utilisateurs et d'autres facteurs. Une configuration minimale peut ralentir les performances.

Le tableau suivant présente la configuration minimale requise pour les composants principaux.

Composant	Minimum
Tous les composants principaux et StoreFront sur un serveur, pour évaluation uniquement (ne pas installer sur un déploiement de production)	5 Go de RAM
Tous les composants principaux et StoreFront sur un serveur, pour un déploiement test ou un environnement de production de petite taille	12 Go de RAM
Delivery Controller (espace disque supplémentaire requis pour le cache d'hôte local)	5 Go de RAM, 800 Mo de disque dur, base de données : voir Recommandations sur le dimensionnement
Studio	1 Go de RAM, 100 Mo de disque dur
Director	2 Go de RAM, 200 Mo de disque dur
StoreFront	2 Go de RAM, consultez la documentation StoreFront pour les recommandations de disque
Serveur de licences	2 Go de RAM, consultez la documentation relative au système de licences pour les recommandations de disque

Dimensionnement des machine virtuelle qui mettent à disposition les bureaux et les applications

Nous ne pouvons pas fournir de recommandations en raison de la nature complexe et dynamique du matériel et chaque déploiement a des exigences différentes. En général, le dimensionnement d'une machine virtuelle de Citrix Virtual Apps est basé sur le matériel et non pas sur les charges de travail de l'utilisateur. L'exception est la RAM. Vous avez besoin de plus de RAM pour les applications qui consomment plus.

Informations supplémentaires :

- Citrix Tech Zone contient des recommandations sur le dimensionnement.
- L'article Scalabilité d'un serveur unique Citrix Virtual Apps and Desktops explique le nombre d'utilisateurs ou de machines virtuelles pouvant être pris en charge sur un seul hôte physique.

Microsoft Visual C++

Lors de l'installation d'un Delivery Controller, Virtual Delivery Agent (VDA) ou d'un serveur d'impression universelle, le programme d'installation Citrix installe automatiquement Microsoft Visual C++ 2015–2022 Redistributable.

- Si la machine contient une version antérieure de ce composant d'exécution (telle que 2015-2019), le programme d'installation Citrix la met à niveau.
- Si la machine contient une version antérieure à 2015, Citrix installe la nouvelle version en parallèle.

Delivery Controller

Systèmes d'exploitation pris en charge :

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, éditions Standard et Datacenter, avec option Server Core
- Windows Server 2016, éditions Standard et Datacenter, avec option Server Core

Exigences :

- Microsoft .NET Framework 4.8 est automatiquement installé si cette version ou une version ultérieure n'est pas déjà installée.
- Windows PowerShell 3.0, 4.0 ou 5.0.
- Microsoft Visual C++ 2015–2019 Redistributable.

Base de données

Les versions de Microsoft SQL Server prises en charge pour les bases de données de configuration de site, de journalisation de la configuration et de surveillance :

- SQL Server 2022, éditions Express, Standard et Entreprise.
- SQL Server 2019, éditions Express, Standard et Entreprise.
- SQL Server 2017, éditions Express, Standard et Entreprise.
  - Pour les nouvelles installations : Par défaut, SQL Server Express 2017 avec mise à jour cumulative 16 est installé lors de l'installation du Controller, si une installation SQL Server prise en charge existante n'est pas détectée.
  - Pour les mises à niveau, toute version SQL Server Express existante n'est pas mise à niveau.
- SQL Server 2016 SP2, éditions Express, Standard et Entreprise.

Les solutions haute disponibilité de base de données suivantes sont prises en charge (à l'exception de SQL Server Express qui prend uniquement en charge le mode autonome) :

- Instances de cluster de basculement AlwaysOn SQL Server
- Groupes de disponibilité SQL Server AlwaysOn (y compris les groupes de disponibilité de base)
- Mise en miroir de base de données SQL Server

L'authentification Windows est requise pour les connexions entre le Controller et la base de données de site SQL Server.

Considérations relatives au cache d'hôte local : Microsoft SQL Server Express LocalDB est une fonctionnalité de SQL Server Express que le cache d'hôte local utilise de manière autonome. Le cache d'hôte local ne nécessite aucun composant de SQL Server Express autre que SQL Server Express LocalDB.

- Lors de l'installation d'un Controller, Microsoft SQL Server Express LocalDB 2019 avec mise à jour cumulative 15 est installé pour une utilisation avec le cache d'hôte local. (Cette installation est différente de l'installation de SQL Server Express par défaut pour la base de données du site.)
- Lors de la mise à niveau d'un Controller, la version existante de Microsoft SQL Server Express LocalDB n'est pas mise à niveau automatiquement. Pour connaître les exigences et les procédures de remplacement, reportez-vous à Remplacer SQL Server Express LocalDB.

Informations supplémentaires sur la base de données :

- Bases de données
- CTX114501 répertorie les dernières versions des bases de données prises en charge
- Recommandations sur le dimensionnement des bases de données
- Cache d'hôte local

Studio Web

> **Remarque :**
>
> - Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.
> - Web Studio est une console de gestion Web qui vous permet de configurer et de gérer votre déploiement Citrix Virtual Apps and Desktops sur site. Il est conçu pour améliorer l'expérience utilisateur et répond généralement plus rapidement que Citrix Studio, la console de gestion basée sur Windows. Reportez-vous à la section Installer Web Studio.

Systèmes d'exploitation pris en charge :

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, éditions Standard et Datacenter, avec option Server Core
- Windows Server 2016, éditions Standard et Datacenter, avec option Server Core

Citrix Director

Systèmes d'exploitation pris en charge :

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, éditions Standard et Datacenter, avec option Server Core
- Windows Server 2016, éditions Standard et Datacenter, avec option Server Core

Exigences :

- Microsoft .NET Framework 4.8 est automatiquement installé si cette version ou une version ultérieure n'est pas déjà installée.
- Microsoft Internet Information Services (IIS) 7.0 et ASP.NET 2.0. Assurez-vous que le service de rôle Contenu statique est installé sur le serveur IIS. Si ce logiciel n'est pas déjà installé, vous êtes invité à insérer le support d'installation de Windows Server. Ensuite, ce logiciel est installé pour vous.
- Pour afficher les journaux des événements sur les machines sur lesquelles Citrix Director est installé, vous devez installer Microsoft .NET Framework 2.0.

Citrix Profile Management :

- Assurez-vous que Citrix Profile Management et Citrix Profile Management WMI Plugin sont installés sur le VDA (page **Composants supplémentaires** de l'assistant d'installation) et que Citrix Profile Management Service est en cours d'exécution pour afficher les détails du profil utilisateur dans Director.

L'intégration de System Center Operations Manager (SCOM) requiert :

- System Center 2012 R2 Operations Manager

Navigateurs pris en charge pour l'affichage de Director :

- Internet Explorer 11. Le mode de compatibilité n'est pas pris en charge pour Internet Explorer. Utilisez les paramètres de navigateur recommandés pour accéder à Director. Lorsque vous installez Internet Explorer, acceptez la valeur par défaut pour utiliser les paramètres de sécurité et de compatibilité recommandés. Si vous avez déjà installé le navigateur et que vous avez choisi de ne pas utiliser les paramètres recommandés, rendez-vous dans **Outils > Options Internet > Avancé > Réinitialiser** et suivez les instructions.
- Microsoft Edge.
- Firefox ESR (version de prise en charge étendue).
- Chrome.

La résolution d'écran optimale recommandée pour afficher Director est 1440 x 1024.

Virtual Delivery Agent (VDA) pour OS mono-session

Systèmes d'exploitation pris en charge :

- Windows 11
- Windows 10 (x64 uniquement), toutes les versions actuellement prises en charge par le support standard.
  - Pour connaître les éditions prises en charge, consultez l'article du centre de connaissances CTX224843.

Exigences :

- Microsoft .NET Framework 4.8 est automatiquement installé si cette version ou une version ultérieure n'est pas déjà installée.
- Microsoft Visual C++ 2015–2019 Redistributable.

Remote PC Access utilise ce VDA, que vous installez sur les PC de bureau physiques. Ce VDA prend en charge le démarrage sécurisé pour Citrix Virtual Desktops Remote PC Access sur Windows 10 et Windows 11.

Plusieurs fonctionnalités d'accélération multimédia (telles que la redirection Windows Media HDX Mediastream) requièrent que Microsoft Media Foundation soit installé sur la machine sur laquelle vous installez le VDA. Si la machine ne possède pas Media Foundation installé, les fonctionnalités d'accélération multimédia ne sont pas installées et ne fonctionnent pas. Ne supprimez pas Media Foundation de la machine après l'installation du logiciel Citrix. Dans le cas contraire, les utilisateurs ne peuvent pas se connecter à la machine. Sur la plupart des éditions d'OS mono-session Windows prises en charge, la prise en charge Media Foundation est déjà installée et ne peut pas être supprimée. Toutefois, N éditions n'incluent pas certaines technologies multimédia ; vous pouvez obtenir ce logiciel depuis Microsoft ou un composant tiers. Pour plus d'informations, veuillez consulter la section Préparer l'installation.

Pour plus d'informations sur les VDA Linux, consultez les articles Virtual Delivery Agent Linux.

Pour utiliser la fonctionnalité Server VDI, vous pouvez utiliser l'interface de ligne de commande pour l'installation d'un VDA pour OS mono-session Windows sur une machine Windows Server prise en charge. Consultez Server VDI pour plus d'informations.

Pour plus d'informations sur l'installation d'un VDA sur une machine Windows 7, voir Systèmes d'exploitation antérieurs.

Virtual Delivery Agent (VDA) pour OS multi-session

Systèmes d'exploitation pris en charge :

- Windows 11 (pris en charge uniquement avec Citrix DaaS)
- Windows 10 (x64 uniquement ; pris en charge uniquement avec Citrix DaaS), toute version offrant actuellement un support standard.
- Windows Server 2022
- Windows Server 2019, éditions Standard et Datacenter
- Windows Server 2016, édition Standard et Datacenter

Le programme d'installation déploie automatiquement la configuration requise, qui est également disponible sur le support d'installation Citrix dans les dossiers **Support** :

- Microsoft .NET Framework 4.8 est automatiquement installé si cette version ou une version ultérieure n'est pas déjà installée.
- Microsoft Visual C++ 2015–2019 Redistributable.

Le programme d'installation installe et active automatiquement les services de rôle des services Bureau à distance, s'ils ne sont pas déjà installés et activés.

Plusieurs fonctionnalités d'accélération multimédia (telles que la redirection Windows Media HDX Mediastream) requièrent que Microsoft Media Foundation soit installé sur la machine sur laquelle vous installez le VDA. Si la machine ne possède pas Media Foundation installé, les fonctionnalités d'accélération multimédia ne sont pas installées et ne fonctionnent pas. Ne supprimez pas Media Foundation de la machine après l'installation du logiciel Citrix ; sinon, les utilisateurs ne pourront pas ouvrir une session sur la machine. Sur la plupart des versions de Windows Server, la fonctionnalité Media Foundation est installée via le Gestionnaire de serveur. Pour plus d'informations, veuillez consulter la section Préparer l'installation.

Si Media Foundation n'est pas présent sur le VDA, les fonctionnalités multimédias suivantes ne fonctionnent pas :

- Redirection Windows Media
- Redirection vidéo HTML5
- Redirection de webcam HDX RealTime

Pour plus d'informations sur les VDA Linux, consultez les articles Virtual Delivery Agent Linux.

Pour plus d'informations sur l'installation d'un VDA sur une machine Windows Server 2008 R2, voir Systèmes d'exploitation antérieurs.

Hôtes et ressources de virtualisation

Les ressources hôte/virtualisation suivantes (répertoriées par ordre alphabétique) sont prises en charge. Le cas échéant, les versions *major.minor* sont prises en charge, y compris les mises à jour de ces versions. L'article du centre de connaissances CTX131239 contient des informations sur la version actuelle, ainsi que des liens vers les problèmes connus.

Certaines des fonctionnalités peuvent ne pas être prises en charge sur toutes les plates-formes hôte ou toutes les versions de plate-forme. Pour de plus amples informations, consultez la documentation relative aux fonctionnalités.

La fonctionnalité Remote PC Access Wake on LAN requiert Microsoft System Center Configuration Manager minimum 2012.

Hyperviseurs pris en charge :

- **XenServer (anciennement Citrix Hypervisor)**

  L'article CTX131239 contient des informations sur la version actuelle, ainsi que des liens vers les problèmes connus.

  Pour plus d'informations, consultez l'article Environnements de virtualisation XenServer.

- **Microsoft System Center Virtual Machine Manager**

  Comprend toute version d'Hyper-V qui peut s'inscrire auprès des versions prises en charge de System Center Virtual Machine Manager.

  L'article CTX131239 contient des informations sur la version actuelle, ainsi que des liens vers les problèmes connus.

  Pour de plus amples informations, consultez Environnements de virtualisation Microsoft System Center Virtual Machine Manager.

- **Nutanix Acropolis**

  L'article CTX131239 contient des informations sur la version actuelle, ainsi que des liens vers les problèmes connus.

  Pour plus d'informations, veuillez consulter Environnements de virtualisation Nutanix.

- **VMware vSphere (vCenter + ESXi)**

  aucune prise en charge n'est fournie pour l'opération vSphere vCenter Linked Mode.

  L'article CTX131239 contient des informations sur la version actuelle, ainsi que des liens vers les problèmes connus.

  Pour plus d'informations, voir Environnements de virtualisation VMware.

Hôtes cloud publics pris en charge :

- **Amazon Web Services (AWS)**

  Pour plus d'informations sur l'utilisation d'AWS pour provisionner des machines virtuelles, consultez Environnements de virtualisation Amazon Web Services.

- **Google Cloud Platform**
  Pour plus d'informations, voir Environnements de virtualisation Google Cloud Platform et Getting Started with Citrix DaaS on Google Cloud.

- **Microsoft Azure Resource Manager**

  Pour plus d'informations sur l'utilisation de Microsoft Azure Resource Manager pour provisionner des machines virtuelles, consultez Environnements de virtualisation Microsoft Azure Resource Manager.

- **Solutions partenaires et cloud Nutanix**

  Pour plus d'informations sur l'utilisation des solutions cloud et partenaires Nutanix, consultez Solutions cloud et partenaires Nutanix.

- **Solutions VMware Cloud et partenaires**

  Pour plus d'informations sur l'utilisation des solutions cloud et partenaires VMware, consultez Solutions cloud et partenaires VMware.

Lorsque vous ajoutez des connexions hôtes de cloud public à votre déploiement, tenez compte des points suivants :

- Vous avez besoin d'une licence de droits hybrides. Pour plus d'informations sur la licence de droits hybrides, consultez Transition et échange (TTU) avec droits hybrides. Pour plus d'informations sur l'ajout d'une licence, consultez Créer un site.
- Les sources d'informations vous dirigent vers la documentation Citrix DaaS. Si vous connaissez les hôtes de cloud public du produit Citrix DaaS, veuillez noter que la version sur site présente plusieurs différences.
  - Dans Citrix DaaS, l'interface de gestion est appelée Configuration complète. Dans Citrix Virtual Apps and Desktops sur site, l'interface de gestion est appelée Web Studio.
  - Les mises à jour sont déployées sur Citrix DaaS environ toutes les quatre semaines. Par conséquent, vous pourrez constater que certaines fonctionnalités disponibles avec Citrix DaaS ne sont pas disponibles avec la version sur site.

Niveaux fonctionnels Active Directory

Les niveaux fonctionnels de la forêt et du domaine Active Directory sont pris en charge :

- Windows Server 2016
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

HDX

Audio

L'audio UDP pour Multi-Stream ICA est pris en charge sur l'application Citrix Workspace pour Windows et l'application Citrix Workspace pour Linux 13.

L'annulation de l'écho est prise en charge sur l'application Citrix Workspace pour Windows.

Consultez la prise en charge et la configuration requise pour chaque fonctionnalité HDX spécifique. Pour plus d'informations sur les fonctionnalités HDX et les applications Citrix Workspace, voir le tableau des fonctionnalités.

Mise à disposition Windows Media HDX

Les clients suivants sont pris en charge pour la récupération de contenu côté client Windows Media, la redirection Windows Media, le transcodage multimédia en temps réel de Windows Media : application Citrix Workspace pour Windows, application Citrix Workspace pour iOS et application Citrix Workspace pour Linux.

Pour utiliser la récupération de contenu côté client Windows Media sur des machines Windows 8, définissez Citrix Multimedia Redirector comme programme par défaut : dans **Panneau de configuration > Programmes > Programmes par défaut > Choisir les programmes par défaut**, sélectionnez **Citrix Multimedia Redirector** et cliquez sur **Définir ce programme comme programme par défaut** ou **Choisir les paramètres par défaut pour ce programme**. Un transcodage GPU requiert un processeur graphique compatible NVIDIA CUDA avec Compute Capability 1.1 ou version ultérieure ; voir https://developer.nvidia.com/cuda/cuda-gpus.

HDX 3D Pro

Le VDA pour OS mono-session Windows détecte la présence de matériel GPU au moment de l'exécution.

La machine physique ou virtuelle qui héberge l'application peut utiliser la fonctionnalité GPU Passthrough de traitement graphique (GPU) ou virtuel (vGPU) :

- GPU Passthrough est disponible avec :
  - XenServer
  - Nutanix AHV
  - VMware vSphere et VMware ESX, où il est appelé accélération graphique virtuelle (vDGA)
  - Microsoft Hyper-V dans Windows Server 2016 où il est appelé attribution discrète de périphériques (DDA)

- vGPU est disponible avec :
  - XenServer
  - Nutanix AHV
  - VMware vSphere

Voir https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/2402-ltsr/graphics/hdx-3d-pro.

Citrix recommande que l'ordinateur hôte dispose au minimum de 4 Go de mémoire vive et d'une UC à quadruple cœur offrant une vitesse d'horloge de 2,3 GHz ou plus.

Unité de traitement graphique (GPU) :

- Pour une accélération graphique virtualisée à l'aide de l'API NVIDIA GRID, vous pouvez utiliser HDX 3D Pro avec tous les GPU NVIDIA GRID pris en charge par la version 13 et ultérieure du logiciel NVIDIA Virtual GPU (vGPU), voir https://docs.nvidia.com/grid/index.html.
  Pour obtenir une liste détaillée des hyperviseurs et du matériel pris en charge, consultez la documentation logiciel NVIDIA vGPU.
- L'accélération graphique virtualisée est prise en charge sur la gamme E3 d'Intel Xeon Processor de plates-formes graphiques pour centres de données et sur la série Flex de GPU pour centres de données d'Intel. Pour en savoir plus, consultez la série GPU Flex.
- Les GPU AMD sont compatibles avec la virtualisation MxGPU d'AMD. Pour en savoir plus sur le matériel pris en charge, consultez la documentation AMD.

Machine utilisateur :

- Citrix prend en charge jusqu'à 8 écrans 4K, en fonction des ressources matérielles. Selon le GPU utilisé, d'autres restrictions matérielles peuvent s'appliquer à ce plafond.
- Citrix recommande que les machines utilisateur disposent d'au moins 4 Go de RAM et d'une UC avec une vitesse d'horloge de 1,6 GHz ou plus. Pour des performances optimales, nous recommandons que les machines utilisateur disposent d'au moins 8 Go de RAM et d'une UC avec une vitesse d'horloge de 3 GHz ou plus.
- Pour accéder à plusieurs moniteurs, Citrix recommande que les machines utilisateur soient équipées d'UC quadruple cœur.
- L'application Citrix Workspace doit être installée.

Pour de plus amples informations, consultez les articles HDX 3D Pro et www.citrix.com/xenapp/3d.

Serveur d'impression universelle

Le serveur d'impression universelle comprend les composants client et serveur. Le composant UpsClient est inclus dans l'installation du VDA. Vous installez le composant UpsServer sur chaque serveur

d'impression où les imprimantes partagées résident que vous souhaitez provisionner avec le pilote d'impression universelle Citrix dans les sessions utilisateur.

Le composant UpsServer est pris en charge sur :

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Exigences :

- Microsoft Visual C++ 2015–2019 Redistributable
- Microsoft .NET Framework 4.8 (minimum)

Pour les VDA pour OS multi-session Windows, l'authentification de l'utilisateur lors des opérations d'impression nécessite que le Serveur d'impression universelle appartienne au même domaine que le VDA.

Des packs de composants client et serveur autonomes peuvent également être téléchargés.

Pour de plus amples informations, consultez la section Provisionner des imprimantes.

Autre

Seuls les serveurs de licences Citrix 11.17.2 et versions ultérieures sont pris en charge. Pour plus d'informations, consultez l'article Licences.

Consultez la matrice des produits pour plus d'informations sur la compatibilité des versions.

Pour connaître les versions StoreFront prises en charge, consultez la configuration système requise pour StoreFront.

La console de gestion des stratégies de groupe de Microsoft (GPMC) est nécessaire si vous stockez les informations de stratégie Citrix dans Active Directory au lieu de la base de données de configuration de site. Si vous installez `CitrixGroupPolicyManagement_x64.msi` séparément (par exemple, sur une machine sur laquelle n'est pas installé de composant principal Citrix Virtual Apps and Desktops), Visual Studio 2015 Runtime doit être installé sur cette machine. Pour de plus amples informations, consultez la documentation de Microsoft.

Si vous souhaitez modifier les objets de stratégie de groupe de domaine à l'aide de la console de gestion des stratégies de groupe, activez la fonctionnalité Gestion des stratégies de groupe (dans le Gestionnaire Windows Server) sur toutes les machines contenant des Delivery Controller.

Plusieurs cartes réseau sont prises en charge.

Par défaut, l'application Citrix Workspace pour Windows n'est pas installée lorsque vous installez un VDA de version courante. Pour plus d'informations, consultez la documentation de l'application Citrix Workspace pour Windows.

Consultez la section Local App Access pour des informations sur les navigateurs pris en charge pour cette fonctionnalité.

Cette version de Citrix Virtual Apps and Desktops nécessite HDX RealTime Connector 2.9 LTSR comme version minimale. Pour en savoir plus, consultez la documentation HDX RealTime Optimization Pack.

Ce produit prend en charge les versions 3 à 5 de PowerShell.

Vue d'ensemble technique

June 27, 2024

Citrix Virtual Apps and Desktops sont des solutions de virtualisation qui fournissent au personnel informatique un contrôle des machines virtuelles, des applications, des licences et de la sécurité tout en offrant un accès à n'importe quel périphérique.

Les solutions Citrix Virtual Apps and Desktops permettent :

- Aux utilisateurs d'exécuter des applications et des bureaux indépendamment du système d'exploitation et de l'interface de le périphérique.
- Aux administrateurs de gérer le réseau et contrôler l'accès à partir de périphériques sélectionnés ou depuis tous les périphériques.
- Aux administrateurs de gérer l'ensemble d'un réseau à partir d'un centre de données unique.

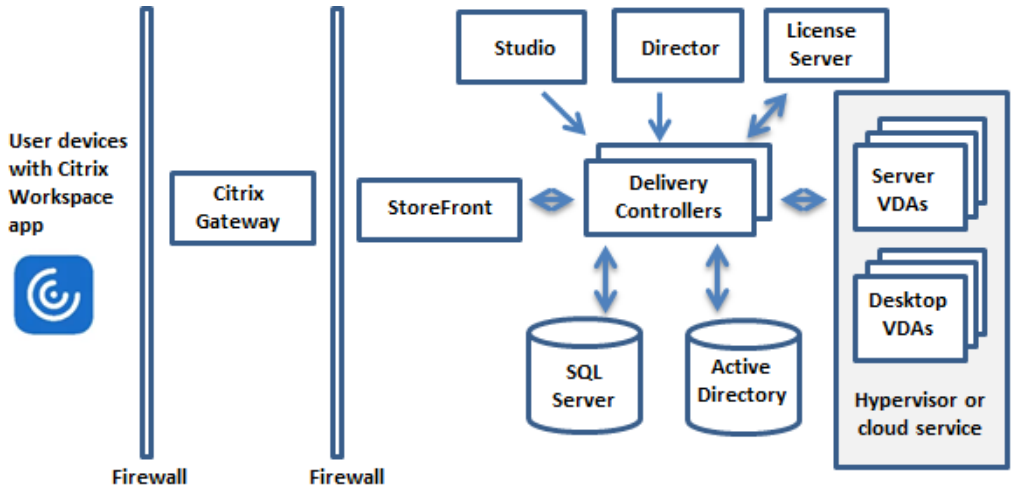
Citrix Virtual Apps and Desktops partagent une architecture unifiée appelée FlexCast Management Architecture (FMA). Les fonctionnalités clé de FMA comprennent la possibilité d'exécuter plusieurs versions de Citrix Virtual Apps ou Citrix Virtual Desktops à partir d'un site unique et un provisioning intégré.

En savoir plus sur les changements de nom de produit.

Composants principaux

Cet article est très utile si vous découvrez Citrix Virtual Apps and Desktops.

Cette illustration affiche les composants principaux d'un déploiement typique, qui est appelé un site.



Delivery Controller

Delivery Controller est le composant de gestion centralisée d'un site. Chaque site possède un ou plusieurs Delivery Controller. Il est installé sur au moins un serveur dans le centre de données. Pour la fiabilité et la disponibilité du site, installez des Controller sur plusieurs serveurs. Si votre déploiement inclut un hyperviseur ou un autre service, les services de Controller communiquent avec lui pour :

- Distribuer des applications et bureaux
- Authentifier et gérer l'accès des utilisateurs
- Établir les connexions entre les utilisateurs et leurs applications et bureaux
- Optimiser les connexions utilisateur
- Équilibrer la charge des connexions

Le service broker du Controller contrôle quels utilisateurs sont connectés et depuis quel endroit, quelles ressources de session les utilisateurs possèdent-ils et si les utilisateurs doivent se reconnecter aux applications existantes. Le service broker exécute des applets de commande PowerShell et communique avec l'agent broker situé sur les VDA via le port TCP 80. Il n'est pas possible d'utiliser le port TCP 443.

Monitor Service collecte les données historiques et les place dans la base de données de contrôle. Ce service utilise le port TCP 80 ou 443.

Les données provenant des services Controller sont stockées dans la base de données du site.

Le Controller gère l'état des bureaux, les démarre ou les arrête à la demande et en fonction de la configuration de l'administration.

Base de données

Au moins une base de données Microsoft SQL Server est requise pour chaque site pour stocker toutes les informations de configuration et de session. Cette base de données stocke les données collectées et gérés par les services qui constituent le Controller. Installez la base de données dans votre centre de données et assurez-vous qu'elle possède une connexion permanente au Controller.

Le site utilise également une base de données de journalisation de la configuration et une base de données de contrôle. Par défaut, ces bases de données sont installées dans le même emplacement que la base de données du site, mais vous pouvez modifier ce paramètre.

Virtual Delivery Agent (VDA)

Le VDA est installé sur chaque machine physique ou virtuelle de votre site que vous mettez à disposition des utilisateurs. Ces machines fournissent des applications ou des postes de travail. Le VDA permet aux machines de s'enregistrer auprès du Controller, qui permet à la machine et aux ressources qu'elle héberge d'être mise à la disposition des utilisateurs. Les VDA établissent et gèrent la connexion entre la machine et le périphérique de l'utilisateur. Les VDA vérifient également qu'une licence Citrix est disponible pour l'utilisateur ou la session et appliquent les stratégies configurées pour la session.

Le VDA communique des informations de session au service Broker dans le Controller via l'agent Broker dans le VDA. L'agent broker héberge de multiples plug-ins et collecte des données en temps réel. Il communique avec le Controller sur le port TCP 80.

Le mot « VDA » est souvent utilisé pour faire référence à l'agent ainsi qu'à la machine sur laquelle il est installé.

Les VDA sont disponibles pour les systèmes d'exploitation Windows mono-session et multi-session. Les VDA pour les systèmes d'exploitation multi-session Windows autorisent plusieurs utilisateurs à se connecter au serveur à un moment donné. Les VDA pour les systèmes d'exploitation mono-session Windows ne permettent qu'à un seul utilisateur de se connecter au bureau à la fois. Les VDA Linux sont également disponibles.

Citrix StoreFront

StoreFront authentifie les utilisateurs et gère les magasins de bureaux et d'applications auxquels les utilisateurs accèdent. Il peut héberger votre magasin d'applications d'entreprise qui fournit aux utilisateurs un accès en libre-service aux bureaux et aux applications que vous mettez à leur disposition. Il assure également le suivi des abonnements aux applications des utilisateurs, des noms de raccourcis et d'autres données. Cela permet de garantir que les utilisateurs ont une expérience cohérente sur plusieurs périphériques.

Application Citrix Workspace

Installée sur les machines utilisateur et autres points de terminaison, tels que les bureaux virtuels, l'application Citrix Workspace offre aux utilisateurs un accès en libre-service, rapide et sécurisé aux documents, applications et bureaux. L'application Citrix Workspace offre également un accès à la demande aux applications Windows, Web et SaaS (Software as a Service). Pour les périphériques qui ne peuvent pas installer le logiciel de l'application Citrix Workspace spécifique au périphérique, l'application Citrix Workspace pour HTML5 offre une connexion via un navigateur Web compatible HTML5.

Studio

Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). La documentation de ce produit ne couvre que Web Studio. Pour plus d'informations sur Citrix Studio, consultez Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Studio Web Web Studio est une console de gestion Web qui vous permet de configurer et de gérer votre déploiement Citrix Virtual Apps and Desktops sur site. Il est conçu pour améliorer l'expérience utilisateur et répond généralement plus rapidement que Citrix Studio, la console de gestion basée sur Windows. Reportez-vous à la section Installer Web Studio.

Citrix Studio Citrix Studio est la console de gestion où vous configurez et gérez votre déploiement Citrix Virtual Apps and Desktops. Citrix Studio élimine le besoin de consoles de gestion distinctes pour gérer la mise à disposition des applications et des postes de travail. Citrix Studio offre des assistants pour vous guider dans le processus de configuration de votre environnement, créer des charges de travail pour héberger les applications et bureaux, et attribuer des applications et des bureaux aux utilisateurs. Vous pouvez également utiliser Studio pour allouer et suivre les licences Citrix pour votre site.

Citrix Studio obtient les informations qu'il affiche à partir du Broker Service dans le Controller, communiquant via le port TCP 80.

Secure Private Access

La solution Citrix Secure Private Access locale améliore la posture globale de sécurité et de conformité d'une organisation en permettant de fournir facilement un accès réseau Zero Trust aux applications basées sur un navigateur (applications Web internes et applications SaaS) en utilisant StoreFront comme portail d'accès unifié aux applications Web et SaaS, ainsi qu'aux applications et bureaux virtuels intégrés à Citrix Workspace. La solution est compatible avec les versions existantes de

NetScaler et StoreFront sans aucune modification des versions. Pour plus de détails, consultez la section Citrix Secure Private Access pour les applications locales.

Citrix Director

Director est un outil Web qui permet aux équipes d'assistance informatique de surveiller un environnement, de résoudre les problèmes avant qu'ils ne deviennent critiques et de réaliser des tâches d'assistance pour les utilisateurs finaux. Vous pouvez utiliser un déploiement de Director pour vous connecter à et contrôler plusieurs sites Citrix Virtual Apps ou Citrix Virtual Desktops.

Director affiche les éléments suivants :

- Données de session en temps réel à partir du Broker Service dans le Controller, qui comprennent des données que le service Broker obtient depuis l'agent broker dans le VDA.
- Données de site historiques provenant de Monitor Service dans le Controller.

Director utilise les données de performances et heuristiques ICA capturées par le périphérique Citrix Gateway pour créer des analyses à partir des données, puis les présenter aux administrateurs.

Vous pouvez également afficher et interagir avec les sessions d'un utilisateur via Director, à l'aide de l'Assistance à distance Windows.

Serveur de licences Citrix

Le serveur de licences gère les licences de vos produits Citrix. Il communique avec le Controller pour gérer les licences pour chaque session utilisateur et avec Studio pour allouer les fichiers de licences. Un site doit avoir au moins un serveur de licences pour stocker et gérer vos fichiers de licences.

Hyperviseur ou autre service

L'hyperviseur ou autre service héberge les machines virtuelles de votre site. Il peut s'agir des machines virtuelles que vous utilisez pour héberger les applications et les bureaux, ainsi que les machines virtuelles que vous utilisez pour héberger les composants de Citrix Virtual Apps and Desktops. Un hyperviseur est installé sur un ordinateur hôte entièrement dédié à l'exécution de l'hyperviseur et l'hébergement des machines virtuelles.

Les solutions Citrix Virtual Apps and Desktops prennent en charge divers hyperviseurs et services.

Bien que de nombreux déploiements requièrent un hyperviseur, vous n'en avez pas besoin pour fournir un accès PC distant. De même, un hyperviseur n'est pas requis lorsque vous utilisez Provisioning Services (PVS) pour provisionner des machines virtuelles.

Composants supplémentaires

Les composants suivants peuvent également être inclus dans les déploiements Citrix Virtual Apps and Desktops. Pour de plus amples informations, consultez leur documentation respective.

Citrix Provisioning

Citrix Provisioning (anciennement Provisioning Services) est un composant facultatif disponible avec certaines éditions. Il offre une alternative à MCS pour le provisioning des machines virtuelles. Alors que MCS permet de créer des copies d'une image principale, PVS livre l'image principale en streaming vers les machines utilisateur. PVS ne nécessite pas d'hyperviseur pour effectuer cette opération, vous pouvez donc l'utiliser pour héberger des machines physiques. PVS communique avec le Controller afin de fournir aux utilisateurs des ressources.

Citrix Gateway

Lorsque les utilisateurs se connectent en dehors du pare-feu d'entreprise, Citrix Virtual Apps and Desktops peut utiliser la technologie Citrix Gateway (anciennement Access Gateway et NetScaler Gateway) pour sécuriser les connexions avec le protocole TLS. L'appliance virtuelle Citrix Gateway ou VPX est une appliance SSL VPN déployée dans la zone démilitarisée (DMZ). Il fournit un point d'accès sécurisé unique via le pare-feu d'entreprise.

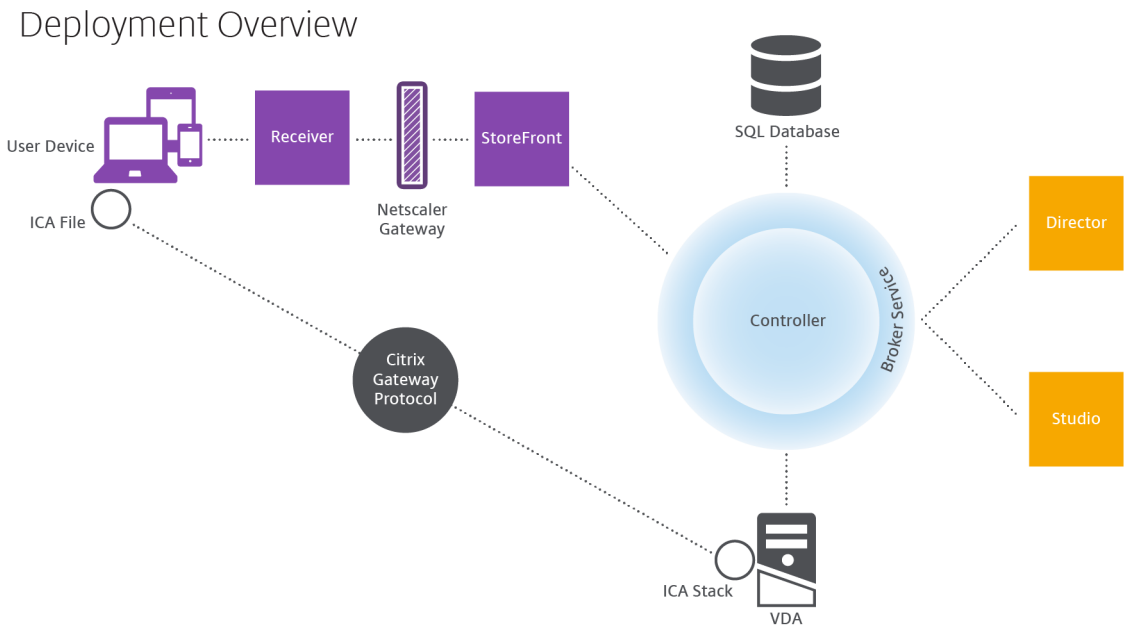
Citrix SD-WAN

Dans les déploiements dans lesquels des bureaux virtuels sont mis à disposition auprès des utilisateurs dans des emplacements distants, des succursales par exemple, la technologie Citrix SD-WAN peut être utilisée pour optimiser les performances. Les répéteurs accélèrent les performances sur les réseaux WAN. Avec les répéteurs, les utilisateurs des succursales bénéficient des performances d'un réseau local sur le réseau étendu. Citrix SD-WAN permet de définir des priorités dans l'expérience des utilisateurs, par exemple pour éviter une dégradation des performances au niveau de la succursale en cas d'envoi de fichiers volumineux ou de tâches d'impression importantes sur le réseau. L'optimisation WAN HDX assure une compression avec système de jetons et déduplication des données, réduisant considérablement les besoins en bande passante tout en améliorant les performances.

Comment fonctionnent les déploiements typiques

Un site est composé de machines avec des rôles dédiés qui permettent de garantir une certaine évolutivité, une haute disponibilité, la capacité de basculement, et fournir une solution qui est sécurisé

par nature. Un site comprend des serveurs et des machines de bureau installés sur un VDA, ainsi que le Delivery Controller, qui gère l'accès.



Le VDA permet aux utilisateurs de se connecter à des bureaux et des applications. Il est installé sur des machines virtuelles dans le centre de données pour la plupart des méthodes de mise à disposition, mais il peut également être installé sur des ordinateurs physiques pour Remote PC Access.

Le Controller est constitué de services Windows indépendants qui permettent de gérer les ressources, les applications et les bureaux, et optimiser et équilibrer les connexions utilisateur. Chaque site possède un ou plusieurs Delivery Controller. Étant donné que les sessions sont affectées par la latence, de la bande passante et de fiabilité du réseau, placez tous les Controller sur le même réseau local, si possible.

Les utilisateurs n'accèdent jamais directement au Controller. Le VDA est utilisé en tant que intermédiaire entre les utilisateurs et le Controller. Lorsque les utilisateurs se connectent à l'aide de StoreFront, leurs informations d'identification sont transmises au service Broker sur le Controller. Le service Broker obtient ensuite les profils et les ressources disponibles en fonction des stratégies définies.

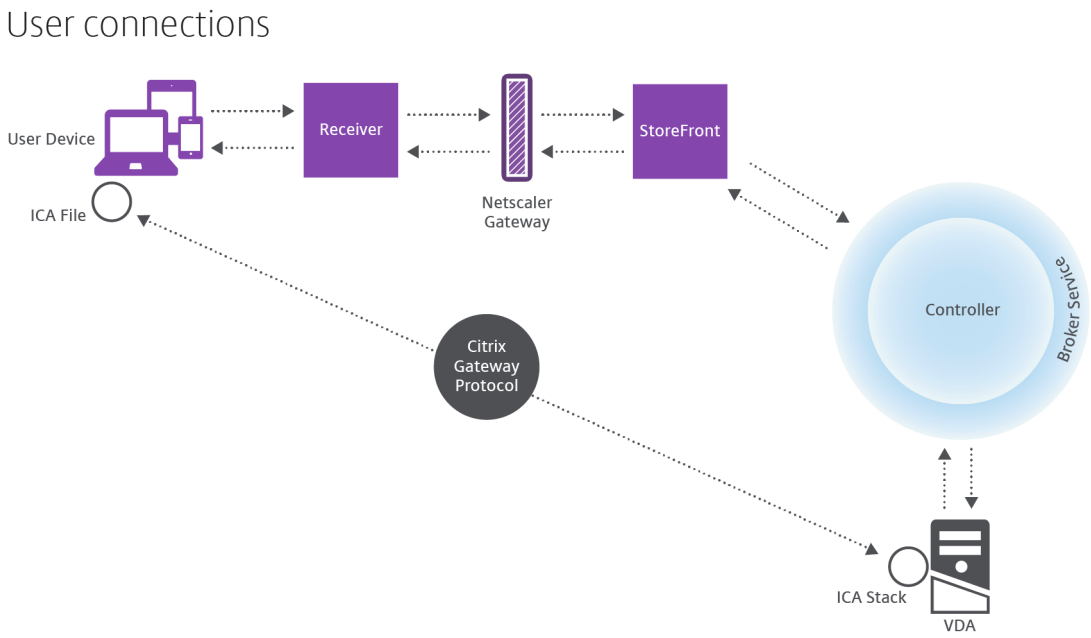
Comment sont traitées les connexions utilisateur

Pour démarrer une session, l'utilisateur se connecte, soit via application Citrix Workspace installé sur la machine utilisateur, soit par le biais d'un site Web StoreFront.

L'utilisateur sélectionne les bureaux virtuels ou physiques ou l'application virtuelle nécessaire(s).

Les informations d'identification de l'utilisateur passent par le biais de cette piste pour accéder au Controller, qui détermine quelles ressources sont nécessaires à la communication avec un service

Broker. Citrix recommande aux administrateurs de placer un certificat SSL sur StoreFront pour chiffrer les informations d'identification provenant de l'application Citrix Workspace.



Le Service Broker détermine la nature des bureaux et des applications que l'utilisateur est autorisé à accéder.

Une fois les informations d'identification vérifiées, les informations sur les applications ou les bureaux disponibles sont envoyées à l'utilisateur au travers de la piste StoreFront-application Citrix Workspace. Lorsque l'utilisateur sélectionne des applications ou des bureaux depuis cette liste, ces informations retournent à la piste vers le Delivery Controller. Le Controller détermine ensuite le VDA approprié pour héberger les applications ou le bureau spécifiques.

Le Controller envoie un message au VDA avec les informations d'identification de l'utilisateur et envoie toutes les données à propos de l'utilisateur et de la connexion au VDA. Le VDA accepte la connexion et renvoie les informations vers les mêmes pistes jusqu'à l'application Citrix Workspace. Un ensemble de paramètres requis est collecté sur StoreFront. Ces paramètres sont ensuite envoyés à l'application Citrix Workspace, soit dans le cadre de la conversation de protocole entre l'application Citrix Workspace et StoreFront, ou convertis en fichier ICA (Independent Computing Architecture) et téléchargés. Tant que le site a été correctement configuré, les informations d'identification sont chiffrées dans ce processus.

Le fichier ICA est copié vers la machine de l'utilisateur et établit une connexion directe entre le périphérique et la pile ICA en cours d'exécution sur le VDA. Cette connexion ignore l'infrastructure de gestion (application Citrix Workspace, StoreFront et Controller).

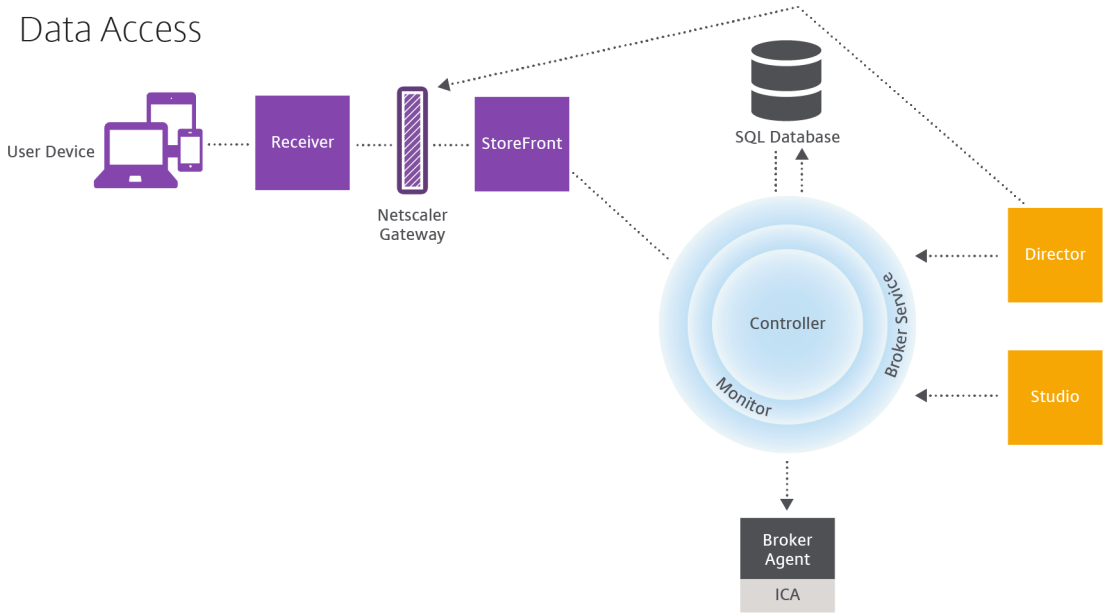
La connexion entre l'application Citrix Workspace et le VDA utilise Citrix Gateway Protocol (CGP). Si une connexion est interrompue, la fonction de fiabilité de session permet à l'utilisateur de se recon-

necter au VDA plutôt que d'avoir à redémarrer via l'infrastructure de gestion. La fiabilité de session peut être activée ou désactivée à l'aide de stratégies Citrix.

Une fois que le client est connecté au VDA, le VDA notifie le Controller que l'utilisateur est connecté. Le Controller envoie ensuite ces informations à la base de données du site et commence à enregistrer les données dans la base de données de surveillance.

Comment fonctionne l'accès aux données

Chaque session Citrix Virtual Apps and Desktops génère des données auxquelles le service informatique peut accéder au travers de Studio ou Director. Studio permet aux administrateurs d'accéder à des données en temps réel à partir de l'agent Broker afin de gérer les sites. Director accède aux mêmes données et aux données historiques stockées dans la base de données de surveillance. Il accède également aux données HDX de NetScaler Gateway pour le support et le dépannage du service d'assistance.



Dans le Controller, le service Broker signale des données de session pour chaque session sur la machine fournissant des données en temps réel. Le service de surveillance (Monitor) suit également les données en temps réel et les stocke en tant que données d'historique dans la base de données de surveillance.

Studio communique uniquement avec le service Broker. Il n'accède qu'aux données en temps réel. Director communique avec le service Broker (via un plug-in dans l'agent Broker) pour accéder à la base de données du site.

Director peut également accéder à Citrix Gateway pour obtenir des informations sur les données

HDX.

Mise à disposition d'applications et de bureaux

Vous configurez les machines qui mettent à disposition les applications et les bureaux avec des catalogues de machines. Ensuite, vous créez des groupes de mise à disposition qui spécifient les applications et bureaux qui seront disponibles (à l'aide des machines des catalogues), et les utilisateurs qui peuvent y accéder. Vous pouvez également créer des groupes d'applications pour gérer des collections d'applications.

Catalogues de machines

Les catalogues de machines sont des collections de machines physiques ou virtuelles que vous gérez comme une seule entité. Ces machines, et les applications ou les bureaux virtuels sur celles-ci, sont les ressources que vous mettez à la disposition de vos utilisateurs. Toutes les machines d'un catalogue ont le même système d'exploitation et VDA installé. Elles possèdent également les mêmes applications ou bureaux virtuels.

En général, vous pouvez créer une image principale et l'utiliser pour créer les mêmes machines virtuelles dans le catalogue. Pour les VM, vous pouvez spécifier la méthode de provisioning pour les machines de ce catalogue : outils Citrix (Citrix Provisioning ou MCS) ou autres outils. Vous pouvez également utiliser vos propres images existantes. Dans ce cas, vous devez gérer les machines cibles individuellement ou collectivement à l'aide d'outils de distribution logiciel électronique tiers (ESD).

Les types de machines valides sont les suivants :

- **OS multi-session :** machines virtuelles ou physiques avec un système d'exploitation multi-session. Utilisé pour mettre à disposition des applications publiées Citrix Virtual Apps (également appelées applications hébergées sur un serveur) et les bureaux publiés Citrix Virtual Desktops (également appelés bureaux hébergés sur un serveur). Ces machines autorisent plusieurs utilisateurs à se connecter à un moment donné.
- **Système d'exploitation mono-session :** machines virtuelles ou physiques dotées d'un système d'exploitation mono-session. Utilisé pour fournir des postes de travail VDI (postes de travail exécutant des systèmes d'exploitation mono-session pouvant être personnalisés), des applications hébergées sur machine virtuelle (applications sur des systèmes d'exploitation mono-session) et des postes de travail physiques hébergés. Un seul utilisateur à la fois peut se connecter à chacun de ces bureaux.
- **Remote PC Access :** permet aux utilisateurs distants d'accéder à leurs ordinateurs de bureau physiques à partir de tout périphérique exécutant l'application Citrix Workspace. Les ordina-

teurs de bureau sont gérés via le déploiement Citrix Virtual Desktops et nécessitent que les machines utilisateur soient spécifiées dans une liste de blocage.

Pour plus d'informations, consultez Gestion des images Citrix Virtual Apps and Desktopset Créer des catalogues de machines.

Groupes de mise à disposition

Les groupes de mise à disposition spécifient quels utilisateurs ont accès à quelles applications et/ou quels bureaux sur quelles machines. Les groupes de mise à disposition contiennent les machines de vos catalogues de machines et les utilisateurs Active Directory qui ont accès à votre site. Vous pouvez attribuer des utilisateurs à vos groupes de mise à disposition en fonction de leur groupe Active Directory, car les groupes Active Directory et les groupes de mise à disposition représentent des modes de regroupement des utilisateurs ayant les mêmes spécifications.

Chaque groupe de mise à disposition peut contenir des machines provenant de plusieurs catalogues de machines et chaque catalogue peut contribuer des machines à plus d'un groupe de mise à disposition. Toutefois, une machine individuelle peut appartenir à un seul groupe de mise à disposition à la fois.

Vous définissez les ressources auxquelles les utilisateurs dans le groupe de mise à disposition peuvent accéder. Par exemple, pour mettre à disposition des applications différentes pour différents utilisateurs, vous pouvez installer toutes les applications sur l'image principale pour un catalogue et créer suffisamment de machines dans ce catalogue à répartir sur plusieurs groupes de mise à disposition. Vous pouvez ensuite configurer chaque groupe de mise à disposition pour fournir un sous-ensemble différent d'applications installées sur les machines.

Pour plus d'informations, consultez la section Créer des groupes de mise à disposition.

Groupes d'applications

Comparativement à l'utilisation d'un plus grand nombre de groupes de mise à disposition, les groupes d'applications permettent de gérer les applications et de contrôler les ressources : Avec les restrictions de balise, vous pouvez utiliser des machines existantes pour plusieurs tâches de publication, éliminant ainsi les coûts associés avec le déploiement et la gestion de machines supplémentaires. L'utilisation d'une restriction de balise équivaut à diviser (ou partitionner) des machines dans un groupe de mise à disposition. Les groupes d'applications peuvent également être utiles pour isoler et dépanner un sous-ensemble de machines dans un groupe de mise à disposition.

Pour de plus amples informations, consultez l'article Créer des groupes d'applications.

Informations supplémentaires

- Diagrammes Citrix Virtual Apps and Desktops
- Ports réseau
- Bases de données
- Hyperviseurs et autres services pris en charge

Base de données

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Un site Citrix Virtual Apps ou Citrix Virtual Desktops Site utilise trois bases de données SQL Server :

- **Site :** (également appelé Configuration de site) stocke les données de configuration du site, ainsi que les informations sur l'état de la session et la connexion.
- **Journalisation :** (également appelée Journalisation de la configuration) stocke des informations sur les modifications apportées à la configuration du site et les activités administratives. Cette base de données est utilisée lorsque la fonction Journalisation de la configuration est activée (valeur par défaut=activée).
- **Contrôle :** stocke les données utilisées par Director, telles que les informations de session et de connexion.

Chaque Delivery Controller communique directement avec la base de données du site. L'authentification Windows est requise entre le Controller et les bases de données. Il est possible de déconnecter un Controller ou de le mettre hors tension sans affecter les autres Controller du site. L'unique point de défaillance reste par conséquent la base de données. Si le serveur de base de données échoue, les connexions existantes continuent de fonctionner jusqu'à ce que l'utilisateur ferme sa session ou se déconnecte. Pour plus d'informations sur le comportement de la connexion lorsque la base de données de site devient indisponible, consultez la section Cache d'hôte Local.

Citrix recommande les actions suivantes en ce qui concerne les bases de données :

- **Sauvegardez régulièrement.** Sauvegardez régulièrement les bases de données afin de pouvoir les restaurer en cas de défaillance du serveur de base de données. La stratégie de sauve-

garde pour chaque base de données peut différer. Pour plus d'informations, consultez l'article CTX135207. Notez toutefois qu'il fait référence à CitrixXenDesktopDB, qui n'est plus pris en charge ni disponible pour les clients.

- **Sauvegardez et restaurez régulièrement les bases de données SQL Server de site, de surveillance et de journalisation.** Pour des informations spécifiques sur les bases de données SQL Server, consultez Création de sauvegardes différentielles et complètes d'une base de données SQL Server.

Si votre site contient plus d'une zone, assurez-vous que la zone principale contient toujours la base de données du site. Les Controller de chaque zone communiquent avec cette base de données.

Haute disponibilité

Il existe trois solutions de haute disponibilité à considérer pour garantir le basculement automatique :

- **Groupes de disponibilité AlwaysOn (y compris les groupes de disponibilité de base) :** cette solution à haute disponibilité et reprise après sinistre introduite dans SQL Server 2012 vous permet d'optimiser la disponibilité pour une ou plusieurs bases de données. Les Groupes de disponibilité AlwaysOn nécessitent que les instances SQL Server résident les nœuds WSFC (Windows Server Failover Clustering). Pour plus d'informations, consultez la section Clustering de basculement Windows Server avec SQL Server.
- **Mise en miroir de la base de données SQL Server :** la mise en miroir de la base de données garantit qu'en cas d'indisponibilité soudaine du serveur de base de données actif, le basculement automatique se produit au bout de quelques secondes seulement, évitant généralement toute gêne pour les utilisateurs. Cette méthode est plus coûteuse que les autres solutions car des licences complètes de SQL Server sont requises sur chaque serveur de base de données. Vous ne pouvez pas utiliser l'édition SQL Server Express dans un environnement de mise en miroir.
- **Mise en cluster SQL :** la technologie de mise en cluster SQL de Microsoft peut être utilisée pour permettre à un serveur d'assurer automatiquement la reprise des tâches et des responsabilités d'un autre serveur défaillant. Toutefois, cette solution est plus complexe à mettre en place et le basculement automatique est généralement plus lent qu'avec les autres méthodes, comme la mise en miroir SQL.
- **À l'aide des fonctionnalités de haute disponibilité de l'hyperviseur :** avec cette méthode, vous déployez la base de données en tant que machine virtuelle et utilisez les fonctionnalités de haute disponibilité de votre hyperviseur. Cette solution est moins coûteuse que la mise en miroir du fait qu'elle utilise votre logiciel d'hyperviseur et que vous pouvez également utiliser l'édition SQL Server Express. Cependant, le processus de basculement automatique est plus lent

car il faut un certain temps pour qu'une nouvelle machine démarre pour la base de données, avec le risque d'interrompre le service fourni aux utilisateurs.

La fonctionnalité Cache d'hôte local complète les meilleures pratiques de haute disponibilité de SQL Server. Le cache hôte local permet aux utilisateurs de se connecter et de se reconnecter aux applications et aux bureaux même lorsque la base de données de site n'est pas disponible. Pour plus d'informations, veuillez consulter la section Cache d'hôte local.

Si tous les Controller d'un site échouent, vous pouvez configurer les VDA pour fonctionner en mode haute disponibilité, qui permet aux utilisateurs de continuer à accéder à leurs bureaux et applications. En mode haute disponibilité, le VDA accepte des connexions ICA directes provenant des utilisateurs, plutôt que des connexions négociées par le Controller. Utilisez cette fonctionnalité uniquement dans les rares cas où la communication avec tous les Controllers échoue. Il ne s'agit pas d'une solution alternative aux autres solutions de haute disponibilité. Pour plus d'informations, veuillez consulter l'article CTX 127564.

L'installation d'un Controller sur un nœud dans une installation de mise en cluster SQL ou mise en miroir SQL n'est pas prise en charge.

Installer le logiciel de base de données

Par défaut, l'édition SQL Server Express est installée lorsque vous installez le premier Delivery Controller, si une autre instance SQL Server n'est pas détectée sur ce serveur. Cette mesure par défaut est généralement suffisante pour la preuve de concept ou pour les déploiements pilotes. Toutefois, SQL Server Express ne prend pas en charge les fonctionnalités de haute disponibilité de Microsoft.

L'installation par défaut utilise les comptes de service et autorisations Windows par défaut. Reportez-vous à la documentation Microsoft pour de plus amples informations sur ces défauts, y compris l'ajout de comptes de service Windows au rôle sysadmin. Le Controller utilise le compte de service réseau de cette configuration. Le Controller ne requiert aucun rôle ni autorisation SQL Server supplémentaire.

Le cas échéant, vous pouvez sélectionner **Masquer l'instance** pour l'instance de base de données. Lors de la configuration de l'adresse de la base de données dans Web Studio, entrez le numéro de port statique de l'instance plutôt que son nom. Reportez-vous à la documentation Microsoft pour de plus amples informations sur le masquage d'une instance du moteur de base de données SQL Server.

Pour la plupart des déploiements de production et tout déploiement utilisant les fonctionnalités de haute disponibilité Microsoft, nous vous recommandons d'utiliser uniquement les éditions non-Express prises en charge de SQL Server. Installez SQL Server sur des machines autres que le serveur sur lequel le premier Controller est installé. La section Configuration système requise répertorie les versions de SQL Server prises en charge. Les bases de données peuvent résider sur une ou plusieurs machines.

Assurez-vous que le logiciel SQL Server est installé avant de créer un site. Vous n'avez pas besoin de créer la base de données, mais si vous le faites, elle doit être vide. La configuration de technologies haute disponibilité de Microsoft est également recommandée.

Utilisez Windows Update pour conserver SQL Server à jour.

Configurer les bases de données à partir de l'assistant de création de site

Indiquez le nom et l'adresse des bases de données (emplacement) sur la page **Bases de données** dans l'assistant de création de site. (voir Formats d'adresse de base de données.) Pour éviter des erreurs lorsque Director interroge le service Monitor, n'utilisez pas d'espaces dans le nom de la base de données de contrôle.

La page **Bases de données** offre deux options pour configurer les bases de données : automatiquement et à l'aide de scripts. En général, vous pouvez utiliser l'option automatique si vous (utilisateur de Web Studio et administrateur de Citrix) disposez des privilèges de base de données requis. (voir Autorisations requises pour configurer les bases de données.)

Vous pouvez modifier l'emplacement des bases de données de journalisation de la configuration et de contrôle après la création du site. Voir Modifier l'emplacement des bases de données.

Pour configurer un site pour utiliser une base de données mise en miroir, effectuez les étapes suivantes, puis passez à la procédure de configuration automatique ou à l'aide d'un script.

1. Installez le logiciel SQL Server sur deux serveurs, A et B
2. Sur le serveur A, créez la base de données destinée à être utilisée comme base de données principale. Sauvegardez la base de données sur le serveur A, puis copiez-la sur le serveur B.
3. Sur le serveur B, restaurez le fichier de sauvegarde.
4. Démarrez la mise en miroir sur le serveur A.

Pour vérifier la mise en miroir après la création du site, exécutez le cmdlet PowerShell `get-configdbconnection` pour vous assurer que le partenaire de basculement a été défini dans la chaîne de connexion pour le miroir.

Si vous ajoutez, déplacez ou supprimez un Delivery Controller dans un environnement de base de données mise en miroir ultérieurement, consultez Delivery Controller.

Configuration automatique

Si vous disposez des privilèges de base de données requis, sélectionnez **Créer et configurer les bases de données à partir de Studio** sur la page **Bases de données** de l'assistant de création de site. Ensuite, indiquez les noms et adresses des bases de données principales.

Si une base de données existe sur une adresse spécifiée, elle doit être vide. Si les bases de données n'existent pas sur une adresse spécifiée, vous êtes informé qu'aucune base de données n'a été détectée, puis vous êtes invité à indiquer si vous souhaitez que la base de données soit créée pour vous. Lorsque vous confirmez, Web Studio crée automatiquement les bases de données, puis applique les scripts d'initialisation pour les bases de données principales et les copies.

Installation à l'aide de scripts

Si vous ne disposez pas des droits de base de données requis, demandez de l'aide à quelqu'un qui a ces droits, par exemple un administrateur de base de données. Voici la séquence :

1. Sur la page **Bases de données** de l'assistant de création de site, sélectionnez **Générer des scripts pour configurer manuellement**. Cette action génère les trois types de scripts suivants pour chacune des bases de données principales et réplica suivantes : bases de données de site, de surveillance et de journalisation.

   - *Script contenant « SysAdmin » dans son nom*. Script qui crée les bases de données et la connexion Delivery Controller. Ces tâches nécessitent des droits securityadmin.
   - *Script contenant « DbOwner » dans son nom*. Script qui crée les rôles utilisateur dans la base de données, ajoute les connexions, puis crée les schémas de base de données. Ces tâches requièrent des droits `db_owner`.
   - *Script contenant « Mixed » dans son nom*. Toutes les tâches dans un seul script, quels que soient les droits requis.

   Vous pouvez indiquer l'emplacement de stockage des scripts.

   > **Remarque :**
   >
   > Dans les environnements d'entreprise, la configuration de la base de données inclut des scripts qui doivent être gérés par différentes équipes ayant des rôles (droits) différents : `securityadmin` ou `db_owner`. Le cas échéant, les scripts « SysAdmin » sont d'abord exécutés par des administrateurs avec le rôle `securityadmin`, puis les scripts « DbOwner » sont exécutés par des administrateurs dotés de droits `db_owner`. Pour générer ces scripts, vous pouvez également utiliser PowerShell. Pour plus d'informations, voir Scripts de droits de base de données préférés.

2. Donnez ces scripts à votre administrateur de base de données. L'assistant de création de site s'arrête automatiquement à ce stade. Lorsque vous revenez plus tard, vous êtes invité à poursuivre la création du site.

L'administrateur de base de données crée alors les bases de données. Chaque base de données doit présenter les caractéristiques suivantes :

- Utilisez un classement qui se termine par `_CI_AS_KS`. Nous vous recommandons d'utiliser un classement qui se termine par `_100_CI_AS_KS`.
- Pour des performances optimales, activez l'option Capture instantanée Read Committed de SQL Server. Pour plus d'informations, veuillez consulter l'article CTX 137161.
- Fonctionnalités haute disponibilité configurées, le cas échéant.
- Pour configurer la mise en miroir, vous devez tout d'abord définir la base de données pour utiliser le modèle de récupération complet (le modèle simple est la valeur par défaut). Sauvegardez la base de données principale dans un fichier et copiez-la sur le serveur miroir. Ensuite, restaurez le fichier de sauvegarde sur le serveur miroir. Enfin, démarrez la mise en miroir sur le serveur principal.

L'administrateur de base de données utilise l'utilitaire de ligne de commande SQLCMD ou SQL Server Management Studio en mode SQLCMD pour :

- Exécuter chacun des scripts `xxx_Replica.sql` sur les instances de base de données SQL Server haute disponibilité (si la haute disponibilité est configurée)
- Exécuter chacun des scripts `xxx\\_Principal.sql` sur les instances de base de données SQL Server principales.

Consultez la documentation Microsoft sur SQLCMD pour plus de détails.

Lorsque tous les scripts sont terminés, l'administrateur de la base de données donne à l'administrateur Citrix les trois adresses de base de données principale.

Web Studio vous invite à poursuivre la création du site. Vous revenez à la page **Bases de données**. Entrez les adresses. Si l'un des serveurs hébergeant une base de données ne peut pas être contacté, un message d'erreur s'affiche.

Autorisations requises pour configurer les bases de données

Vous devez être un administrateur local et un utilisateur du domaine pour créer et initialiser les bases de données (ou modifier l'emplacement de la base de données). Vous devez également disposer de certaines autorisations SQL Server. Les autorisations suivantes peuvent être explicitement configurées ou acquises par l'appartenance à un groupe Active Directory. Si vos informations d'identification d'utilisateur Web Studio ne comprennent pas ces autorisations, vous êtes invité à entrer les informations d'identification d'utilisateur SQL Server.

Opération	Motif	Rôle de serveur	Rôle de base de données
Créer une base de données	Créer une base de données vide appropriée	`dbcreator`	
Créer un schéma	Créer tous les schémas spécifiques au service et ajouter le premier Controller au site	`securityadmin`*	`db_owner`
Ajouter un Controller	Ajouter un Controller (autre que le premier) au site	`securityadmin`*	`db_owner`
Ajouter un Controller (serveur miroir)	Ajouter une ouverture de session Controller au serveur de base de données assumant actuellement le rôle de miroir d'une base de données en miroir	`securityadmin`*	
Supprimer Controller	Supprimer le Controller du site	**	`db_owner`
Mettre à jour un schéma	Appliquer les mises à jour ou correctifs au schéma		`db_owner`

* Bien que techniquement plus restrictif, en pratique, vous pouvez traiter le rôle de serveur `securityadmin` comme équivalent au rôle de serveur `sysadmin`.

** Lorsqu'un Controller est supprimé d'un site, l'ouverture de session Controller sur le serveur de base de données n'est pas supprimée. Cela permet d'éviter de supprimer potentiellement une ouverture de session utilisée par des services autres que ce produit Citrix sur la même machine. L'ouverture de session doit être supprimée manuellement si elle n'est plus requise. Cette action nécessite l'appartenance au rôle de serveur `securityadmin`.

Lors de l'utilisation de Web Studio pour effectuer ces opérations, l'utilisateur Web Studio doit disposer d'un compte de serveur de base de données explicitement membre des rôles serveur appropriés, ou être en mesure de fournir les informations d'identification d'un compte qui est membre.

Scripts de droits de base de données préférés

Dans les environnements d'entreprise, la configuration de la base de données inclut des scripts qui doivent être gérés par différentes équipes ayant des rôles (droits) différents : `securityadmin` ou `db_owner`.

Avec PowerShell, vous pouvez spécifier les droits de base de données préférés. La spécification d'une valeur autre que celle par défaut entraîne la création de scripts distincts. Un script contient des tâches nécessitant le rôle `securityadmin`. L'autre script ne requiert que des droits `db_owner` et peut être exécuté par un administrateur Citrix sans avoir à contacter un administrateur de base de données.

Dans les applets de commande `get-*DBSchema`, l'option `-DatabaseRights` a les valeurs valides suivantes :

- `SA` : génère un script qui crée les bases de données et la connexion Delivery Controller. Ces tâches requièrent des droits `securityadmin`.
- `DBO` : génère un script qui crée les rôles utilisateur dans la base de données, ajoute les connexions, puis crée les schémas de base de données. Ces tâches requièrent des droits `db_owner`.
- `Mixed` : (valeur par défaut) toutes les tâches dans un seul script, quels que soient les droits requis.

Pour plus d'informations, consultez l'aide de l'applet de commande.

Formats d'adresse de base de données

Vous pouvez spécifier une adresse de base de données dans l'un des formats suivants :

- `ServerName`
- `ServerName\InstanceName`
- `ServerName,PortNumber`

Pour un groupe de disponibilité AlwaysOn, spécifiez l'écouteur du groupe dans le champ d'emplacement.

Modifier l'emplacement des bases de données

Après avoir créé un site, vous pouvez modifier l'emplacement des bases de données de journalisation de la configuration et de contrôle. (Vous ne pouvez pas modifier l'emplacement de la base de données du site.) Lorsque vous modifiez l'emplacement d'une base de données :

- Les données provenant de la base de données précédente ne sont pas importées vers la nouvelle base de données.

- Les journaux ne peuvent pas être regroupés pour les deux bases de données lors de la récupération des journaux.
- La première entrée du journal dans la nouvelle base de données indique qu'une modification a été apportée dans une base de données, mais elle n'identifie pas la base de données précédente.

Vous ne pouvez pas modifier l'emplacement de la base de données de journalisation de la configuration lorsque la journalisation obligatoire est activée.

Pour modifier l'emplacement d'une base de données :

1. Assurez-vous qu'une version prise en charge de Microsoft SQL Server est installée sur le serveur sur lequel vous souhaitez que la base de données réside. Configurez les fonctionnalités de haute disponibilité en fonction de vos besoins.
2. Connectez-vous à Web Studio, puis sélectionnez **Paramètres** dans le volet de gauche.
3. Localisez la vignette **Base de données** et sélectionnez **Modifier**.
4. Sur la page **Gérer la base de données**, sélectionnez la base de données pour laquelle vous souhaitez spécifier un nouvel emplacement, puis sélectionnez **Modifier la base de données** dans la barre d'actions.
5. Spécifiez le nouvel emplacement et le nom de la base de données.
6. Si vous souhaitez que Web Studio crée la base de données et que vous possédez les autorisations appropriées, cliquez sur **OK**. Lorsque vous y êtes invité, cliquez sur **Terminé** ; Web Studio crée la base de données automatiquement. Web Studio tente d'accéder à la base de données à l'aide de vos informations d'identification. Si la tentative échoue, vous êtes invité à entrer les informations d'identification de l'utilisateur de la base de données. Web Studio télécharge ensuite le schéma de base de données vers la base de données. Les informations d'identification ne sont conservées que durant la création de la base de données.
7. Si vous ne souhaitez pas que Web Studio crée la base de données, ou si vous ne disposez pas des autorisations suffisantes, cliquez sur **Générer script de base de données**. Les scripts générés contiennent des instructions permettant de créer manuellement la base de données et une base de données miroir, si nécessaire. Avant le chargement du schéma, assurez-vous que la base de données est vide et qu'au moins un utilisateur est autorisé à accéder et modifier la base de données.

Informations supplémentaires

- Outil de dimensionnement de base de données.
- Le dimensionnement de la base de données du site et la configuration des chaînes de connexion lors de l'utilisation de solutions de haute disponibilité de SQL Server.

Méthodes de mise à disposition

June 27, 2024

Citrix Virtual Apps and Desktops propose différentes méthodes de remise. Une seule méthode de mise à disposition ne répondra probablement pas à tous vos besoins.

Introduction

Le choix de la méthode appropriée permet d'améliorer la capacité à monter en charge, la gestion et l'expérience utilisateur.

- **Application installée :** l'application fait partie de l'image de bureau de base. Le processus d'installation implique l'exécution de fichiers dll, exe et d'autres fichiers copiés sur le lecteur d'image ainsi que des modifications du registre. Pour de plus amples informations, consultez la section Créer des catalogues de machines.
- **Applications livrées en streaming (Microsoft App-V) :** l'application est profilée et mise à disposition à la demande sur les bureaux du réseau. Les fichiers d'applications et les paramètres du Registre sont placés dans un conteneur sur le bureau virtuel et isolés du système d'exploitation et les uns des autres. Cet isolement permet de résoudre les problèmes de compatibilité. Pour plus d'informations, consultez la section Déployer et fournir des applications App-V.
- **Application en couche (Citrix application Layering) :** chaque couche contient une seule application, un seul agent ou un seul système d'exploitation. En intégrant une couche d'OS, une couche de plate-forme (VDA, agent Citrix Provisioning) et de multiples couches d'applications, un administrateur peut facilement créer de nouvelles images déployables. Le layering simplifie les activités de maintenance régulières, car un système d'exploitation, une application et un agent existent dans une seule couche. Lorsque vous mettez à jour la couche, toutes les images déployées contenant cette couche sont mises à jour. Pour plus d'informations, consultez la section Citrix App Layering.
- **Application Windows hébergée :** application installée sur un hôte Citrix Virtual Apps multi-utilisateur et déployée en tant qu'application et non en tant que bureau. Un utilisateur accède à l'application Windows hébergée en toute transparence à partir d'un bureau VDI ou d'une machine de point de terminaison, ce qui occulte le fait que l'application est exécutée à distance. Pour de plus amples informations, consultez la section Créer des groupes de mise à disposition.
- **Application locale :** application déployée sur la machine de point de terminaison. L'interface applicative s'affiche dans la session de VDI hébergée de l'utilisateur, bien qu'elle soit exécutée sur le point de terminaison. Pour de plus amples informations, consultez Local App Access et redirection d'adresse URL.

Pour les bureaux, vous pouvez envisager des bureaux publiés ou des bureaux VDI.

Applications et bureaux publiés avec Citrix Virtual Apps

Utilisez les machines avec OS multi-session pour mettre à disposition des applications publiées et des bureaux publiés Citrix Virtual Apps and Desktops.

Cas d'utilisation :

- Une mise à disposition peu onéreuse sur le serveur pour réduire le coût de mise à disposition des applications pour un grand nombre d'utilisateurs, tout en offrant une expérience utilisateur haute définition en toute sécurité.
- Vos utilisateurs effectuent des tâches clairement définies, et qui ne requièrent aucune personnalisation ou accès en mode déconnecté aux applications. Les utilisateurs peuvent inclure des travailleurs productifs, tels que des opérateurs de centre d'appel et des travailleurs au détail, ou des utilisateurs qui partagent des stations de travail.
- Types d'application : toute application.

Avantages et considérations :

- Solution gérable et évolutive dans votre datacenter.
- Solution de mise à disposition des applications la moins onéreuse.
- Les applications hébergées sont gérées de manière centralisée et les utilisateurs ne peuvent pas les modifier. Cela permet de fournir une expérience utilisateur cohérente, sûre et fiable.
- Les utilisateurs doivent être en ligne pour accéder à leurs applications.

Expérience utilisateur :

- L'utilisateur demande une ou plusieurs applications depuis StoreFront, le menu **Démarrer** ou une adresse URL que vous fournissez.
- Les applications sont mises à disposition virtuellement et s'affichent en toute transparence en haute définition sur les machines utilisateur.
- En fonction des paramètres de profil, les modifications apportées par l'utilisateur sont enregistrées lorsque la session applicative de l'utilisateur prend fin. Sinon, les modifications sont supprimées.

Traiter, héberger et mettre à disposition des applications :

- Le traitement de l'application a lieu sur les machines hôtes, plutôt que sur les machines utilisateur. La machine hôte peut être une machine physique ou virtuelle.
- Les applications et les bureaux résident sur une machine équipée d'un système d'exploitation multi-session.
- Les machines deviennent disponibles au travers des catalogues de machines.
- Les machines présentes dans des catalogues de machines sont organisées en groupes de mise à disposition qui mettent à disposition le même ensemble d'applications vers des groupes d'utilisateurs.

- Les machines avec système d'exploitation multi-session prennent en charge les groupes de mise à disposition qui hébergent des applications, des bureaux, ou les deux.

Gestion et attribution de sessions :

- Les machines équipées d'un système d'exploitation multi-session exécutent plusieurs sessions à partir d'une seule machine pour mettre à disposition plusieurs applications et bureaux vers de multiples utilisateurs connectés simultanément. Chaque utilisateur requiert une seule session depuis laquelle il peut exécuter toutes ses applications hébergées.

  Par exemple, un utilisateur ouvre une session et requiert une application. Une session sur cette machine devient indisponible pour d'autres utilisateurs. Un second utilisateur ouvre une session et requiert une application que cette machine héberge. Une seconde session sur la même machine est maintenant disponible. Si les deux utilisateurs demandent des applications supplémentaires, aucune session supplémentaire n'est requise, car un utilisateur peut exécuter de multiples applications à l'aide de la même session. Si deux utilisateurs ou plus ouvrent une session et demandent des bureaux, et deux sessions sont disponibles sur la même machine, cette machine unique utilise maintenant quatre sessions pour héberger quatre utilisateurs différents.
- Dans le groupe de mise à disposition auquel un utilisateur est attribué, une machine sur le serveur le moins chargé est sélectionnée. Une machine avec une session de disponibilité est attribuée de manière aléatoire pour mettre à disposition les applications à un utilisateur lorsque ce dernier ouvre une session.

VM hosted Apps

Utiliser des machines avec OS mono-session pour mettre à disposition des applications hébergées sur une machine virtuelle

Cas d'utilisation :

- Vous recherchez une solution de mise à disposition d'applications basée sur client qui soit sécurisée, offre une gestion centralisée et prenne en charge un grand nombre d'utilisateurs par serveur hôte. Vous voulez fournir à ces utilisateurs des applications affichées en haute définition.
- Vos utilisateurs sont des sous-traitants internes ou externes, des collaborateurs tiers et autres membres d'équipe provisoire. Vos utilisateurs ne requièrent aucun accès à des applications hébergées en mode déconnecté.
- Types d'application : applications qui risquent de ne pas fonctionner correctement avec d'autres applications ou qui peuvent interagir avec le système d'exploitation, telles que .NET Framework. Ces types d'applications sont idéaux pour l'hébergement sur des machines virtuelles.

Avantages et considérations :

- Les applications et les bureaux sur l'image principale sont hébergés, gérés et exécutés en toute sécurité sur les machines de votre centre de données, qui fournissent une solution de mise à disposition d'applications la moins onéreuse.
- Dès l'ouverture de session, les utilisateurs peuvent être attribués à une machine de manière aléatoire au sein d'un groupe de mise à disposition qui est configuré pour héberger la même application. Vous pouvez également attribuer une machine unique pour mettre une application une application vers un seul utilisateur chaque fois que l'utilisateur ouvre une session. Les machines attribuées de manière statique permettent aux utilisateurs d'installer et de gérer leurs propres applications sur la machine virtuelle.
- L'exécution de plusieurs sessions n'est pas prise en charge sur des machines équipées d'un OS mono-session. Par conséquent, chaque utilisateur utilise une seule machine au sein d'un groupe de mise à disposition lorsqu'il ouvre une session, et les utilisateurs doivent être en ligne pour accéder à leurs applications.
- Cette méthode peut augmenter la quantité de ressources serveur nécessaires au traitement des applications et augmenter la quantité de stockage pour les données des utilisateurs.

Expérience utilisateur :

- La même expérience d'application transparente que l'hébergement des applications partagées sur les machines équipées d'un OS multi-session.

Traiter, héberger et mettre à disposition des applications :

- Identique aux machines avec OS multi-session, sauf qu'il s'agit de machines avec OS virtuel mono-session.

Gestion et attribution de sessions :

- Les machines équipées d'un OS mono-session exécutent une seule session de bureau à partir d'une seule machine. Lors de l'accès à des applications uniquement, un seul utilisateur peut utiliser plusieurs applications (et n'est pas limité à une seule application), car le système d'exploitation accède à chaque application comme une nouvelle session.
- Dans un groupe de mise à disposition, lorsque les utilisateurs ouvrent une session, ils peuvent accéder à une machine affectée de manière statique (à chaque fois que l'utilisateur ouvre une session sur la même machine) ou une machine affectée de manière aléatoire qui est sélectionnée en fonction de la disponibilité de session.

Bureaux VDI

Utilisez des machines avec OS mono-session pour mettre à disposition des bureaux VDI Citrix Virtual Apps and Desktops.

Les bureaux VDI sont hébergés sur des machines virtuelles et fournissent à chaque utilisateur un système d'exploitation de bureau.

Les bureaux VDI requièrent plus de ressources que les bureaux publiés, mais n'exigent pas que les applications installées sur ceux-ci prennent en charge des systèmes d'exploitation serveur. De plus, selon le type de bureau VDI que vous choisissez, ces bureaux peuvent être affectés à des utilisateurs individuels. Cela fournit aux utilisateurs un haut degré de personnalisation.

Lorsque vous créez un catalogue de machines pour les bureaux VDI, vous créez un de ces types de bureaux :

- **Bureaux aléatoires non persistants, également appelé bureaux VDI regroupés :** chaque fois qu'un utilisateur ouvre une session sur l'un de ces bureaux, cet utilisateur se connecte à un bureau sélectionné à partir d'un groupe de bureaux. Ce groupe est basé sur une image principale unique. Toutes les modifications apportées au bureau sont perdues lorsque la machine redémarre.
- **Bureau statique non persistant :** lors de la première connexion, un bureau est affecté à un utilisateur à partir d'un pool de bureaux. (Chaque machine dans le pool est basée sur une image principale unique.) Après la première utilisation, chaque fois qu'un utilisateur ouvre une session sur un bureau, cet utilisateur se connecte au même bureau qui lui a été affecté lors de la première utilisation. Toutes les modifications apportées au bureau sont perdues lorsque la machine redémarre.
- **Bureau statique persistant :** à l'inverse des autres types de bureaux VDI, les utilisateurs peuvent entièrement personnaliser ces bureaux. Lors de la première connexion, un bureau est affecté à un utilisateur à partir d'un pool de bureaux. Les ouvertures de session suivantes de cet utilisateur se connectent au bureau qui a été affecté lors de la première utilisation. Les modifications apportées au bureau sont conservées lorsque la machine redémarre.

Remote PC Access

Remote PC Access est une fonctionnalité de Citrix Virtual Apps and Desktops qui permet aux entreprises d'autoriser facilement leurs employés à accéder aux ressources de l'entreprise à distance et de manière sécurisée. La plate-forme Citrix rend cet accès sécurisé possible en donnant aux utilisateurs l'accès à leurs ordinateurs de bureau physiques. Si les utilisateurs peuvent accéder à leurs ordinateurs de bureau, ils peuvent accéder à toutes les applications, données et ressources dont ils ont besoin pour effectuer leur travail. Remote PC Access élimine le besoin d'introduire et de fournir d'autres outils pour permettre le télétravail. Par exemple, les bureaux virtuels ou les applications et l'infrastructure associée.

Remote PC Access utilise les composants Citrix Virtual Apps and Desktops qui fournissent des bureaux virtuels et des applications. Par conséquent, les exigences et le processus de déploiement et de configuration de Remote PC Access sont les mêmes que ceux requis pour déployer Citrix Virtual Apps and

Desktops pour la mise à disposition de ressources virtuelles. Cette uniformité offre une expérience administrative cohérente et unifiée. Les utilisateurs bénéficient d'une meilleure expérience utilisateur lorsque Citrix HDX est utilisé pour fournir leur session PC de bureau.

Pour plus d'informations, consultez Remote PC Access.

Ports réseau

June 27, 2024

Des informations complètes sur les ports réseau sont fournies dans Ports de communication utilisés par les technologies Citrix.

Lorsque les composants Citrix sont installés, le pare-feu hôte du système d'exploitation est également mis à jour pour correspondre aux ports réseau par défaut.

Les informations de port peuvent vous être utiles :

- À des fins de conformité réglementaire.
- S'il existe un pare-feu réseau entre les composants Citrix Virtual Apps and Desktops et d'autres produits ou composants Citrix, de façon à ce que vous puissiez configurer ce pare-feu correctement.
- Si vous utilisez un pare-feu hôte tiers, tel que celui fourni avec un logiciel anti-malware, plutôt que l'hôte pare-feu du système d'exploitation.
- Si vous modifiez la configuration du pare-feu hôte sur ces composants (généralement le service Pare-feu Windows).
- Si vous reconfigurez des fonctionnalités de composants afin d'utiliser une plage de ports ou un port différent, et que vous voulez désactiver ou bloquer les ports non utilisés dans votre configuration.

Certains des ports sont enregistrés auprès de l'IANA (Internet Assigned Numbers Authority). Les détails concernant ces attributions sont disponibles sur http://www.iana.org/assignments/port-numbers. Cependant, les informations descriptives détenues par l'IANA ne reflètent pas toujours l'utilisation d'aujourd'hui.

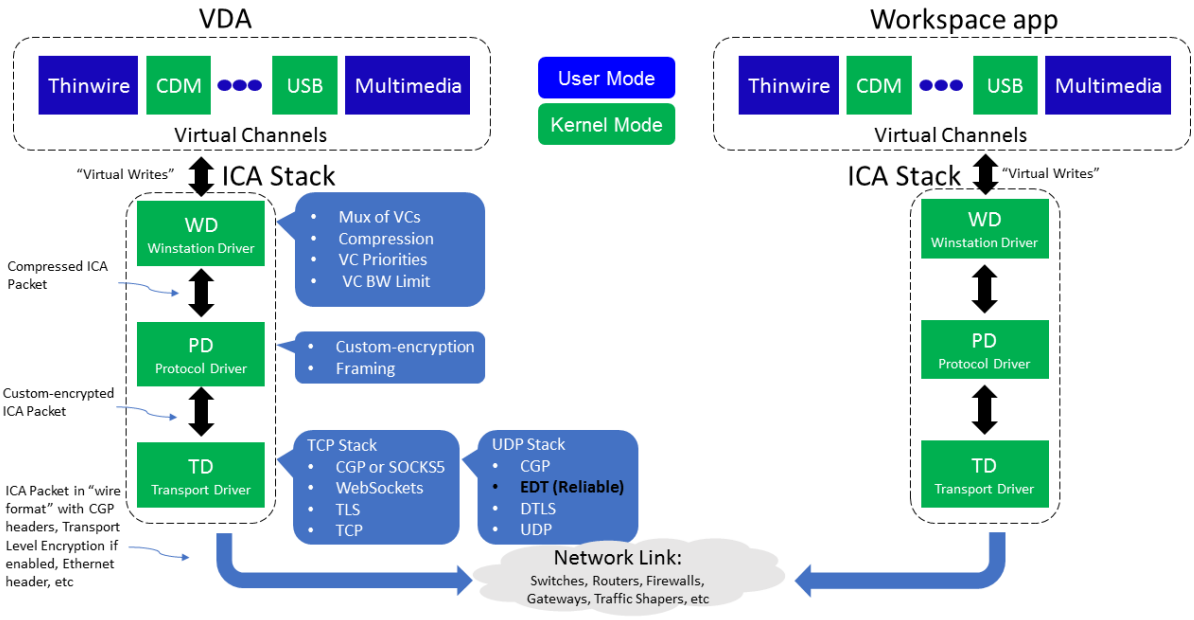
Par ailleurs, les systèmes d'exploitation sur le VDA et Delivery Controller nécessitent des ports entrants pour leur propre usage. Consultez la documentation Microsoft Windows pour plus de détails.

HDX

June 27, 2024

> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Citrix HDX représente un large ensemble de technologies qui offrent une expérience haute définition aux utilisateurs d'applications et de bureaux centralisés, sur tout périphérique et sur tout réseau.



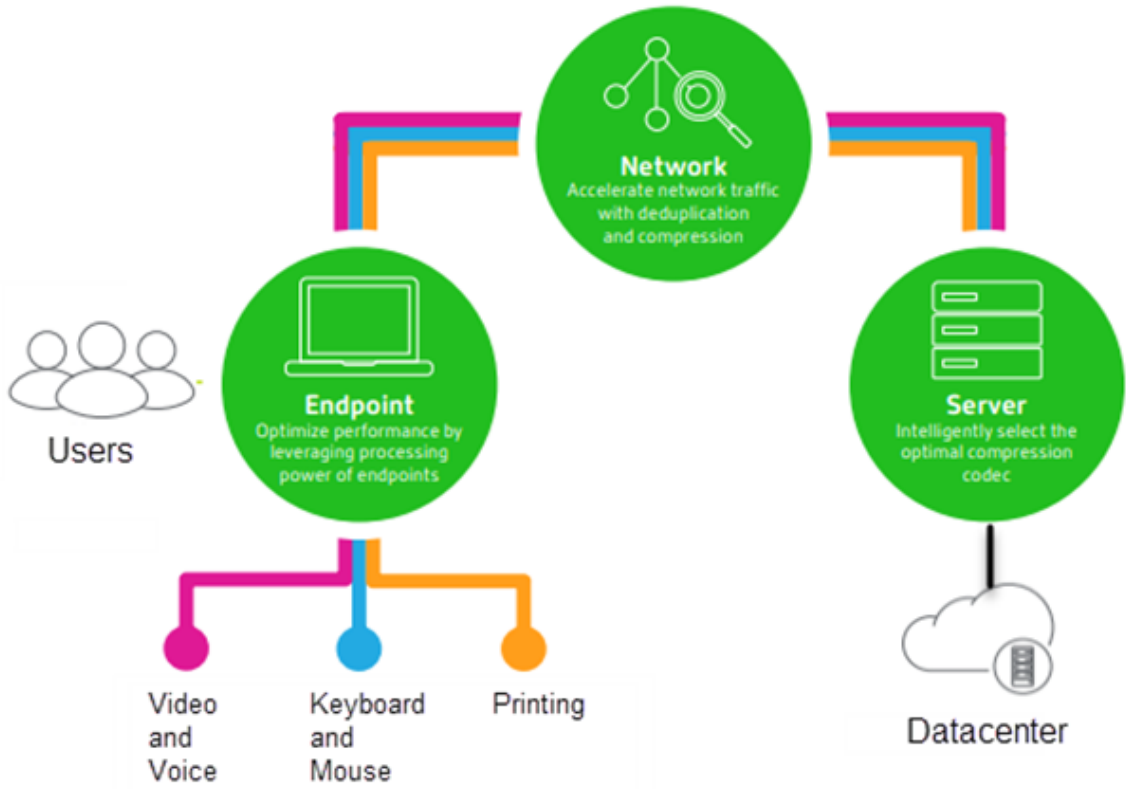
HDX est conçu autour de trois principes techniques :

- Redirection intelligente
- Compression adaptative
- Déduplication des données

Appliqués selon différentes combinaisons, ils optimisent l'expérience du service informatique et des utilisateurs, réduisent la consommation de bande passante et augmentent la densité utilisateur par serveur d'hébergement.

- **Redirection intelligente** - La redirection intelligente examine l'activité de l'écran, les commandes de l'application, la machine de point de terminaison, ainsi que les fonctionnalités réseau et serveur, afin de déterminer instantanément où et comment restituer l'activité d'une application ou d'un bureau. Le rendu peut avoir lieu sur la machine de point de terminaison ou sur le serveur d'hébergement.

- **Compression adaptative** - La compression adaptative permet aux affichages multimédias riches d'être livrés sur des connexions réseau légères. HDX commence par évaluer plusieurs variables, telles que le type d'entrée, le périphérique et l'affichage (texte, vidéo, voix et multimédia). Il choisit le codec de compression optimal et la meilleure proportion d'utilisation d'UC et de processeur graphique. Il s'adapte ensuite intelligemment en fonction de chaque utilisateur et de chaque base. Cette adaptation intelligente se fait par utilisateur, voire par session.



- **Déduplication des données** - La déduplication du trafic réseau réduit l'ensemble des données envoyées entre le client et le serveur. Pour ce faire, elle tire parti des schémas répétitifs dans les données couramment utilisées, telles que les graphiques bitmap, les documents, les travaux d'impression et le multimédia en streaming. La mise en cache de ces modèles permet de transmettre uniquement les modifications sur le réseau, ce qui évite de dupliquer le trafic. HDX prend également en charge la multidiffusion de flux multimédias, dans lesquels une seule transmission à partir de la source est visualisée par plusieurs abonnés à un même emplacement, plutôt qu'une connexion individuelle pour chaque utilisateur.

Pour plus d'informations, voir Augmenter votre productivité avec un espace de travail utilisateur haute définition.

Sur la machine

HDX utilise les capacités informatiques des machines utilisateur pour améliorer et optimiser l'expérience utilisateur. La technologie HDX offre aux utilisateurs un rendu fluide et transparent du contenu multimédia disponible sur leur bureau ou application virtuels. Le contrôle de l'espace de travail permet aux utilisateurs de suspendre les applications et les bureaux virtuels et de continuer à travailler à partir d'une autre machine, à l'endroit où ils l'ont laissé.

Sur le réseau

HDX offre des fonctionnalités d'accélération et d'optimisation pour mettre à disposition les meilleures performances réseau, y compris sur les connexions à faible bande passante ou en réseau étendu présentant une forte latence.

Les fonctionnalités HDX s'adaptent aux modifications de l'environnement. Elles équilibrent les performances et la bande passante. Elles appliquent les meilleures technologies possibles à chaque scénario, que le bureau ou l'application soit accessible localement sur le réseau d'entreprise ou à distance, en dehors du pare-feu de l'entreprise.

Dans le data center

HDX utilise la puissance de calcul et de la scalabilité des serveurs de façon à offrir des performances graphiques avancées, quelles que soient les capacités de la machine utilisateur.

La surveillance du canal HDX, fournie par Citrix Director, affiche le statut des canaux HDX connectés sur les machines utilisateur.

HDX Insight

HDX Insight est l'intégration de NetScaler Network Inspector et de Performance Manager avec Director. Il capture des données sur le trafic ICA et propose un tableau de bord des données en temps réel et historiques. Ces données comprennent la latence de session ICA côté client et côté serveur, l'utilisation de bande passante des canaux ICA et la durée des boucles ICA de chaque session.

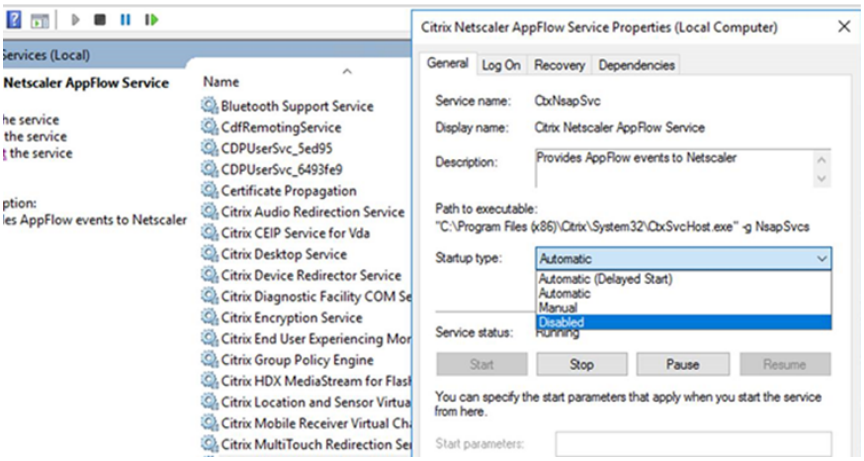
Vous pouvez activer NetScaler pour utiliser le canal virtuel HDX Insight afin de déplacer tous les points de données requis dans un format non compressé. Si vous désactivez cette fonctionnalité, le périphérique NetScaler déchiffre et décompresse la propagation du trafic ICA sur différents canaux virtuels. L'utilisation du canal virtuel unique réduit la complexité, améliore la scalabilité et est plus rentable.

Configuration minimale requise :

- NetScaler version 12.0 Build 57.x
- Application Citrix Workspace pour Windows 1808
- Citrix Receiver pour Windows 4.10
- Application Citrix Workspace pour Mac 1808
- Citrix Receiver pour Mac 12.8

Activer ou désactiver le canal virtuel HDX Insight

Pour désactiver cette fonctionnalité, définissez les propriétés du service Citrix NetScaler Application Flow sur Désactivé. Pour activer cette fonctionnalité, définissez le service sur Automatique. Dans les deux cas, nous vous recommandons de redémarrer le serveur après avoir modifié ces propriétés. Ce service est activé par défaut (Automatique).



Bénéficiez des capacités HDX de votre bureau virtuel

- Pour voir comment la redirection du contenu du navigateur, une des quatre technologies de redirection multimédia HDX, accélère la mise à disposition de contenu multimédia HTML5 et WebRTC :

  1. Téléchargez l'extension de navigateur Chrome et installez-la sur le bureau virtuel.
  2. Pour découvrir la manière dont la redirection du contenu du navigateur accélère la mise à disposition du contenu multimédia vers des bureaux virtuels, affichez une vidéo sur votre bureau à partir d'un site Web contenant des vidéos HTML5, comme YouTube. Les utilisateurs ne savent pas quand la redirection du contenu du navigateur est en cours d'exécution. Pour voir si la redirection du contenu du navigateur est utilisée, faites glisser rapidement la fenêtre du navigateur. Vous verrez un délai ou un décalage entre la fenêtre et l'interface utilisateur. Vous pouvez également cliquer avec le bouton droit sur la page Web et rechercher **À propos de la redirection de navigateur HDX** dans le menu.

- Pour voir comment HDX diffuse l'audio à définition élevée :

    1. Configurez le client Citrix pour une qualité audio maximale ; consultez la documentation relative à l'application Citrix Workspace pour plus de détails.
    2. Lire les fichiers musicaux à l'aide d'un lecteur audio numérique (tels que iTunes) sur votre bureau.

HDX offre des graphiques et une expérience vidéo supérieurs pour la plupart des utilisateurs par défaut, sans configuration requise. Les paramètres de stratégie Citrix qui offrent la meilleure expérience possible à la plupart des cas d'utilisation sont activés par défaut.

- HDX sélectionne automatiquement la meilleure méthode de mise à disposition basée sur le client, la plate-forme, l'application et la bande passante réseau, puis ajuste le tout basé sur la modification des conditions.
- HDX optimise les performances de graphiques 2D et 3D et de la vidéo.
- HDX permet aux machines utilisateur de livrer en streaming des fichiers multimédia directement à partir du fournisseur source sur Internet ou l'intranet, plutôt qu'au travers du serveur hôte. Si la configuration requise pour la récupération de contenu côté client n'est pas présente, la diffusion de contenu multimédia revient à la redirection multimédia et à la récupération de contenu côté serveur. En général, aucune modification des stratégies de fonctionnalité de la redirection multimédia n'est nécessaire.
- HDX diffuse des vidéos riches en contenu, générées par le serveur, sur les bureaux virtuels lorsque la redirection multimédia n'est pas disponible : afficher une vidéo sur un site Web contenant des vidéos haute définition, par exemple, http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.

À savoir :

- Pour plus d'informations sur la prise en charge et la configuration requise pour les fonctionnalités HDX, consultez l'article Configuration système requise. Sauf mention contraire, les fonctionnalités HDX sont disponibles pour la prise en charge des machines avec OS multi-session Windows et avec OS mono-session Windows et les bureaux Remote PC Access.
- Ce contenu décrit comment optimiser l'expérience utilisateur, améliorer l'extensibilité du serveur ou réduire les besoins en bande passante. Pour de plus amples informations sur l'utilisation des stratégies Citrix et des paramètres de stratégie, consultez la documentation relative aux stratégies Citrix pour cette version.
- Pour obtenir des instructions qui incluent la modification du Registre, faites attention : la modification du Registre peut entraîner de sérieux problèmes qui pourraient nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Reconnexion automatique des clients et fiabilité de session

Lors de l'accès à des applications ou bureaux hébergés, une interruption du réseau peut se produire. Pour bénéficier d'une reconnexion plus fluide, nous offrons la reconnexion automatique des clients et la fiabilité de session. Dans une configuration par défaut, la fiabilité de session commence, puis la reconnexion automatique des clients suit.

Reconnexion automatique des clients :

La reconnexion automatique des clients relance le moteur client pour reconnecter une session déconnectée. La fonction de reconnexion automatique des clients ferme (ou déconnecte) la session utilisateur après la durée spécifiée dans le paramètre. Si la reconnexion automatique des clients est en cours, le système envoie à l'utilisateur une notification d'interruption du réseau pour les applications et les bureaux de cette manière :

- **Bureaux.** La fenêtre de session est grisée et un minuteur affiche le temps restant avant la reconnexion.
- **Applications.** La fenêtre de session se ferme et une boîte de dialogue s'affiche avec un minuteur qui indique le temps restant avant les tentatives de reconnexion.

Lors d'une reconnexion automatique de client, les sessions redémarrent en supposant une connectivité réseau. L'utilisateur ne peut pas interagir avec les sessions lorsque la reconnexion automatique de client est en cours.

À la reconnexion, les sessions déconnectées se reconnectent à l'aide des informations de connexion enregistrées. L'utilisateur peut interagir normalement avec les applications et bureaux.

Paramètres de reconnexion automatique des clients par défaut :

- Délai de reconnexion automatique des clients : 120 secondes
- Reconnexion automatique des clients : activée
- Authentification de la reconnexion automatique des clients : désactivée
- Journalisation de la reconnexion automatique des clients : désactivée

Pour plus d'informations, consultez la section Paramètres de stratégie Reconnexion automatique des clients.

Fiabilité de session :

La fiabilité de session reconnecte les sessions ICA en toute transparence pour toutes les interruptions réseau. La fonction de fiabilité de session ferme (ou déconnecte) la session utilisateur après la durée spécifiée dans le paramètre. Après l'expiration du délai de fiabilité de session, les paramètres de reconnexion automatique des clients s'appliquent et la fonction tente d'opérer la reconnexion de l'utilisateur à la session déconnectée. Lorsque la fiabilité de session est en cours, une notification d'interruption du réseau pour les applications et les bureaux est envoyée comme suit à l'utilisateur :

- **Bureaux.** La fenêtre de session devient translucide et un minuteur affiche le temps restant avant la reconnexion.
- **Applications.** La fenêtre devient translucide et des messages de connexion interrompue s'affichent depuis la barre d'état système.

Lorsque la fiabilité de session est active, l'utilisateur ne peut pas interagir avec les sessions ICA. Toutefois, les actions utilisateur telles que les frappes au clavier sont mises en mémoire tampon pendant quelques secondes juste après l'interruption du réseau et retransmises une fois que le réseau est disponible.

À la reconnexion, le client et le serveur reprennent au point où ils se trouvaient dans leur échange de protocole. Les fenêtres de session ne sont plus translucides et des messages de barre d'état système appropriés s'affichent pour les applications.

Paramètres de fiabilité de session par défaut

- Expiration de délai de la fiabilité de session : 180 secondes
- Niveau d'opacité de l'interface durant la reconnexion : 80 %
- Connexion de fiabilité de session : activée
- Numéro de port de la fiabilité de session : 2598

Pour plus d'informations, consultez la section Paramètres de stratégie Fiabilité de session.

NetScaler avec reconnexion automatique des clients et fiabilité de session :

Si les stratégies Multi-Stream et Multi-Port sont activées sur le serveur et que tout ou partie de ces informations sont vraies, la reconnexion automatique des clients ne fonctionne pas :

- La fonction de fiabilité de session est désactivée sur NetScaler Gateway.
- Un basculement est effectué sur le boîtier NetScaler.
- NetScaler SD-WAN est utilisé avec NetScaler Gateway.

Débit adaptatif HDX

Le débit adaptatif HDX affine intelligemment le débit maximal de la session ICA en ajustant les tampons de sortie. Le nombre de tampons de sortie est initialement défini sur une valeur élevée. Cette valeur élevée permet de transmettre les données au client plus rapidement et efficacement, en particulier dans les réseaux à latence élevée. Grâce à une meilleure interactivité, à des transferts de fichiers plus rapides, à une lecture vidéo plus fluide, à une fréquence d'images et à une résolution plus élevées, vous bénéficiez d'une meilleure expérience utilisateur.

L'interactivité des sessions est constamment mesurée pour déterminer si des flux de données au sein de la session ICA nuisent à l'interactivité. Si c'est le cas, le débit diminue pour réduire l'impact du flux de données volumineux sur la session et permettre la récupération de l'interactivité.

> **Important :**
>
> Le débit adaptatif HDX modifie la façon dont les tampons de sortie sont définis en déplaçant ce mécanisme du client vers le VDA et aucune configuration manuelle n'est nécessaire.

Cette fonctionnalité nécessite les éléments suivants :

- VDA version 1811 ou ultérieure
- Application Workspace pour Windows 1811 ou version ultérieure

Améliorer la qualité d'image envoyée aux machines utilisateur

Les paramètres de stratégie d'affichage visuel suivants contrôlent la qualité des images envoyées depuis des bureaux virtuels vers les machines utilisateur.

- Qualité visuelle. Contrôle la qualité visuelle des images affichées sur la machine utilisateur : moyenne, élevée, toujours sans perte, sans perte si possible (valeur par défaut = moyenne). La qualité de la vidéo avec le paramètre par défaut « moyenne » dépend de la bande passante disponible.
- Taux de trames cible. Spécifie le nombre maximal de trames par seconde envoyées depuis le bureau virtuel vers la machine utilisateur (valeur par défaut = 30). Pour les périphériques avec des UC plus lents, la spécification d'une valeur inférieure permet d'améliorer l'expérience de l'utilisateur. Le taux maximal pris en charge est 60 trames par seconde.
- Limite de mémoire d'affichage. Spécifie la taille maximale de la mémoire tampon vidéo (en kilo-octets) pour la session (valeur par défaut = 65536 Ko). Pour les connexions nécessitant un nombre de couleurs et une résolution élevés, augmentez la limite. Vous pouvez calculer la mémoire maximale nécessaire.

> **Remarque :**
>
> Le paramètre **Limite de mémoire d'affichage** est obsolète. Avec cette modification, Citrix ne limite plus la mémoire d'affichage. Au lieu de cela, la quantité minimale de mémoire requise est allouée pour garantir que la disposition d'affichage du client est parfaitement adaptée.

Améliorer les performances de conférence vidéo

Plusieurs applications de visioconférence populaires sont optimisées pour la mise à disposition à partir de Citrix Virtual Apps and Desktops via la redirection multimédia (voir, par exemple, le pack d'optimisation HDX RealTime). Pour les applications qui ne sont pas optimisées, la compression vidéo de webcam HDX permet d'améliorer l'efficacité de la bande passante et la tolérance à la latence pour les webcams durant la visioconférence dans une session. Cette technologie livre en streaming le trafic de webcam sur un canal virtuel multimédia dédié. Cette technologie utilise moins de bande passante

par rapport à la prise en charge de la redirection USB Plug-n-Play HDX isochrone et fonctionne bien sur des connexions en réseau étendu.

Toutefois, les utilisateurs de l'application Citrix Workspace peuvent remplacer le comportement par défaut en choisissant le paramètre Mic & Webcam de Desktop Viewer : **Ne pas utiliser mon micro ou ma webcam**. Pour empêcher les utilisateurs de basculer depuis la compression vidéo de webcam HDX, désactivez la redirection du périphérique USB en utilisant Paramètres de stratégie sous ICA > Périphériques USB.

La compression vidéo de webcam HDX nécessite que les paramètres de stratégie suivants soient activés (tous sont activés par défaut).

- Redirection audio cliente
- Redirection du microphone client
- Conférences multimédia

Si une webcam prend en charge le codage matériel, la compression vidéo HDX utilise le codage matériel par défaut. Le codage matériel peut consommer plus de bande passante que le logiciel de codage. Pour forcer la compression logicielle, ajoutez la valeur de clé DWORD suivante pour la clé de Registre HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

Priorités du trafic réseau

Les priorités sont attribuées au trafic réseau sur plusieurs connexions pour une session à l'aide de routeurs prenant en charge la qualité de service. Quatre flux TCP et deux flux UDP sont disponibles pour transporter le trafic ICA entre la machine utilisateur et le serveur :

- Flux TCP : en temps réel, interactifs, arrière-plan et en bloc
- Flux UDP : pour la voix et pour la communication à distance d'écran Framehawk

Chaque canal virtuel est associé à une priorité spécifique et transporté dans la connexion correspondante. Vous pouvez définir les canaux indépendamment, en fonction du numéro de port TCP utilisé pour la connexion.

Les connexions en streaming de canal multiples sont prises en charge pour les Virtual Delivery Agents (VDA) installés sur les machines Windows 10, Windows 8 et Windows 7. Travaillez avec votre administrateur réseau pour vous assurer que les ports Common Gateway Protocol (CGP) configurés dans le paramètre **Stratégie multi-ports** sont correctement attribués sur les routeurs réseau.

La qualité de service n'est prise en charge que lorsque des ports de fiabilité de session multiples, ou des ports CGP, sont configurés.

> **Avertissement :**
>
> Lors de l'utilisation de cette fonctionnalité, assurez-vous que le transport est sécurisé. Citrix vous recommande d'utiliser Internet Protocol Security (IPsec) ou Transport Layer Security (TLS). Les connexions TLS sont prises en charge uniquement lorsque les connexions traversent une passerelle NetScaler Gateway qui prend en charge Multi-Stream ICA. Sur un réseau d'entreprise interne, les connexions multi-stream avec TLS ne sont pas prises en charge.

Pour définir la qualité de service pour plusieurs connexions en streaming, ajoutez les paramètres de stratégie Citrix suivants pour une stratégie (voir Paramètres de stratégie Connexions Multi-Stream pour plus de détails) :

- Stratégie Multi-Port : ce paramètre spécifie les ports pour le trafic ICA au travers de plusieurs connexions et établit des priorités de réseau.
  - Sélectionnez une priorité dans la liste Priorité de port CGP par défaut. Par défaut, le port principal (2598) a une priorité élevée.
  - Entrez des ports CGP supplémentaires dans Port1 CGP, port2 CGP et port3 CGP le cas échéant et attribuez-leur des priorités. Chaque port doit disposer d'une priorité unique.

  Configurez explicitement les pare-feu sur les VDA pour autoriser le trafic TCP supplémentaire.
- Paramètre d'ordinateur Multi-Stream : ce paramètre est désactivé par défaut. Si vous utilisez Citrix NetScaler SD-WAN et que le Multi-Stream est pris en charge dans votre environnement, il n'est pas nécessaire de configurer ce paramètre. Configurez ce paramètre de stratégie lorsque vous utilisez des routeurs tiers ou des NetScaler SD-WAN d'ancienne génération pour réaliser la qualité de service désirée.
- Paramètre utilisateur Multi-Stream : ce paramètre est désactivé par défaut.

Pour que les stratégies contenant ces paramètres soient appliquées, les utilisateurs doivent fermer leur session, puis ouvrir une session sur le réseau.

Affichage ou masquage de la barre de langue distante

La barre de langue affiche la langue de saisie préférée dans une session. Si cette fonctionnalité est activée (par défaut), vous pouvez afficher ou masquer la barre de langue depuis **Préférences avancées > Barre de langue** dans application Citrix Workspace pour Windows. En utilisant un paramètre de Registre du côté VDA, vous pouvez désactiver le contrôle client de la fonctionnalité de barre de langue. Si cette fonctionnalité est désactivée, le paramètre de l'interface utilisateur du client ne prend pas effet et le paramètre actuel de l'utilisateur détermine l'état de la barre de langue. Pour de plus amples informations, consultez l'article Améliorer l'expérience utilisateur.

Pour désactiver le contrôle client de la fonctionnalité de barre de langue du VDA :

1. Dans l'éditeur de registre, accédez à HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfsl
2. Créez une clé de valeur DWORD, SeamlessFlags, et définissez-la sur 0x40000.

Mappage de clavier Unicode

Citrix Receiver non Windows utilise la disposition du clavier local (Unicode). Si un utilisateur modifie la disposition du clavier local et la disposition du clavier du serveur (code d'analyse), il se peut qu'ils ne soient pas synchronisés et que la sortie soit incorrecte. Par exemple, Utilisateur1 modifie la disposition du clavier local de l'anglais vers l'allemand. Utilisateur1 change ensuite le clavier côté serveur vers l'allemand. Même si les deux dispositions de clavier sont en allemand, il se peut qu'elles ne soient pas synchronisées, ce qui entraîne une sortie de caractère incorrecte.

Activer ou désactiver le mappage de disposition du clavier Unicode

Par défaut, la fonctionnalité est désactivée sur le VDA. Pour activer la fonctionnalité, basculez-la via l'éditeur de registre regedit sur le VDA. Ajoutez la clé de registre suivante :

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nom : EnableKlMap

Type : DWORD

Valeur : 1

Pour désactiver cette fonctionnalité, définissez **EnableKlMap** sur 0 ou supprimez la clé **CTxKlMap**.

Activer le mode compatible de mappage de disposition du clavier Unicode

Par défaut, le mappage de disposition du clavier Unicode effectue automatiquement un hooking sur certaines API de Windows pour recharger le nouveau mappage de disposition de clavier Unicode lorsque vous modifiez la disposition du clavier côté serveur. Certaines applications ne peuvent pas être accrochées dans le cadre d'un hooking. Pour conserver la compatibilité, vous pouvez modifier la fonctionnalité vers le mode compatible pour prendre en charge ces applications non accrochées. Ajoutez la clé de registre suivante :

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nom : DisableWindowHook

Type : DWORD

Valeur : 1

Pour utiliser le mappage de disposition du clavier Unicode normal, définissez **DisableWindowHook** sur 0.

Canaux virtuels ICA Citrix

June 27, 2024

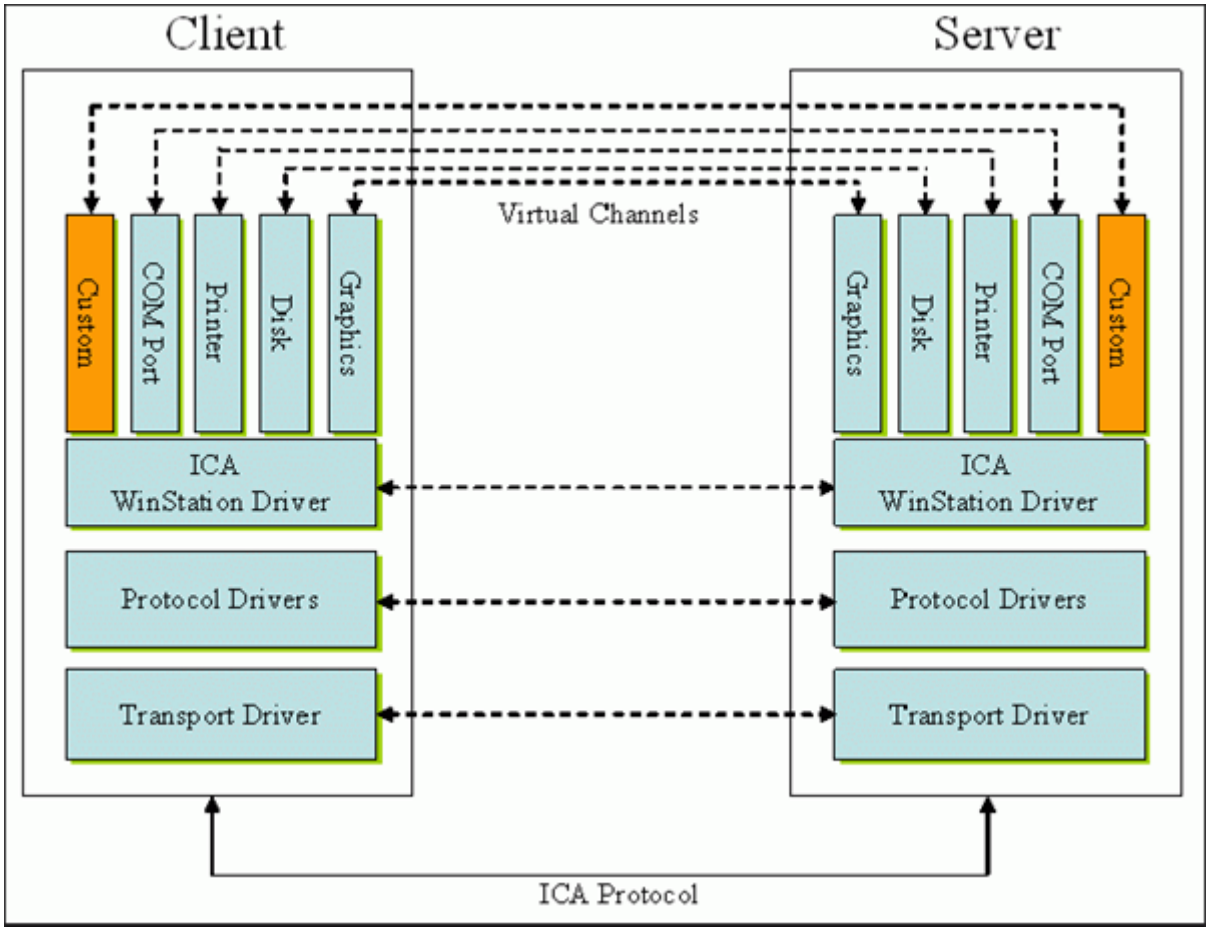
> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Que sont les canaux virtuels ICA ?

Une grande partie des fonctionnalités et de la communication entre l'application Citrix Workspace et les serveurs Citrix Virtual Apps and Desktops se produit sur des canaux virtuels. Les canaux virtuels font partie intégrante de l'expérience à distance avec les serveurs Citrix Virtual Apps and Desktops. Les canaux virtuels sont utilisés pour les éléments suivants :

- Audio
- Ports COM
- Disques
- Graphiques
- Ports LPT
- Imprimantes
- Cartes à puce
- Canaux virtuels personnalisés tiers
- Vidéo

De nouveaux canaux virtuels sont parfois publiés avec les nouvelles versions des serveurs Citrix Virtual Apps and Desktops et de l'application Citrix Workspace pour fournir plus de fonctionnalités.



Un canal virtuel consiste en un pilote virtuel côté client qui communique avec une application côté serveur. Citrix Virtual Apps and Desktops inclut différents canaux virtuels. Ils sont conçus pour permettre aux clients et aux fournisseurs tiers de créer leurs propres canaux virtuels à l'aide de l'un des kits de développement logiciel fournis (SDK).

Les canaux virtuels offrent un moyen sécurisé d'accomplir diverses tâches. Par exemple, une application qui s'exécute sur un serveur Citrix Virtual Apps qui communique avec un périphérique côté client ou une application qui communique avec l'environnement côté client.

Côté client, les canaux virtuels correspondent à des pilotes virtuels. Chaque pilote virtuel fournit une fonction spécifique. Certains sont requis pour le fonctionnement normal, et d'autres sont facultatifs. Les pilotes virtuels fonctionnent au niveau du protocole de la couche de présentation. Plusieurs protocoles peuvent être actifs à tout moment en multipliant les canaux fournis par la couche du protocole Windows Station (WinStation).

Les fonctions suivantes sont contenues dans la valeur de Registre VirtualDriver sous ce chemin de registre :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\
Advanced\Modules\ICA 3.0
```


Ou

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` (pour 64 bits)

- Thinwire3.0 (obligatoire)
- ClientDrive
- ClentPrinterQueue
- ClentPrinterPort
- Presse-papiers
- ClientComm
- ClientAudio
- LicenseHandler (obligatoire)
- TWI (obligatoire)
- SmartCard
- ICACTL (obligatoire)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> **Remarque :**
>
> Vous pouvez désactiver une fonctionnalité client spécifique en supprimant une ou plusieurs de ces valeurs de la clé de registre. Par exemple, si vous souhaitez supprimer le Presse-papiers client, supprimez le mot **Presse-papiers** (Clipboard).

Cette liste contient les fichiers de pilotes virtuels client et leurs fonctions respectives. Citrix Virtual Apps et l'application Citrix Workspace pour Windows utilisent ces fichiers. Ils se présentent sous la forme de bibliothèques de liens dynamiques (mode utilisateur), et non de pilotes Windows (mode noyau) à l'exception d'USB générique comme décrit dans Canal virtuel USB générique.

- vd3dn.dll –Canal virtuel Direct3D utilisé pour la redirection de composition du bureau
- vdcamN.dll –Audio bidirectionnel
- vdcdm30n.dll –Mappage de lecteur client
- vdcom30N.dll –Mappage de port COM client
- vdcpm30N.dll –Mappage d'imprimante client
- vdctln.dll –Canal de contrôle ICA
- vddvc0n.dll –Canal virtuel dynamique
- vdeuemn.dll –Surveillance de l'expérience utilisateur final
- vdgusbn.dll –Canal virtuel USB générique
- vdkbhook.dll –Transfert de touche transparent
- vdlfpn.dll –Canal d'affichage Framehawk sur UDP comme le transport

- vdmmn.dll –Support multimédia
- vdmrvc.dll –Canal virtuel du récepteur mobile
- vdmtchn.dll –Prise en charge multipoint
- vdscardn.dll –Prise en charge cartes à puce
- vdsens.dll –Canal virtuel des capteurs
- vdspl30n.dll –UPD client
- vdsspin.dll –Kerberos
- vdtuin.dll –Interface transparente
- vdtw30n.dll –Thinwire client
- vdtwin.dll –Transparence
- vdtwn.dll –Twain

Certains canaux virtuels sont compilés dans d'autres fichiers. Par exemple, le mappage du presse-papiers est disponible dans wfica32.exe

Compatibilité 64 bits

L'application Citrix Workspace pour Windows est compatible 64 bits. Comme pour la plupart des binaires compilés pour 32 bits, ces fichiers clients ont des équivalents compilés pour 64 bits :

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

Canal virtuel USB générique

L'implémentation du canal virtuel USB générique utilise deux pilotes en mode noyau avec le pilote de canal virtuel vdgusbn.dll :

- ctxusbm.sys
- ctxusbr.sys

Fonctionnement des canaux virtuels ICA

Les canaux virtuels sont chargés de plusieurs manières. L'environnement de ligne de commande (WFShell pour le serveur et PicaShell pour le poste de travail) charge certains canaux virtuels. Certains canaux virtuels sont hébergés en tant que services Windows.

Modules de canal virtuels chargés par l'environnement de ligne de commande Shell, par exemple :

- EUEM
- Twain
- Presse-papiers
- Multimédia
- Partage de session transparent
- Fuseau horaire

Certains sont chargés en mode noyau, par exemple :

- CtxDvcs.sys –Canal virtuel dynamique
- Icausbb.sys –Redirection USB générique
- Picadm.sys –Mappage des lecteurs clients
- Picaser.sys –Redirection de port COM
- Picapar.sys –Redirection de port LPT

Canal virtuel graphique côté serveur

`ctxgfx.exe` héberge le canal virtuel graphique pour les sessions basées sur poste de travail et serveur de terminal. `Ctxgfx` héberge des modules spécifiques aux plate-formes qui interagissent avec le pilote correspondant (`Icardd.dll` pour RDSH, et `vdod.dll` et `vidd.dll` pour poste de travail).

Pour les déploiements XenDesktop 3D Pro, un pilote graphique OEM est installé pour le GPU correspondant sur le VDA. `Ctxgfx` charge des modules adaptateurs spécialisés pour interagir avec le pilote graphique OEM.

Hébergement de canaux spécialisés dans les services Windows

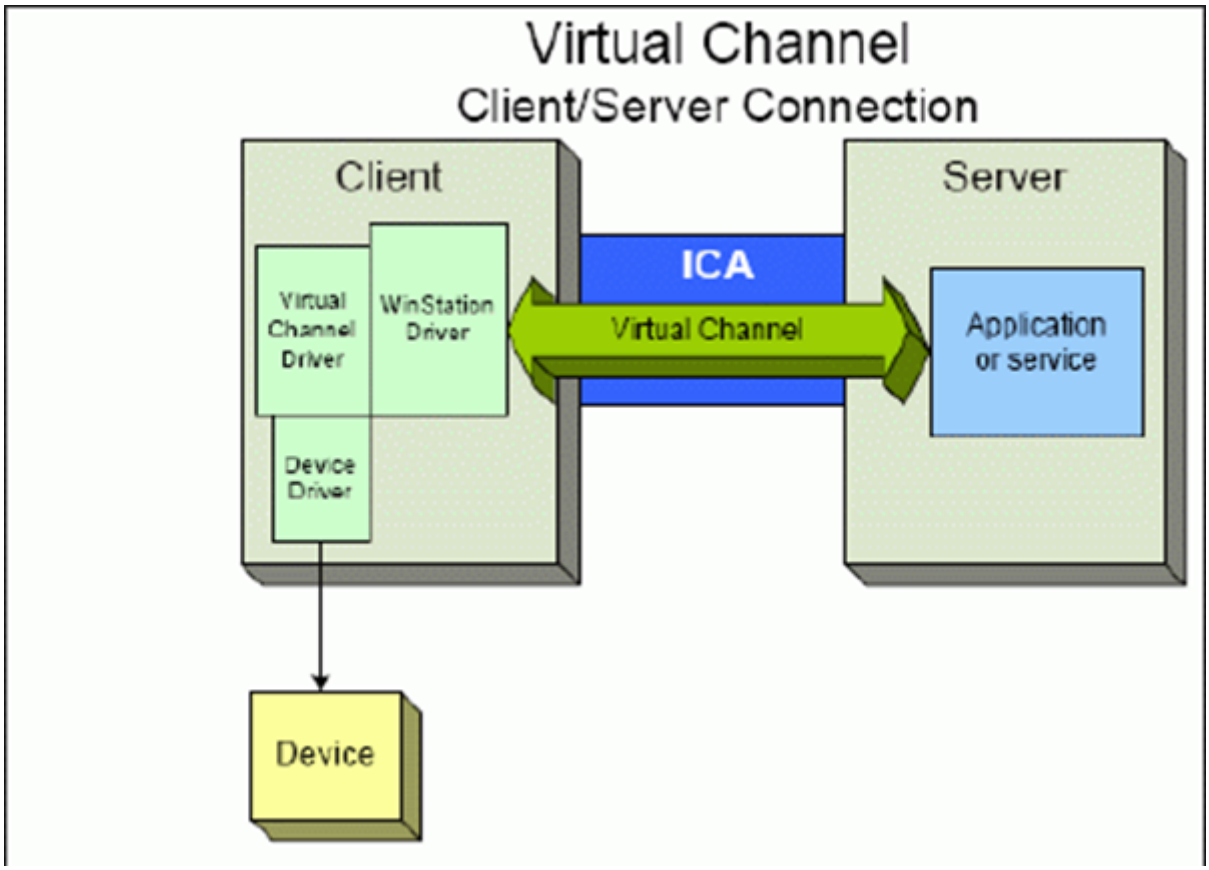
Sur les serveurs Citrix Virtual Apps and Desktops, différents canaux sont hébergés sous forme de services Windows. Ce type d'hébergement fournit une sémantique « one-to-many » pour plusieurs applications dans une session et plusieurs sessions sur le serveur. Voici des exemples de ces services :

- Citrix Device Redirector Service

- Citrix Dynamic Virtual Channel Service
- Citrix End User Experience Monitoring Service
- Citrix Location and Sensor Virtual Channel Service
- Citrix MultiTouch Redirection Service
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix Audio Redirection Service (Citrix Virtual Desktops uniquement)
- Service Citrix ICA Status Channel

Le canal virtuel audio sur Citrix Virtual Apps est hébergé à l'aide du service Windows Audio.

Côté serveur, tous les canaux virtuels client sont acheminés via le pilote WinStation, Wdica.sys. Côté client, le pilote WinStation correspondant, intégré dans wfica32.exe, interroge les canaux virtuels client. Cette image illustre la connexion client-serveur de canal virtuel.



Cette configuration contient un échange de données client-serveur utilisant un canal virtuel.

1. Le client se connecte au serveur Citrix Virtual Apps and Desktops. Le client transmet des informations sur les canaux virtuels qu'il prend en charge au serveur.
2. L'application côté serveur démarre, obtient un descripteur du canal virtuel et, éventuellement, demande des informations supplémentaires à propos du canal.

3. Le pilote virtuel client et l'application côté serveur transmettent les données en utilisant les deux méthodes suivantes :

    - Si l'application serveur a des données à envoyer au client, les données sont envoyées au client immédiatement. Lorsque le client reçoit les données, le pilote WinStation démultiplexe les données du canal virtuel à partir du flux ICA et les transmet immédiatement au pilote virtuel du client.
    - Si le pilote virtuel client a des données à envoyer au serveur, les données sont envoyées la prochaine fois que le pilote WinStation l'interroge. Lorsque le serveur reçoit les données, elles sont mises en file d'attente jusqu'à ce que l'application de canal virtuel les lise. Il n'y a aucun moyen d'alerter l'application de canal virtuel du serveur que des données ont été reçues.

4. Lorsque l'application de canal virtuel du serveur a terminé, elle ferme le canal virtuel et libère toutes les ressources allouées.

Création de votre propre canal virtuel à l'aide du SDK de canal virtuel

> **Remarque :**
>
> Les SDK Citrix sont disponibles sur le portail Citrix Developer à l'adresse https://developer.cloud.com.

La création d'un canal virtuel à l'aide du SDK de canal virtuel nécessite des connaissances intermédiaires en programmation. Utilisez cette méthode pour fournir un chemin de communication majeur entre le client et le serveur. Par exemple, si vous implémentez l'utilisation d'un périphérique côté client, tel qu'un analyseur, à utiliser avec un processus de la session.

> **Remarque :**
>
> - Le SDK de canal virtuel requiert le SDK WFAPI pour écrire sur le côté serveur du canal virtuel.
> - En raison de la sécurité renforcée pour Citrix Virtual Apps and Desktops, vous devez spécifier les canaux virtuels autorisés à ouvrir dans une session ICA. Pour de plus amples informations, consultez la section Paramètres de stratégie de liste d'autorisation des canaux virtuels.

Création de votre propre canal virtuel à l'aide du SDK d'objet client ICA

La création d'un canal virtuel à l'aide de l'objet client ICA (ICO) est plus facile que l'utilisation du SDK de canal virtuel. Utilisez l'objet ICO et créez un objet nommé dans votre programme à l'aide de la méthode **CreateChannels**.

> **Important :**
>
> En raison de la sécurité renforcée à compter de la version 10.00 de Citrix Receiver pour Windows et versions ultérieures (et des applications Citrix Workspace pour Windows), vous devez effectuer une étape supplémentaire lors de la création d'un canal virtuel ICO.

Fonctionnalité de transfert des canaux virtuels

La plupart des canaux virtuels que Citrix fournit fonctionnent sans modification lorsque vous utilisez l'application Citrix Workspace pour Windows dans une session ICA (également appelée session de transfert). Il y a des points à prendre en compte lors de l'utilisation du client dans des sauts supplémentaires.

Les fonctions suivantes fonctionnent de la même manière avec un ou plusieurs sauts :

- Mappage de port COM client
- Mappage des lecteurs clients
- Mappage d'imprimante client
- UPD client
- Surveillance de l'expérience utilisateur final
- USB générique
- Kerberos
- Support multimédia
- Prise en charge des cartes à puce
- Transfert de touche transparent
- Twain

Étant donné la nature inhérente de la latence et des facteurs tels que la compression, la décompression et le rendu qui se produisent à chaque saut, chaque saut supplémentaire du client peut avoir un effet sur les performances. Les éléments concernés sont les suivants :

- Audio bidirectionnel
- Transferts de fichiers
- Redirection USB générique
- Transparence
- Thinwire

> **Important :**
>
> Par défaut, les lecteurs client mappés par une instance du client exécutée dans une session de transfert sont limités aux lecteurs du client qui se connecte.

Fonctionnalité de transfert des canaux virtuels entre une session Citrix Virtual Desktop et une session Citrix Virtual App

La plupart des canaux virtuels que Citrix fournit fonctionnent sans modification lorsque vous utilisez l'application Citrix Workspace pour Windows dans une session ICA sur un serveur Citrix Virtual Desktops (également appelée session de transfert).

En particulier, sur le serveur Citrix Virtual Desktops, un hook de VDA exécute **picaPassthruHook**. Ce hook donne au client l'impression qu'il s'exécute sur un serveur CPS et place le client en mode de transfert traditionnel.

Nous prenons en charge les canaux virtuels traditionnels suivants ainsi que leurs fonctionnalités :

- Client
- Mappage de port COM client
- Mappage des lecteurs clients
- Mappage d'imprimante client
- USB générique (limité en raison des performances)
- Support multimédia
- Prise en charge des cartes à puce
- SSON
- Transfert de touche transparent

Canaux virtuels de sécurité et ICA

La sécurisation est un élément important de la planification, du développement et de la mise en œuvre des canaux virtuels. Vous trouverez plusieurs références à des aspects précis de la sécurité dans le présent document.

Recommandations

Ouvrez les canaux virtuels à la **connexion** et à la **reconnexion**. Fermez les canaux virtuels à la **déconnexion**.

Suivez ces conseils lorsque vous créez des scripts qui utilisent des fonctions de canal virtuel.

Nom des canaux virtuels :

Vous pouvez créer un maximum de 32 canaux virtuels. 17 des 32 canaux sont réservés à des utilisations spécifiques.

- Les noms des canaux virtuels ne doivent pas dépasser 7 caractères.

- Les 3 premiers caractères sont réservés au nom du fournisseur et les 4 suivants pour le type de canal. Par exemple, **CTXAUD** représente le canal virtuel audio Citrix.

Les canaux virtuels sont désignés par un nom ASCII de 7 caractères (ou moins). Dans certains versions précédentes du protocole ICA, les canaux virtuels étaient numérotés. Les numéros sont désormais attribués de façon dynamique en fonction du nom ASCII, ce qui facilite l'implémentation. Les utilisateurs qui développent le code de canaux virtuels réservés à un usage interne peuvent utiliser tout nom de 7 caractères qui n'entre pas en conflit avec des canaux virtuels existants. Utilisez uniquement des chiffres et des caractères ASCII. Suivez les conventions d'appellation suivantes lors de l'ajout de vos propres canaux virtuels. Il existe plusieurs canaux prédéfinis. Les canaux prédéfinis commencent par l'identifiant OEM CTX et sont utilisés uniquement par Citrix.

Prise en charge de double-hop :

Canal virtuel	Est-ce que le double-hop est pris en charge ?
Audio	Non
Redirection de contenu du navigateur	Non
CDM	Oui
CEIP	Non
Presse-papiers	Oui
Continuum (MRVC)	Non
Control VC	Oui
Redirection vidéo HTML5 (v1)	Oui
Clavier, Souris	Oui
Multipoint	Non
NSAPVC	Non
Impression	Oui
SensVC	Non
SmartCard	Oui
Twain	Oui
USB VC	Oui
Périphériques WAYCOM -K2M utilisant USB VC	Oui
Compression vidéo de webcam	Oui
Redirection Windows Media	Oui

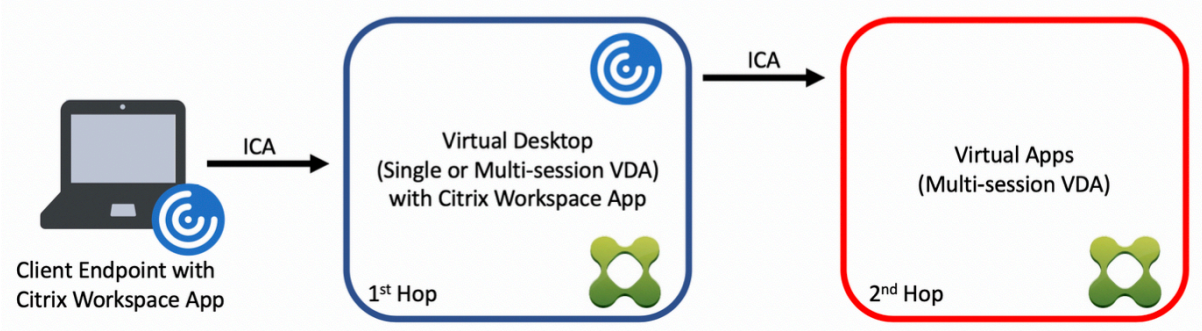
Voir aussi

- SDK du canal virtuel ICA
- Le réseau Citrix Developer Network héberge toutes les ressources techniques et toutes les discussions impliquant l'utilisation de SDK Citrix. Dans ce réseau, vous pouvez accéder aux SDK, obtenir des exemples de code et de scripts ainsi que des extensions et plug-ins et consulter la documentation SDK. Sont également inclus les forums Citrix Developer Network, où des discussions techniques ont lieu autour de chacun des kits SDK de Citrix.

Double saut dans Citrix Virtual Apps and Desktops

June 27, 2024

Dans le contexte d'une session client Citrix, le terme « double saut » fait référence à une session Citrix Virtual App qui s'exécute dans une session Citrix Virtual Desktop. Le diagramme suivant illustre un double saut.



Dans un scénario de double saut, lorsque l'utilisateur se connecte à un Citrix Virtual Desktop s'exécutant sur un VDA avec OS mono-session (connu sous le nom de VDI) ou un VDA avec OS multi-sessions (connu sous le nom de bureau publié), cette étape est considérée comme le premier saut. Une fois que l'utilisateur se connecte au bureau virtuel, il peut lancer une session Citrix Virtual Apps. Cette étape est considérée comme le deuxième saut.

Vous pouvez utiliser un modèle de déploiement double saut pour prendre en charge divers cas d'utilisation. Il est fréquent que les environnements Citrix Virtual Desktop et Citrix Virtual Apps soient gérés par différentes entités. Cette méthode peut également être efficace pour résoudre les problèmes de compatibilité des applications.

Configuration système requise

Toutes les éditions Citrix Virtual Apps and Desktops, y compris le service Citrix Cloud, prennent en charge le double saut.

Le premier saut doit utiliser une version prise en charge du VDA avec OS mono-session ou multi-sessions et de l'application Citrix Workspace. Le deuxième saut doit utiliser une version prise en charge du VDA avec OS multi-session. Consultez la page Tableau des produits pour connaître les versions prises en charge.

Pour des performances et une compatibilité optimales, Citrix recommande d'utiliser un client Citrix de la même version ou d'une version plus récente que les versions de VDA utilisées.

Dans les environnements où le premier saut implique une solution de bureau virtuel tierce (non Citrix) associée à une session Citrix Virtual Apps, la prise en charge est limitée à l'environnement Citrix Virtual Apps. En cas de problèmes liés au bureau virtuel tiers, notamment, mais sans s'y limiter, la compatibilité de l'application Citrix Workspace, la redirection de périphériques matériels et les performances de session, Citrix peut fournir un support technique limité. Un bureau virtuel Citrix au premier saut peut être requis dans le cadre du dépannage.

Considérations relatives au déploiement pour HDX en double saut

En général, chaque session dans un double saut est unique et les fonctions client-serveur sont isolées à un saut donné. Cette section inclut des éléments nécessitant une attention particulière de la part des administrateurs Citrix. Citrix recommande aux clients d'effectuer des tests approfondis des fonctionnalités HDX requises pour s'assurer que l'expérience utilisateur et les performances sont adéquates pour une configuration d'environnement donnée.

Graphiques

Utilisez les paramètres graphiques par défaut (codage sélectif) sur le premier et le deuxième sauts. Dans le cas de HDX 3D Pro, Citrix recommande fortement que toutes les applications qui nécessitent une accélération graphique s'exécutent localement au premier saut avec les ressources GPU appropriées disponibles pour le VDA.

Latence

La latence de bout en bout peut avoir un impact sur l'expérience utilisateur globale. Prenez en considération la latence ajoutée entre le premier et le deuxième sauts. Ceci est particulièrement important avec la redirection des périphériques matériels.

Multimédia

Le rendu côté serveur (en session) du contenu audio et vidéo fonctionne mieux dans le premier saut. La lecture vidéo dans le deuxième saut nécessite le décodage et le réencodage au premier saut, ce qui

augmente l'utilisation de la bande passante et des ressources matérielles. Le contenu audio et vidéo doit être limité au premier saut dans la mesure du possible.

Redirection de périphérique USB

HDX inclut des modes de redirection génériques et optimisés pour prendre en charge un large éventail de types de périphériques USB. Portez une attention particulière au mode utilisé à chaque saut et utilisez le tableau suivant comme référence pour obtenir les meilleurs résultats. Pour plus d'informations sur les modes de redirection génériques et optimisés, reportez-vous à la section Périphériques USB génériques.

Premier saut (VDI ou bureau publié)	Deuxième saut (Applications virtuelles)	Notes de support
Optimisé	Optimisé	Recommandé (en fonction des périphériques compatibles). Par exemple, stockage de masse USB, scanners TWAIN, webcam, audio.
Générique	Générique	Pour les périphériques pour lesquels l'option optimisée n'est pas disponible.
Générique	Optimisé	Si c'est techniquement possible, il est recommandé d'utiliser le mode optimisé sur les deux sauts lorsque le périphérique est pris en charge.
Optimisé	Générique	Non pris en charge

> **Remarque :**
>
> En raison du bavardage inhérent des protocoles USB, les performances peuvent diminuer d'un saut à l'autre. Les fonctionnalités et les résultats varient en fonction des exigences spécifiques du périphérique et de l'application. Des tests de validation sont fortement recommandés dans tous les cas de redirection de périphérique et particulièrement importants dans les scénarios de double saut.

Exceptions de prise en charge

Les sessions à double saut prennent en charge la plupart des fonctionnalités HDX, à l'exception des suivantes :

- Redirection de contenu du navigateur
- Local App Access
- Pack d'optimisation RealTime pour Skype Entreprise
- Optimisation pour Microsoft Teams

Installer et configurer

June 27, 2024

Consultez les articles référencés avant de démarrer chaque étape de déploiement, de façon à être informé sur ce que vous voyez et sélectionnez lors du déploiement.

Utilisez la séquence suivante pour déployer Citrix Virtual Apps and Desktops.

Préparer

Consultez Préparer l'installation et effectuez toutes les tâches nécessaires.

- Où trouver des informations sur les concepts, les fonctionnalités, les différences avec les versions antérieures, la configuration système requise et les bases de données.
- Considérations à prendre en compte lorsque vous choisissez où vous allez installer les composants principaux.
- Autorisations et configuration Active Directory requise.
- Informations sur les programmes d'installation, outils et interfaces disponibles.

Installer les composants principaux

Installez le Delivery Controller, Web Studio, Citrix Director et le serveur de licences Citrix . Vous pouvez également installer Citrix StoreFront. Pour de plus amples informations, consultez Installer les composants principaux ou Installer à l'aide de la ligne de commande.

Créer un site

Après avoir installé les composants principaux et démarré Studio, vous êtes invité à créer un site.

Installer un ou plusieurs Virtual Delivery Agents (VDA)

Installez un VDA sur une machine exécutant un système d'exploitation Windows, soit sur une image principale soit directement sur chaque machine. Consultez Installer des VDA ou Installer à l'aide de la ligne de commande. Des exemples de scripts sont fournis si vous souhaitez installer des VDA à l'aide d'Active Directory.

Pour les machines avec un système d'exploitation Linux, suivez les instructions dans Virtual Delivery Agent Linux.

Pour un déploiement Remote PC Access, installez un VDA pour OS mono-session sur chaque PC de bureau. Si vous n'avez besoin que des services VDA principaux, utilisez le programme d'installation `VDAWorkstationCoreSetup.exe` autonome et vos méthodes ESD (distribution électronique de logiciels) existantes. (Préparer l'installation décrit les programmes d'installation de VDA disponibles.)

Installer les composants facultatifs

Si vous prévoyez d'utiliser le serveur d'impression universelle Citrix, installez son composant serveur sur vos serveurs d'impression. Consultez Installer les composants principaux ou Installer à l'aide de la ligne de commande.

Pour permettre à StoreFront d'utiliser des options d'authentification telles que les assertions SAML, installez le Service d'authentification fédérée de Citrix.

Pour donner aux utilisateurs un plus grand contrôle sur leurs comptes d'utilisateur, installez la réinitialisation en libre-service des mots de passe.

Si vous le souhaitez, vous pouvez intégrer d'autres composants Citrix dans votre déploiement Citrix Virtual Apps and Desktops.

- Citrix Provisioning est un composant facultatif qui provisionne les machines en livrant en streaming une image principale vers les machines cibles.
- Citrix Gateway est une solution garantissant un accès sécurisé aux applications. Grâce à des stratégies de contrôle d'accès et d'action avancées, elle permet aux administrateurs de renforcer l'accès aux applications et données.
- Citrix SD-WAN est un ensemble d'appliances qui permet d'optimiser les performances du réseau étendu.

Créer un catalogue de machines

Lorsque vous créez un site dans Studio, vous êtes guidé dans la création d'un catalogue de machines.

Un catalogue peut contenir des machines physiques ou virtuelles (VM). Les machines virtuelles peuvent être créées à partir d'une image principale. Si vous utilisez un hyperviseur ou autre service pour fournir des machines virtuelles, vous créez d'abord une image principale sur cet hôte. Ensuite, lorsque vous créez le catalogue, vous spécifiez cette image, qui est utilisée lors de la création de machines virtuelles.

Créer un groupe de mise à disposition

Lorsque vous créez votre premier catalogue de machines dans Web Studio, vous êtes guidé dans la création d'un groupe de mise à disposition.

Un groupe de mise à disposition spécifie quels utilisateurs peuvent accéder aux machines dans un catalogue spécifique et les applications disponibles pour ces utilisateurs.

Créer un groupe d'applications (facultatif)

Lorsque vous créez un groupe de mise à disposition, vous pouvez également créer un groupe d'applications. Vous pouvez créer des groupes d'applications pour les applications qui sont partagées entre différents groupes de mise à disposition ou utilisées par un sous-ensemble d'utilisateurs au sein de groupes de mise à disposition.

Limitation connue

Lorsque vous utilisez l'application Citrix Workspace pour Windows version 1912 ou antérieure, la session est interrompue au bout d'un moment. Ce problème est résolu dans les nouvelles versions LTSR et CR de l'application Citrix Workspace.
Pour plus d'informations sur les versions prises en charge, consultez Application Citrix Workspace pour Windows/Citrix Receiver pour Windows Long Term Service Releases.

Identités des machines

June 27, 2024

Chaque machine doit avoir une identité de machine unique, également appelée compte d'ordinateur. Les identités de machine peuvent être créées et gérées sur les machines localement ou dans un annuaire, comme Active Directory (AD) sur site ou Azure AD. Citrix prend en charge l'hébergement d'applications et de bureaux virtuels sur des machines jointes à Active Directory, à Azure Active Directory, à Azure Active Directory Hybride ou des machines non jointes à un domaine.

Types d'identité de machines

Les types d'identité de machine suivants sont pris en charge.

Type d'identité de machine	Description
Joint à AD	Les identités sont créées et gérées dans Active Directory sur site. Les machines provisionnées sont jointes à Active Directory sur site à l'aide des identités de machine attribuées.
Joint à Azure AD Hybride	Les identités sont créées dans Active Directory sur site et synchronisées avec Azure AD via Azure AD Connect. Les machines provisionnées sont jointes à Active Directory sur site. Les machines sont ensuite jointes à Azure AD Hybride. Pour l'importation d'une machine virtuelle hybride jointe à Azure AD, la machine virtuelle est traitée comme une machine virtuelle jointe à Active Directory par Citrix Virtual Apps and Desktops.

Configurations prises en charge

Vous trouverez ci-dessous des informations détaillées sur les configurations prises en charge pour chaque scénario.

Infrastructure prise en charge

Identité de la machine	Citrix Virtual Apps and Desktops	Citrix Workspace	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
Joint à AD	Oui	Oui	Oui	Oui	Oui
Joint à Azure AD	Non	Oui	Non	Oui	Non
Joint à Azure AD Hybride	Oui	Oui	Oui	Oui	Oui
Non joint au domaine	Non	Oui	Non	Oui	Non

Fournisseurs d'identité d'authentification d'espace de travail pris en charge

Identité de la machine	Azure Active Directory	Active Directory	Active Directory et jeton	Okta	SAML	Citrix Gateway	Authentification adaptative
Joint à AD	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Joint à Azure AD	Oui	Non	Non	Non	Non	Non	Non
Joint à Azure AD Hybride	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Non joint au domaine	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Joint à Active Directory

June 27, 2024

Active Directory est requis pour l'authentification et l'autorisation. L'infrastructure Kerberos dans Active Directory est utilisée pour garantir l'authenticité et la confidentialité des communications avec les Delivery Controller. Pour de plus amples informations sur Kerberos, veuillez consulter la documentation Microsoft.

L'article Configuration système requise répertorie les niveaux fonctionnels pris en charge de la forêt et du domaine. Pour utiliser la modélisation de stratégie, le contrôleur de domaine doit s'exécuter sur Windows Server 2003 à Windows Server 2012 R2. Cela n'affecte pas le niveau fonctionnel du domaine.

Ce produit prend en charge ce qui suit :

- **Déploiements dans lesquels les comptes d'utilisateurs et les comptes d'ordinateurs existent dans les domaines d'une forêt Active Directory unique.** Les comptes d'utilisateurs et d'ordinateurs peuvent exister dans des domaines arbitraires d'une forêt unique. Tous les niveaux fonctionnels de domaine et de forêt sont pris en charge dans ce type de déploiement.
- **Déploiements dans lesquels les comptes d'utilisateurs existent dans une forêt Active Directory qui est différente de celle contenant les comptes d'ordinateurs des Controller et**

des bureaux virtuels. Dans ce type de déploiement, les domaines contenant les comptes d'ordinateurs des contrôleurs et des bureaux virtuels doivent établir l'approbation des domaines dans lesquels figurent les comptes d'utilisateurs. Des approbations de forêt ou des approbations externes peuvent être utilisées. Tous les niveaux fonctionnels de domaine et de forêt sont pris en charge dans ce type de déploiement.

- **Déploiements dans lesquels les comptes d'ordinateurs des contrôleurs figurent dans une forêt Active Directory différente d'une ou de plusieurs forêts Active Directory supplémentaires contenant les comptes d'ordinateurs des bureaux virtuels.** Dans ce type de déploiement, une approbation bilatérale doit exister entre les domaines contenant les comptes d'ordinateurs des contrôleurs et l'ensemble des domaines contenant les comptes d'ordinateurs des bureaux virtuels. Dans ce type de déploiement, tous les domaines contenant les comptes d'ordinateurs des contrôleurs ou des bureaux virtuels doivent figurer au niveau fonctionnel « natif de Windows 2000 » ou supérieur. Tous les niveaux fonctionnels de forêt sont pris en charge.
- **Contrôleurs de domaine accessibles en écriture.** Les contrôleurs de domaine en lecture seule ne sont pas pris en charge.

Facultativement, les VDA (Virtual Delivery Agents) peuvent utiliser des informations publiées dans Active Directory pour déterminer les Controller avec lesquels ils peuvent s'enregistrer (découverte). Cette méthode est principalement prise en charge pour la rétrocompatibilité, et est uniquement disponible si les VDA se trouvent dans la même forêt Active Directory que les Controller. Pour de plus amples informations sur cette méthode de découverte, consultez Découverte basée sur unité d'organisation Active Directory et l'article CTX118976.

> **Remarque :**
>
> Ne modifiez pas le nom de l'ordinateur ou l'appartenance à un domaine d'un Delivery Controller une fois que le site est configuré.

Déployer dans un environnement Active Directory avec des forêts multiples

Dans un environnement Active Directory avec plusieurs forêts, si des approbations à sens unique ou bidirectionnelles sont en place, vous pouvez utiliser les redirecteurs DNS ou conditionnels pour la recherche de nom et l'enregistrement. Pour autoriser les utilisateurs Active Directory appropriés à créer des comptes d'ordinateurs, utilisez l'Assistant Délégation de contrôle. Reportez-vous à la documentation Microsoft pour plus d'informations sur cet assistant.

Aucune zone DNS inversée n'est nécessaire dans l'infrastructure DNS si des redirecteurs DNS appropriés sont en place entre les forêts.

La clé `SupportMultipleForest` n'est nécessaire que si le VDA et le Controller se trouvent dans des forêts différentes que les noms Active Directory et NetBIOS soient différents ou non. Utilisez les

informations suivantes pour ajouter la clé de registre au VDA et aux Delivery Controller :

> **Attention :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

Sur le VDA, configurez : `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`.

- Nom : `SupportMultipleForest`
- Type : `REG_DWORD`
- Données : `0x00000001 (1)`

Sur tous les Delivery Controller, configurez : `HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`.

- Nom : `SupportMultipleForest`
- Type : `REG_DWORD`
- Données : `0x00000001 (1)`

Vous aurez peut-être besoin d'utiliser une configuration DNS inversée si l'espace de noms DNS est différent de celui d'Active Directory.

Une entrée de registre a été ajoutée pour éviter l'activation indésirable de l'authentification NTLM dans les VDA, qui est moins sécurisé que Kerberos. Cette entrée peut être utilisée à la place de l'entrée `SupportMultipleForest`, qui peut toujours être utilisée pour la rétrocompatibilité.

Sur le VDA, configurez : `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgen`

.

- Nom : `SupportMultipleForestDdcLookup`
- Type : `REG_DWORD`
- Données : `0x00000001 (1)`

Cette clé de registre effectue une recherche DDC dans un environnement avec plusieurs forêts impliquant des approbations bidirectionnelles, ce qui vous permet de supprimer l'authentification basée sur NTLM pendant le processus d'enregistrement initial.

Si des approbations externes sont en place au cours de l'installation, la clé de registre `ListOfSIDs` est requise. La clé de registre `ListOfSIDs` est également nécessaire si le nom de domaine complet (FQDN) Active Directory est différent du FQDN DNS ou si le domaine contenant le contrôleur de

domaine porte un nom NetBIOS autre que le FQDN Active Directory. Pour ajouter la clé de registre, utilisez les informations suivantes :

Pour le VDA, recherchez la clé de registre `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`.

- Nom : `ListOfSIDs`
- Type : `REG_SZ`
- Données : identificateur de sécurité (SID) des Controller (Les SID sont inclus dans les résultats de l'applet de commande `Get-BrokerController`.)

Lorsque des approbations externes sont en place, apportez la modification suivante sur le VDA :

1. Localisez le fichier `Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config`.
2. Créez une copie de sauvegarde du fichier.
3. Ouvrez le fichier dans un éditeur de texte tel que le Bloc-notes.
4. Localisez le texte `allowNtlm="false"` et modifiez le texte vers `allowNtlm="true"`.
5. Enregistrez le fichier.

Après l'ajout de la clé de registre `ListOfSIDs` et la modification du fichier `brokeragent.exe.config`, redémarrez le service Citrix Desktop pour appliquer les modifications.

Le tableau suivant dresse la liste des types de prise en charge de l'approbation :

Type d'approbation	Transitivité	Direction	Pris en charge dans cette version
Parent et enfant	Transitive	Bidirectionnelle	Oui
Racine d'arborescence	Transitive	Bidirectionnelle	Oui
Externe	Non transitive	Unidirectionnelle ou bidirectionnelle	Oui
Forêt	Transitive	Unidirectionnelle ou bidirectionnelle	Oui
Raccourci	Transitive	Unidirectionnelle ou bidirectionnelle	Oui
Domaine	Transitive ou non transitive	Unidirectionnelle ou bidirectionnelle	Non

Pour de plus amples informations sur les environnements Active Directory complexes, consultez l'article CTX134971.

Joint à Azure Active Directory Hybride

June 27, 2024

> **Remarque :**
>
> Depuis juillet 2023, Microsoft a renommé Azure Active Directory (Azure AD) Microsoft Entra ID. Dans ce document, toute occurrence de l'appellation Azure Active Directory, Azure AD ou de l'acronyme AAD fait désormais référence à Microsoft Entra ID.

Cet article décrit les conditions requises pour créer des catalogues joints à Azure Active Directory Hybride (HAAD) à l'aide de Citrix DaaS, en plus des exigences décrites dans la section Configuration système requise pour Citrix DaaS.

Les machines jointes à Azure AD Hybride utilisent AD sur site comme fournisseur d'authentification. Vous pouvez les attribuer à des utilisateurs ou à des groupes de domaine dans AD sur site. Pour permettre une expérience d'authentification unique transparente dans Azure AD, vous devez synchroniser les utilisateurs de domaine avec Azure AD.

> **Remarque :**
>
> Les machines virtuelles jointes à Azure AD Hybride sont prises en charge dans les infrastructures d'identité fédérées et gérées.

Exigences

- Type de VDA : mono-session (bureaux uniquement) ou multisession (applications et bureaux)
- Version de VDA : 2212 ou ultérieure
- Type de provisioning : Machine Creation Services (MCS) persistant et non persistant
- Type d'affectation : dédié et regroupé
- Plate-forme d'hébergement : tout hyperviseur ou service cloud

Limitations

- Si le service d'authentification fédérée de Citrix (FAS) est utilisé, l'authentification unique (Single Sign-On) est dirigée vers le domaine AD local plutôt que vers Azure AD. Dans ce cas, il est recommandé de configurer l'authentification basée sur les certificats Azure AD afin que le jeton d'actualisation principal (PRT) soit généré lors de la connexion de l'utilisateur, ce qui facilite l'authentification unique aux ressources Azure AD au sein de la session. Sinon, le PRT ne sera pas présent et l'authentification unique aux ressources Azure AD ne fonctionnera pas. Pour plus d'informations sur la mise en place de l'authentification unique (SSO) Azure AD sur des VDA

joints hybrides à l'aide du service d'authentification fédérée (FAS) Citrix, consultez la section VDA joints hybrides.

- N'ignorez pas la préparation des images lors de la création ou de la mise à jour des catalogues de machines. Si vous souhaitez ignorer la préparation des images, assurez-vous que les VM principales ne sont pas jointes à Azure AD ou à Azure AD Hybride.

Considérations

- La création de machines hybrides jointes à Azure Active Directory requiert l'autorisation `Write userCertificate` dans le domaine cible. Assurez-vous de saisir les informations d'identification d'un administrateur disposant de cette autorisation lors de la création du catalogue.
- Le processus Azure AD Hybride est géré par Citrix. Vous devez désactiver le paramètre `autoWorkplaceJoin` contrôlé par Windows dans les VM principales comme suit. La désactivation manuelle de `autoWorkplaceJoin` est requise uniquement pour la version 2212 ou antérieure du VDA.

  1. Exécutez `gpedit.msc`.
  2. Accédez à **Configuration ordinateur > Modèles d'administration > Composants Windows > Enregistrement d'appareil**.
  3. Définissez **Enregistrer les ordinateurs appartenant à un domaine en tant qu'appareils** sur **Désactivé**.

- Sélectionnez l'unité d'organisation (UO) configurée pour être synchronisée avec Azure AD lorsque vous créez les identités de machine.
- Pour la machine virtuelle principale basée sur Windows 11 22H2 : créez une tâche planifiée dans la machine virtuelle principale qui exécute la commande suivante au démarrage du système à l'aide du compte système. Cette planification de tâche dans la machine virtuelle principale n'est requise que pour la version 2212 ou antérieure du VDA.

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'
$WorkplaceJoinKeyPath = 'HKLM:\SOFTWARE\Policies\Microsoft\
   Windows\WorkplaceJoin'
$MaxCount = 60

for ($count = 1; $count -le $MaxCount; $count++)
{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)
  {

    $provider = (Get-Item -Path $VirtualDesktopKeyPath).GetValue(
       "Provider", $null)
    if ($provider -eq 'Citrix')
    {
```



```
14
15          break;
16       }
17
18
19      if ($provider -eq 1)
20      {
21
22          Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
                Provider" -Value "Citrix" -Force
23          Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
                autoWorkplaceJoin" -Value 1 -Force
24          Start-Sleep 5
25          dsregcmd /join
26          break
27       }
28
29     }
30
31
32    Start-Sleep 1
33   }
34
35  <!--NeedCopy-->
```

Autres ressources

Pour plus d'informations sur la création de catalogues joints à Azure Active Directory Hybride, voir Créer des catalogues joints à Azure Active Directory Hybride.

Préparer l'installation

June 27, 2024

Le déploiement de Citrix Virtual Apps and Desktops commence par l'installation des composants suivants. Ce processus prépare la mise à disposition d'applications et de bureaux auprès des utilisateurs se trouvant au sein de votre pare-feu.

- Un ou plusieurs Delivery Controller
- Citrix Director
- Citrix StoreFront
- Serveur de licences Citrix
- Un ou plusieurs Citrix Virtual Delivery Agents (VDA)
- Composants et technologies facultatifs tels que le serveur d'impression universelle, le service d'authentification fédérée et la réinitialisation en libre-service des mots de passe

Pour les utilisateurs en dehors de votre pare-feu, installez et configurez un composant supplémentaire, tel que Citrix Gateway. Pour en savoir plus, voir Intégrer Citrix Virtual Apps and Desktops avec Citrix Gateway.

> **Remarque :**
>
> Assurez-vous que les conditions préalables Microsoft suivantes sont remplies sur le système d'exploitation du serveur et sur celui du poste de travail :
>
> - Les services Microsoft **Volume Shadow Copy** et **Microsoft Software Shadow Copy Provider** sont en cours d'exécution. Pour plus d'informations, consultez Volume Shadow Copy Service.
> - La version de **MS-Defender** doit être supérieure à la version 4.18.2105.5. Pour plus d'informations, consultez la page Microsoft Defender Antivirus security intelligence et mises à jour des produits.

Si votre déploiement inclut des charges de travail Windows Server, configurez un serveur de licences Microsoft RDS.

Vous pouvez utiliser le programme d'installation du produit entier sur l'image ISO du produit pour déployer plusieurs composants et technologies. Vous pouvez utiliser un programme d'installation de VDA autonome pour installer les VDA. Les programmes d'installation de VDA autonomes sont disponibles sur le site de téléchargement de Citrix. Tous les programmes d'installation offrent des interfaces graphique et de ligne de commande. Voir Programmes d'installation.

L'ISO du produit contient des exemples de scripts qui permettent d'installer, mettre à niveau ou supprimer les VDA pour les machines dans un annuaire Active Directory. Vous pouvez également utiliser les scripts pour gérer les images utilisées par Machine Creation Services (MCS) et Citrix Provisioning (anciennement Provisioning Services). Pour de plus amples informations, consultez Installer les VDA à l'aide de scripts.

Informations à consulter avant l'installation

- Vue d'ensemble technique : pour vous familiariser avec le produit et ses composants.
- Sécurité : lors de la planification de votre environnement de déploiement.
- Problèmes connus : problèmes que vous pourriez rencontrer dans cette version.
- Bases de données : pour en apprendre davantage sur les bases de données du système et leur configuration. Lors de l'installation du Controller, vous pouvez installer SQL Server Express pour l'utiliser en tant que base de données du site. Vous configurez la plupart des informations de base de données lorsque vous créez un site, après avoir installé les composants principaux.
- Remote PC Access : si vous déployez un environnement qui permet à vos utilisateurs d'accéder à distance à leurs machines physiques de bureau.

- Connexions et ressources : si vous utilisez un hyperviseur ou un autre service pour héberger ou provisionner des machines virtuelles pour les applications et bureaux. Vous pouvez configurer la première connexion lorsque vous créez un site (après avoir installé les composants principaux). Configurez votre environnement de virtualisation au préalable.
- Microsoft System Center Configuration Manager : si vous utilisez ConfigMgr pour gérer l'accès aux applications et bureaux, ou si vous utilisez la fonctionnalité Wake-on-LAN avec Remote PC Access.
- **Connexions hôtes de cloud public :** si vous disposez d'une licence de droits hybrides, vous pouvez créer des connexions hôtes de cloud public. Pour plus d'informations sur la licence de droits hybrides, consultez Renouvellements de droits hybrides. Pour plus d'informations sur les droits d'accès au cloud public et la raison de ce changement, consultez CTX270373.

Emplacement d'installation des composants

ConsultezConfiguration système requisepour connaître les plates-formes, systèmes d'exploitation et versions pris en charge. Les composants requis sont installés automatiquement, sauf indication contraire. Consultez la documentation relative à Citrix StoreFront et au serveur de licences Citrix pour connaître les plates-formes prises en charge et les composants requis.

Vous pouvez installer les composants principaux sur le même serveur ou sur des serveurs différents.

- L'installation de tous les composants principaux sur un seul serveur peut fonctionner pour les déploiements d'évaluation, de test ou de production de petite taille.
- Il est peut être avisé d'installer les composants sur des serveurs différents en prévision d'une expansion future. Par exemple, l'installation de Studio sur une autre machine que le serveur sur lequel vous avez installé le Controller vous permet de gérer le site à distance.
- Pour la plupart des déploiements de production, l'installation des composants principaux sur des serveurs distincts est recommandée.

  Installez le serveur de licences Citrix et les licences avant d'installer d'autres composants sur d'autres serveurs.
- Pour installer un composant pris en charge sur un système d'exploitation Server Core (tel qu'un Delivery Controller), vous devez utiliser la ligne de commande. Ce type de système d'exploitation n'offre pas d'interface graphique. Installez donc Studio et les autres outils ailleurs, puis pointez-les vers le serveur Controller.

Vous pouvez installer un Delivery Controller et un VDA pour OS multi-session sur le même serveur. Lancez le programme d'installation et sélectionnez le Delivery Controller (ainsi que tout autre composant principal que vous souhaitez sur cette machine). Ensuite, lancez de nouveau le programme d'installation et sélectionnez le **Virtual Delivery Agent** pour OS multi-session.

Assurez-vous que chaque système d'exploitation dispose des dernières mises à jour.

Assurez-vous que les horloges système de toutes les machines sont synchronisées. L'infrastructure Kerberos qui sécurise la communication entre les machines requiert une synchronisation.

Si vous utilisez XenServers, l'état de puissance de la machine virtuelle peut apparaître comme inconnu même si la machine s'affiche comme enregistrée. Pour résoudre ce problème, modifiez la valeur de la clé de Registre `HostTime` pour désactiver la synchronisation de l'heure avec l'hôte :

```
HKEY_LOCAL_MACHINE\Software\Citrix\XenTools\HostTime="Local"
```

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\XenTools\HostTime="
Local"
```

> **Conseil :**
>
> La valeur par défaut est `HostTime="UTC"`. Réglez cette valeur sur autre chose que UTC, par exemple, `Local`. Cette modification désactive efficacement la synchronisation de l'heure avec l'hôte.

Le guide d'optimisation pour les machines mono-session Windows 10 est disponible dans l'article CTX216252.

Emplacements d'installation des composants non pris en charge

- N'installez pas les composants sur un contrôleur de domaine Active Directory.
- L'installation d'un Controller sur un nœud dans une installation de mise en cluster SQL Server, de mise en miroir SQL Server ou sur un serveur exécutant Hyper-V n'est pas prise en charge.

Si vous essayez d'installer ou de mettre à niveau un VDA sur un système d'exploitation Windows que cette version de produit ne prend pas en charge, un message vous guide vers un article décrivant les options.

Autorisations et configuration Active Directory requise

Vous devez être un utilisateur du domaine et un administrateur local sur les machines sur lesquelles vous installez les composants.

Pour utiliser le programme d'installation de VDA autonome, vous devez disposer de privilèges d'administrateur ou utiliser **Exécuter en tant qu'administrateur**.

Configurez votre domaine Active Directory avant de procéder à l'installation.

- La section Configuration système requise répertorie les niveaux fonctionnels d'Active Directory pris en charge. Joint à Active Directory contient plus d'informations.
- Vous devez disposer d'au moins un contrôleur de domaine exécutant les services de domaine Active Directory.

- N'installez aucun composant Citrix Virtual Apps and Desktops sur un contrôleur de domaine.
- N'utilisez pas de barre oblique (/) lorsque vous spécifiez les noms d'unité d'organisation dans Studio.

Le compte d'utilisateur Windows utilisé pour installer le serveur de licences Citrix est automatiquement configuré en tant qu'administrateur complet d'administration déléguée.

Informations supplémentaires :

- Bonnes pratiques en matière de sécurité
- Administration déléguée
- Documentation Microsoft sur la configuration d'Active Directory

Instructions d'installation, considérations et meilleures pratiques

Lors de l'installation d'un composant

- Lors de l'installation ou de la mise à niveau de Delivery Controller, Studio, Serveur de licences ou Director à partir du support du produit complet, si le programme d'installation Citrix détecte qu'un redémarrage est en attente depuis une installation Windows précédente sur l'ordinateur, le programme d'installation s'arrête avec le code de sortie/retour 9. Vous êtes invité à redémarrer la machine.

  Il ne s'agit pas d'un redémarrage forcé Citrix. Cela est dû à d'autres composants installés plus tôt sur la machine. Si cela se produit, redémarrez la machine, puis relancez le programme d'installation Citrix.

  Lorsque vous utilisez l'interface de ligne de commande, vous pouvez empêcher la vérification du redémarrage en attente en incluant l'option `/no_pending_reboot_check` dans la commande.

- En général, si un composant requiert certains éléments, le programme d'installation déploie ces derniers s'ils ne sont pas présents. Certains éléments requis peuvent nécessiter un redémarrage de la machine.

- Lorsque vous créez des objets avant, pendant et après l'installation, spécifiez des noms uniques pour chaque objet. Par exemple, fournissez des noms uniques pour les réseaux, groupes, catalogues et ressources.

- Si un composant n'est pas installé correctement, l'installation s'arrête et un message d'erreur s'affiche. Les composants installés correctement sont conservés. Vous n'avez pas besoin de les réinstaller.

- Des données d'analyse Citrix Analytics sont collectées lorsque vous installez (mettez à niveau) les composants. Par défaut, ces données sont téléchargées automatiquement vers Citrix

lorsque l'installation est terminée. Par ailleurs, lorsque vous installez des composants, vous êtes automatiquement inscrit au Programme d'amélioration de l'expérience utilisateur Citrix (CEIP), qui télécharge des données anonymes.

Lors de l'installation, vous pouvez également choisir de participer à d'autres technologies Citrix qui collectent les diagnostics pour le dépannage et la maintenance. Pour de plus amples informations sur ces programmes, consultez Citrix Insight Services.

- Les données Google Analytics sont automatiquement collectées (et chargées plus tard) lorsque vous installez (ou mettez à niveau) Studio. Après l'installation de Studio, vous pouvez modifier ce paramètre avec la clé de Registre `HKLM\Software\Citrix\DesktopStudio\GAEnabled`. La valeur **1** active la collecte et le chargement, **0** désactive la collecte et le chargement.
- Si une installation de VDA échoue, un analyseur MSI analyse le journal du MSI défaillant, affichant le code d'erreur exact. L'analyseur suggère un article CTX, s'il s'agit d'un problème connu. L'analyseur recueille également des données anonymes sur le code d'erreur de la défaillance. Ces données sont incluses avec d'autres données collectées par le programme CEIP. Si vous annulez l'inscription au CEIP, les données de l'analyseur MSI collectées ne sont plus envoyées à Citrix.

Lors de l'installation de VDA

- L'application Citrix Workspace pour Windows est disponible mais n'est pas installée par défaut lorsque vous installez un VDA. Vous ou vos utilisateurs pouvez télécharger et installer (et mettre à niveau) les versions ultérieures de l'application Citrix Workspace pour Windows et d'autres applications Citrix Workspace à partir du site Web de Citrix. Vous pouvez aussi mettre à disposition ces applications Citrix Workspace à partir de votre serveur StoreFront. Pour plus d'informations, consultez la documentation StoreFront.
- Le service de spouleur d'impression Microsoft doit être activé. Vous ne pourrez pas correctement installer un VDA si ce service est désactivé.
- La plupart des éditions Windows prises en charge sont fournies avec Microsoft Media Foundation. Si la machine ne dispose pas de Media Foundation (éditions N par exemple), plusieurs fonctionnalités multimédia ne sont pas installées et ne fonctionnent pas.
  - Redirection Windows Media
  - Redirection vidéo HTML5
  - Redirection de webcam HDX RealTime

  Vous pouvez accepter cette limitation, ou mettre fin à l'installation du VDA et la redémarrer plus tard, après l'installation de Media Foundation. Dans l'interface graphique, ce choix

est présenté dans un message. Dans la ligne de commande, vous pouvez utiliser l'option `/no_mediafoundation_ack` pour confirmer la limitation.

- Lorsque vous installez le VDA, un nouveau groupe d'utilisateurs locaux appelé **Direct Access Users** est créé automatiquement. Sur un VDA pour OS mono-session, ce groupe s'applique uniquement aux connexions RDP. Sur un VDA pour OS multi-session, ce groupe s'applique aux connexions ICA et RDP.
- Le VDA doit avoir des adresses Controller valides avec lesquelles communiquer. Sinon, les sessions ne peuvent pas être établies. Vous pouvez spécifier les adresses Controller lorsque vous installez le VDA ou ultérieurement. Notez que cette opération est indispensable. Pour plus d'informations, consultez la section Enregistrement de VDA.

Outils de prise en charge VDA

Chaque programme d'installation VDA inclut un MSI de prise en charge qui contient des outils Citrix pour vérifier les performances du VDA, telles que son intégrité globale et la qualité des connexions. Activez ou désactivez l'installation de ce fichier MSI sur la page **Composants supplémentaires** de l'interface graphique du programme d'installation VDA. À partir de la ligne de commande, vous pouvez désactiver l'installation avec l'option `/exclude "Citrix Supportability Tools"`.

Par défaut, le fichier MSI de prise en charge est installé dans `c:\Program Files (x86)\Citrix\Supportability Tools\`. Vous pouvez modifier cet emplacement sur la page **Composants** de l'interface graphique du programme d'installation VDA ou avec l'option de ligne de commande `/installdir`. Notez que la modification de l'emplacement modifie l'emplacement pour tous les composants VDA installés, pas seulement pour les outils de prise en charge.

Outils actuels dans le MSI de prise en charge :

- Assistant d'intégrité Citrix : pour plus de détails, consultezCTX207624.
- Utilitaire de nettoyage de VDA : pour plus de détails, voir l'articleCTX209255.

Si vous n'installez pas les outils lorsque vous installez le VDA, l'article CTX contient un lien vers le pack de téléchargement actuel.

Redémarrages après et lors de l'installation de VDA

Un redémarrage est requis à la fin de l'installation du VDA. Ce redémarrage se produit automatiquement par défaut.

Un redémarrage se produit lors de la mise à niveau d'un VDA vers la version 7.17 (ou une version ultérieure prise en charge). Cela ne peut pas être évité.

Pour minimiser le nombre de redémarrages requis durant l'installation de VDA :

- Assurez-vous qu'une version de .NET Framework prise en charge est installée avant d'installer le VDA.
- Pour les machines équipées d'un OS multi-session Windows, installez et activez les services de rôle RDS avant d'installer le VDA.

Si vous n'installez pas les composants requis avant d'installer le VDA :

- Si vous utilisez l'interface graphique ou l'interface de ligne de commande sans l'option `/noreboot`, la machine redémarre automatiquement après l'installation des composants requis.
- Si vous utilisez l'interface de ligne de commande avec l'option `/noreboot`, vous devez lancer le redémarrage.

Un redémarrage se produit lors de la mise à niveau d'une version de VDA. Cela ne peut pas être évité.

Restauration en cas d'échec de l'installation ou de la mise à niveau

> **Remarque :**
>
> Cette fonctionnalité est disponible pour les VDA mono-session et multi-session.

Si l'installation ou la mise à niveau d'un VDA mono-session échoue et que la fonctionnalité « restauration en cas d'échec » est activée, l'ordinateur est renvoyé à un point de restauration défini avant le début de l'installation ou de la mise à niveau.

Si l'installation ou la mise à niveau d'un VDA multi-session échoue et que la fonctionnalité « restauration en cas d'échec » est activée, l'ordinateur est renvoyé à une sauvegarde effectuée avant le début de l'installation ou de la mise à niveau.

Lorsqu'une installation ou une mise à niveau de VDA mono-session démarre avec cette fonctionnalité activée, le programme d'installation crée un point de restauration du système avant de commencer l'installation ou la mise à niveau. Si l'installation ou la mise à niveau du VDA échoue, l'ordinateur est renvoyé à l'état du point de restauration. Le dossier `%temp%/Citrix` contient des journaux de déploiement et d'autres informations sur la restauration.

Lorsqu'une installation ou une mise à niveau de VDA multi-session démarre avec cette fonctionnalité activée, le programme d'installation crée une sauvegarde de serveur avant de commencer l'installation ou la mise à niveau. Si l'installation ou la mise à niveau du VDA échoue, l'ordinateur est renvoyé à l'état de la sauvegarde. Le dossier `%temp%/Citrix` contient des journaux de déploiement et d'autres informations sur la restauration. La durée de création de la sauvegarde du serveur dépend de la taille de la sauvegarde nécessaire et de la quantité de ressources disponibles pour le serveur. La sauvegarde est stockée dans *C:\WindowsImageBackup\servername*.

Cette fonctionnalité est désactivée par défaut.

Si vous envisagez d'activer cette fonctionnalité, assurez-vous que la restauration du système n'est pas désactivée via un paramètre d'objet de stratégie de groupe (`Computer Configuration` > `Administrative Templates` > `System` > `System Restore`).

> **Remarque :**
>
> Ce paramètre d'objet de stratégie de groupe ne s'applique pas à la restauration d'un VDA multi-session.

Pour activer cette fonctionnalité lors de l'installation ou de la mise à niveau d'un VDA mono-session ou multi-session :

- Lorsque vous utilisez l'interface graphique d'un programme d'installation VDA (par exemple en utilisant le **démarrage automatique** ou la commande `XenDesktopVDASetup.exe` sans options de restauration ou de mode silencieux), activez la case à cocher **Enable automatic restore if update fails** (Activer la restauration automatique en cas d'échec de la mise à jour) sur la page **Résumé**.

  Si l'installation ou la mise à niveau se termine correctement, le point de restauration ou la sauvegarde n'est pas utilisé, mais est conservé.
- Exécutez un programme d'installation de VDA avec l'option `/enablerestore` ou `/enablerestorecleanup` à l'aide de la ligne de commande.
  - Si vous utilisez l'option `/enablerestorecleanup` et que l'installation ou la mise à niveau se termine correctement, le point de restauration/la sauvegarde de serveur est automatiquement supprimé.
  - Si vous utilisez l'option `/enablerestore` et que l'installation ou la mise à niveau se termine correctement, le point de restauration n'est pas utilisé, mais il est conservé.

Programmes d'installation

Programme d'installation du produit entier

À l'aide du programme d'installation du produit entier, fourni dans l'ISO, vous pouvez :

- installer, mettre à niveau ou supprimer des composants principaux : Delivery Controller, Studio, Director, le serveur de licences ;
- installer ou mettre à niveau StoreFront ;
- installer ou mettre à niveau des VDA Windows pour systèmes d'exploitation mono-session ou multi-session ;
- installer le composant `UpsServer` du Serveur d'impression universelle sur vos serveurs d'impression ;

- installer le Service d'authentification fédérée ;
- installer l'enregistrement de session.
- installer Workspace Environment Management.

> **Remarque :**
>
> Le programme d'installation de Workspace Environment Management Agent n'est pas traduit. Il n'est disponible qu'en anglais.

Pour mettre à disposition un bureau depuis un OS multi-session pour un utilisateur unique (par exemple, à des fins de développement Web), utilisez l'interface de ligne de commande du programme d'installation du produit entier. Pour de plus amples informations, consultez la section Server VDI.

Programmes d'installation de VDA autonomes

Les programmes d'installation de VDA autonomes sont disponibles sur les pages de téléchargement de Citrix. (Ils ne sont pas disponibles à partir du support d'installation du produit.) Les programmes d'installation de VDA autonomes sont beaucoup plus petits que l'image ISO du produit complet. Ils conviennent aux déploiements qui :

- utilisent des packages ESD (distribution électronique de logiciels) qui sont préparés ou copiés localement ;
- incluent des machines physiques ;
- incluent des bureaux à distance.

Par défaut, les fichiers contenus dans le pack VDA autonome auto-extractible sont extraits dans le dossier **Temp**. L'espace disque nécessaire sur la machine lors de l'extraction sur le dossier **Temp** est plus important que lors de l'utilisation du programme d'installation du produit entier. Toutefois, les fichiers extraits dans le dossier **Temp** sont automatiquement supprimés après la fin de l'installation. Vous pouvez aussi utiliser la commande `/extract` avec un chemin d'accès absolu.

Trois programmes d'installation de VDA autonomes sont disponibles en téléchargement.

VDAServerSetup.exe:

Installe un VDA pour OS multi-session. Il prend en charge toutes les options de VDA pour OS multi-session qui sont disponibles avec le programme d'installation du produit entier.

VDAWorkstationSetup.exe:

Installe un VDA pour OS mono-session. Il prend en charge toutes les options de VDA pour OS mono-session qui sont disponibles avec le programme d'installation du produit entier.

VDAWorkstationCoreSetup.exe:

Installe un VDA pour OS mono-session qui est optimisé pour les déploiements Remote PC Access ou les installations VDI de base. Remote PC Access utilise des machines physiques. Les installations VDI de base sont des machines virtuelles qui ne sont pas utilisées en tant qu'image. Seuls les services fondamentaux nécessaires aux connexions VDA de tels déploiements sont installés. Par conséquent, il ne prend en charge qu'un sous-ensemble des options qui sont valides avec les programmes d'installation du produit entier ou `VDAWorkstationSetup.exe`.

Ce programme d'installation n'installe pas et ne contient pas les composants utilisés pour :

- App-V.
- Profile Management. L'exclusion de Citrix Profile Management de l'installation affecte les écrans de Citrix Director. Pour plus amples informations, consultez la section Installer des VDA.
- Machine Identity Service.
- Outils de prise en charge Citrix.
- Citrix Files pour Windows.
- Citrix Files pour Outlook.

Le programme d'installation `VDAWorkstationCoreSetup.exe` n'installe pas et ne contient pas l'application Citrix Workspace pour Windows.

L'utilisation de `VDAWorkstationCoreSetup.exe` équivaut à l'utilisation du programme d'installation de `VDAWorkstationSetup` ou du produit entier pour installer un VDA avec OS mono-session et :

- Dans l'interface graphique : sélection de l'option Remote PC Access sur la page **Environnement**.
- Dans l'interface de ligne de commande : spécification de l'option `/remotepc`.
- Dans l'interface de ligne de commande : spécification de l'option `/components vda` plus l'option `/exclude` qui répertorie tous les noms de composants supplémentaires valides.

Vous pouvez installer les composants/fonctionnalités omis ultérieurement en réexécutant le programme d'installation du produit entier. Cette action vous permet d'installer tous les composants manquants.

Le programme d'installation `VDAWorkstationCoreSetup.exe` installe automatiquement le fichier MSI de redirection du contenu du navigateur. Cette installation automatique s'applique aux VDA versions 2003 et ultérieures prises en charge.

Codes de retour d'installation Citrix

Le journal d'installation contient le résultat de l'installation des composants sous forme de code de retour Citrix, et non une valeur Microsoft.

- 0 = Success (Succès)

- 1 = Failed (Échec)
- 2 = PartialSuccess (Succès partiel)
- 3 = PartialSuccessAndRebootNeeded (Succès partiel et redémarrage requis)
- 4 = FailureAndRebootNeeded (Échec et redémarrage requis)
- 5 = UserCanceled (Annulé par l'utilisateur)
- 6 = MissingCommandLineArgument (Argument de ligne de commande manquant)
- 7 = NewerVersionFound (Version plus récente détectée)
- 8 = SuccessRebootNeeded (Réussite, redémarrage requis)
- 9 = FileLockReboot (Redémarrage de FileLock)
- 10 = Aborted (Abandonné)
- 11 = FailedMedia (Échec du média)
- 12 = FailedLicense (Échec de la licence)
- 13 = FailedPrecheck (Échec de la prévérification)
- 14 = AbortedPendingRebootCheck (Abandonné, en attente de redémarrage)
- -1 = Exit (Sortie)

Par exemple, lorsque vous utilisez des outils tels que Microsoft System Center Configuration Manager, une installation VDA scriptée peut échouer lorsque le journal d'installation contient le code de retour 3. Cela peut se produire lorsque le programme d'installation de VDA attend un redémarrage que vous devez initier (par exemple, après l'installation prérequise du rôle RDS sur un serveur). Une installation de VDA est considérée comme réussie uniquement après que toutes les conditions préalables et les composants sélectionnés ont été installés et que la machine a été redémarrée après l'installation.

Vous pouvez également encapsuler votre installation dans des scripts CMD (qui renvoient les codes de sortie Microsoft) ou modifier les codes de réussite dans votre pack Configuration Manager.

Configurer un serveur de licences Microsoft RDS pour les charges de travail Windows Server

Ce produit accède aux fonctionnalités de session distante de Windows Server lors de la mise à disposition d'une charge de travail Windows Server, telle que Windows 2016. Cela nécessite généralement une licence d'accès client Services Bureau à distance (RDS CAL). Le VDA doit pouvoir contacter un serveur de licences RDS pour demander des licences RDS CAL. Installez et activez le serveur de licences. Pour plus d'informations, voir le document Microsoft Activer le serveur de licences Remote Desktop Services. Pour les environnements de validation technique, vous pouvez utiliser le délai de grâce fourni par Microsoft.

Avec cette méthode, vous pouvez faire en sorte que ce service applique les paramètres du serveur de licences. Vous pouvez configurer le serveur de licences et le mode par utilisateur dans la console RDS sur l'image. Vous pouvez également configurer le serveur de licences à l'aide des paramètres de stratégie de groupe Microsoft. Pour plus d'informations, voir le document Microsoft Attribuer une

licence à votre déploiement RDS avec des licences d'accès client (CAL).

Pour configurer le serveur de licences RDS à l'aide des paramètres de stratégie de groupe :

1. Installez un serveur de licences Services Bureau à distance (RDS) sur une machine disponible. La machine doit toujours être disponible. Les charges de travail du produit Citrix doivent pouvoir atteindre ce serveur de licences.
2. Spécifiez l'adresse du serveur de licences et le mode de licence par utilisateur à l'aide de la stratégie de groupe Microsoft. Pour plus de détails, voir le document Microsoft Spécifier le mode de licence Bureau à distance pour un serveur hôte de session Bureau à distance.

Les charges de travail Windows 10 nécessitent l'activation d'une licence Windows 10 appropriée. Nous vous recommandons de suivre la documentation Microsoft pour activer les charges de travail Windows 10.

Informations supplémentaires

Pour configurer l'emplacement des ressources pour des types d'hôtes spécifiques :

- Environnements de cloud AWS
- Environnements de virtualisation XenServer
- Environnements Google Cloud
- Environnements de cloud Microsoft Azure Resource Manager
- Environnements Microsoft System Center Configuration Manager
- Environnements de virtualisation Microsoft System Center Virtual Machine Manager
- Environnements de virtualisation Nutanix
- Solutions partenaires et cloud Nutanix
- Environnements de virtualisation VMware
- Solutions VMware Cloud et partenaires

Environnements de cloud AWS

June 27, 2024

Cet article vous guide au travers de la configuration de votre compte Amazon Web Services (AWS) en tant qu'emplacement de ressources que vous pouvez utiliser avec Citrix Virtual Apps and Desktops. L'emplacement de ressources inclut un jeu de composants standard, idéal pour les déploiements de preuve de concept ou d'autres déploiements qui ne requièrent pas de ressources réparties sur plusieurs zones de disponibilité. Après avoir terminé ces tâches, vous pouvez installer des VDA, provisionner des machines, créer des catalogues de machines et créer des groupes de mise à disposition.

Une fois les tâches décrites dans cet article terminées, votre emplacement de ressources comprend les composants suivants :

- Un cloud privé virtuel (VPC) avec des sous-réseaux publics et privés à l'intérieur d'une seule zone de disponibilité.
- Une instance qui s'exécute en tant que contrôleur de domaine Active Directory et serveur DNS, située dans le sous-réseau privé du VPC.
- Une instance qui agit en tant qu'hôte bastion dans le sous-réseau public de votre VPC. Cette instance est utilisée pour initier des connexions RDP aux instances dans le sous-réseau privé à des fins d'administration. Après avoir terminé la configuration de votre emplacement de ressources, vous pouvez arrêter cette instance de façon à ce qu'elle ne soit plus accessible. Lorsque vous avez besoin de gérer d'autres instances dans le sous-réseau privé, telles que des instances de VDA, vous pouvez redémarrer l'instance de l'hôte Bastion.

Vue d'ensemble des tâches

Définir un cloud privé virtuel (VPC) avec des sous-réseaux publics et privés. Une fois cette tâche terminée, AWS déploie une passerelle NAT avec une adresse IP élastique dans le sous-réseau public. Cette action permet aux instances du sous-réseau privé d'accéder à Internet. Les instances du sous-réseau public sont accessibles au trafic public entrant ce qui n'est pas le cas des instances du sous-réseau privé.

Configurer des groupes de sécurité. Les groupes de sécurité agissent en tant que pare-feu virtuels qui contrôlent le trafic pour les instances dans votre VPC. Vous devez ajouter des règles à vos groupes de sécurité permettant aux instances de votre sous-réseau public de communiquer avec les instances de votre sous-réseau privé. Vous pouvez également associer ces groupes de sécurité à chaque instance dans votre VPC.

Créer une série d'options DHCP. Avec un VPC Amazon, les services DHCP et DNS sont fournis par défaut, ce qui affecte la configuration du DNS sur votre contrôleur de domaine Active Directory. Le DHCP d'Amazon ne peut pas être désactivé et le DNS d'Amazon peut être utilisé uniquement pour la résolution de DNS public, et non pour la résolution de nom Active Directory. Pour spécifier le domaine et nommer les serveurs qui doivent être transmis aux instances via DHCP, créez une série d'options DHCP. Cette série attribue le suffixe de domaine Active Directory et spécifie le serveur DNS pour toutes les instances dans votre VPC. Pour vous assurer que les enregistrements hôte (A) et recherche inversée (PTR) sont enregistrés automatiquement lorsque des instances rejoignent le domaine, vous configurez les propriétés de la carte réseau pour chaque instance que vous ajoutez au sous-réseau privé.

Ajoutez un hôte bastion et un contrôleur de domaine au VPC. Vous pouvez vous connecter via l'hôte bastion à des instances du sous-réseau privé pour configurer le domaine et joindre des instances au domaine.

Tâche 1 : Configurer le VPC

1. Dans la console de gestion AWS, sélectionnez **VPC**.
2. Dans le tableau de bord VPC, sélectionnez **Create VPC**.
3. Sélectionnez **VPC and more**.
4. Sous NAT gateways ($), sélectionnez **In 1 AZ** ou **1 per AZ**.
5. Sous DNS options, laissez l'option **Enable DNS hostnames** sélectionnée.
6. Sélectionnez **Create VPC**. AWS crée les sous-réseaux publics et privés, une passerelle Internet, des tables de routage et un groupe de sécurité par défaut.

Tâche 2 : Configurer des groupes de sécurité

Cette tâche crée et configure les groupes de sécurité suivants pour votre VPC :

- Un groupe de sécurité public à associer aux instances de votre sous-réseau public.
- Un groupe de sécurité privé à associer aux instances de votre sous-réseau privé.

Pour créer des groupes de sécurité, procédez comme suit :

1. Dans le tableau de bord VPC, sélectionnez **Groupes de sécurité**.
2. Créez un groupe de sécurité pour le groupe de sécurité public. Sélectionnez **Create Security Group** et entrez une étiquette de nom et une description pour le groupe. Dans le menu VPC, sélectionnez le VPC que vous avez créé précédemment. Sélectionnez **Oui, créer**.

Configurer le groupe de sécurité public

1. Depuis la liste de groupes de sécurité, sélectionnez le groupe de sécurité public.
2. Sélectionnez l'onglet **Inbound Rules** et sélectionnez **Edit** pour créer les règles suivantes :

Type	Source
ALL Traffic	Sélectionnez le groupe de sécurité privé.
ALL Traffic	Sélectionnez le groupe de sécurité public.
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0

Type	Source
2598 (Session Reliability)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. Lorsque vous avez terminé, sélectionnez **Enregistrer**.
4. Sélectionnez l'onglet **Outbound Rules** et sélectionnez **Edit** pour créer les règles suivantes :

Type	Destination
ALL Traffic	Sélectionnez le groupe de sécurité privé.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0

5. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

Configurer le groupe de sécurité privé

1. Depuis la liste de groupes de sécurité, sélectionnez le groupe de sécurité privé.
2. Si vous n'avez pas configuré le trafic provenant du groupe de sécurité publique, vous devez définir des ports TCP. Sélectionnez l'onglet **Inbound Rules**, puis **Edit** pour créer les règles suivantes :

Type	Source
ALL Traffic	Sélectionnez le groupe de sécurité privé.
ALL Traffic	Sélectionnez le groupe de sécurité public.
ICMP	Sélectionnez le groupe de sécurité public.
TCP 53 (DNS)	Sélectionnez le groupe de sécurité public.
UDP 53 (DNS)	Sélectionnez le groupe de sécurité public.
80 (HTTP)	Sélectionnez le groupe de sécurité public.
TCP 135	Sélectionnez le groupe de sécurité public.
TCP 389	Sélectionnez le groupe de sécurité public.
UDP 389	Sélectionnez le groupe de sécurité public.

Type	Source
443 (HTTPS)	Sélectionnez le groupe de sécurité public.
TCP 1494 (ICA/HDX)	Sélectionnez le groupe de sécurité public.
TCP 2598 (Session Reliability)	Sélectionnez le groupe de sécurité public.
3389 (RDP)	Sélectionnez le groupe de sécurité public.
TCP 49152–65535	Sélectionnez le groupe de sécurité public.

3. Lorsque vous avez terminé, sélectionnez **Enregistrer.**
4. Sélectionnez l'onglet **Outbound Rules** et sélectionnez **Edit** pour créer les règles suivantes :

Type	Destination
ALL Traffic	Sélectionnez le groupe de sécurité privé.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

Tâche 3 : Lancer des instances

Les étapes suivantes permettent de créer quatre instances EC2 et de décrypter le mot de passe administrateur par défaut généré par Amazon :

1. Dans la console de gestion AWS, sélectionnez **EC2**.
2. Dans le tableau de bord EC2, sélectionnez **Launch Instance**.
3. Sélectionnez une image de machine Windows Server et un type d'instance.
4. Sur la page **Configure Instance Details**, entrez un nom pour l'instance et sélectionnez le VPC configuré précédemment.
5. Dans **Subnet**, effectuez les sélections suivantes pour chaque instance :
   - Bastion host : sélectionner le sous-réseau public
   - Domain Controller : sélectionnez le sous-réseau privé
6. Dans **Auto-assign Public IP address**, effectuez les sélections suivantes pour chaque instance :

- Bastion host : sélectionnez **Enable**.
- Domain controller : sélectionnez **Use default setting** ou **Disable**.

7. Dans **Network Interfaces**, entrez une adresse IP principale comprise dans la plage d'adresses IP de votre sous-réseau privé pour le contrôleur de domaine.
8. Sur la page **Add Storage**, modifiez la taille du disque, si nécessaire.
9. Sur la page **Tag Instance**, entrez un nom convivial pour chaque instance.
10. Sur la page **Configure Security Groups**, sélectionnez **Select an existing security group**, puis effectuez les sélections suivantes pour chaque instance :

    - Bastion host : sélectionnez le groupe de sécurité public.
    - Contrôleur de domaine : sélectionnez le groupe de sécurité privé.

11. Passez en revue vos sélections, puis sélectionnez **Launch**.
12. Créez une nouvelle paire de clés ou sélectionnez-en une existante. Si vous créez une paire de clés, téléchargez le fichier de clé privée (.pem) et conservez-le dans un endroit sûr. Vous devez fournir votre clé privée pour obtenir le mot de passe administrateur par défaut de l'instance.
13. Sélectionnez **Launch Instances**. Sélectionnez **View Instances** pour afficher la liste de vos instances. Attendez que l'instance nouvellement lancée ait passé toutes les vérifications avant d'y accéder.
14. Obtenez le mot de passe administrateur par défaut pour chaque instance :

    a) Dans la liste des instances, sélectionnez l'instance et sélectionnez **Connect**.
    b) Accédez à l'onglet **RDP client**, sélectionnez **Get password** et chargez le fichier de clé privée (`.pem`) lorsque vous y êtes invité.
    c) Sélectionnez **Decrypt password** pour obtenir le mot de passe lisible par l'homme. AWS affiche le mot de passe par défaut.

15. Répétez la procédure depuis l'étape 2 jusqu'à ce que vous ayez créé quatre instances :

    - Une instance d'hôte bastion dans le sous-réseau public
    - Une instance de votre sous-réseau privé destinée à servir de contrôleur de domaine.

Tâche 4 : Créer une série d'options DHCP

1. Dans le tableau de bord VPC, sélectionnez **DHCP Options Sets**.
2. Entrez les informations suivantes :

    - Name tag : entrez un nom convivial pour la série.

- Domain name : entrez le nom de domaine complet utilisé lors de la configuration de l'instance du contrôleur de domaine.
- Domain name servers : entrez l'adresse IP privée attribuée à l'instance du contrôleur de domaine et la chaîne **AmazonProvidedDNS**, en les séparant par des virgules.
- NTP servers : laissez ce champ vide.
- NetBIOS name servers : entrez l'adresse IP privée de l'instance du contrôleur de domaine.
- NetBIOS node type : entrez **2**.

3. Sélectionnez **Oui, créer.**
4. Associez la nouvelle série à votre VPC :

   a) Dans le tableau de bord VPC, sélectionnez **Your VPCs** et sélectionnez le VPC configuré précédemment.
   b) Sélectionnez **Actions > Edit DHCP Options Set**.
   c) Lorsque vous y êtes invité, sélectionnez la nouvelle série que vous avez créée et sélectionnez **Save**.

Tâche 5 : Configurer les instances

1. À l'aide d'un client RDP, connectez-vous à l'adresse IP publique de l'instance de l'hôte Bastion. Lorsque vous y êtes invité, entrez les informations d'identification du compte d'administrateur.
2. À partir de l'instance de l'hôte bastion, lancez Remote Desktop Connection et connectez-vous à l'adresse IP privée de l'instance que vous souhaitez configurer. Lorsque vous y êtes invité, entrez les informations d'identification d'administrateur de l'instance.
3. Pour toutes les instances du sous-réseau privé, configurez les paramètres DNS :

   a) Sélectionnez **Démarrer > Panneau de configuration > Réseau et Internet > Centre Réseau et partage > Modifier les paramètres de la carte**. Cliquez deux fois sur la connexion réseau affichée.
   b) Sélectionnez **Propriétés > Protocole Internet version 4 (TCP/IPv4) > Propriétés**.
   c) Sélectionnez **Avancé > DNS**. Assurez-vous que les paramètres suivants sont activés et sélectionnez **OK** :

      - Enregistrer les adresses de cette connexion dans DNS
      - Utiliser le suffixe DNS de cette connexion pour l'enregistrement DNS

4. Configurez le contrôleur de domaine comme suit :

   a) À l'aide du Gestionnaire de serveur, ajoutez le rôle Services de domaine Active Directory avec toutes les fonctionnalités par défaut.

b) Promouvez l'instance en contrôleur de domaine. Lors de la promotion, activez le DNS et utilisez le nom de domaine que vous avez spécifié lors de la création de la série d'options DHCP. Redémarrez l'instance lorsque vous y êtes invité.

Autres ressources

- Installer les composants principaux
- Installer des VDA
- Créer un site
- Pour créer et gérer une connexion dans AWS, consultez Connexion à AWS.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de machines

Environnements de virtualisation XenServer

June 27, 2024

XenServer simplifie la gestion des opérations en garantissant une expérience utilisateur haute définition pour les charges de travail intensives.

Pour configurer votre XenServer, consultez Préparer l'installation.

Autres ressources

- Installer les composants principaux
- Installer des VDA
- Créer un site
- Pour créer et gérer une connexion dans XenServer, consultez Connexion à XenServer

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de machines

Environnements Google Cloud

June 27, 2024

Citrix Virtual Apps and Desktops vous permet de provisionner et de gérer des machines sur Google Cloud.

Exigences

- Compte Citrix Cloud. La fonctionnalité décrite dans cet article est uniquement disponible dans Citrix Cloud.
- Un projet Google Cloud. Le projet stocke toutes les ressources de calcul associées au catalogue de machines. Il peut s'agir d'un projet existant ou d'un nouveau.
- Activez quatre API dans votre projet Google Cloud. Pour plus de détails, voir Activer les API Google Cloud.
- Compte de service Google Cloud. Le compte de service s'authentifie auprès de Google Cloud pour permettre l'accès au projet. Pour plus de détails, voir Configuration et mise à jour des comptes de service.
- Activer l'accès privé à Google Pour plus de détails, consultez Enable-Private-Google-Access.

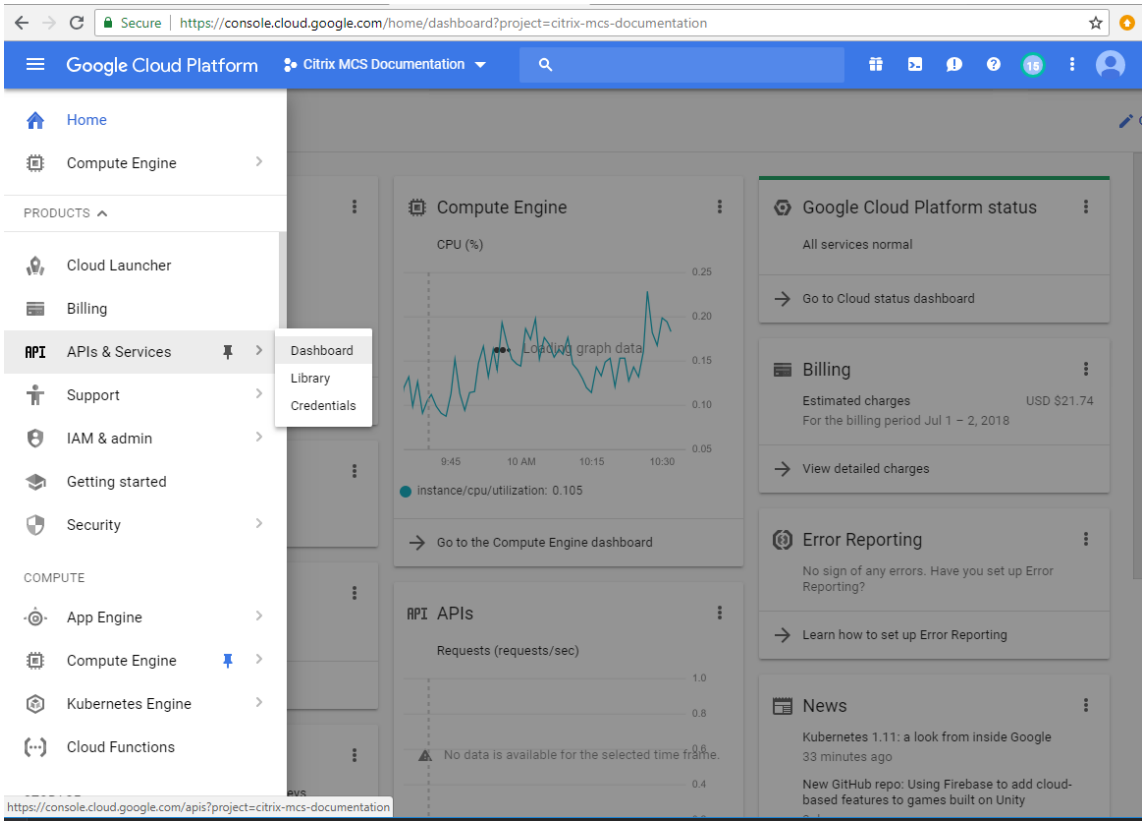
Activer les API Google Cloud

Pour utiliser la fonctionnalité Google Cloud via Web Studio, activez ces API dans votre projet Google Cloud :

- API Compute Engine
- API Cloud Resource Manager
- API IAM (Identity and Access Management)
- API Cloud Build
- Service de gestion des clés dans le cloud (KMS)

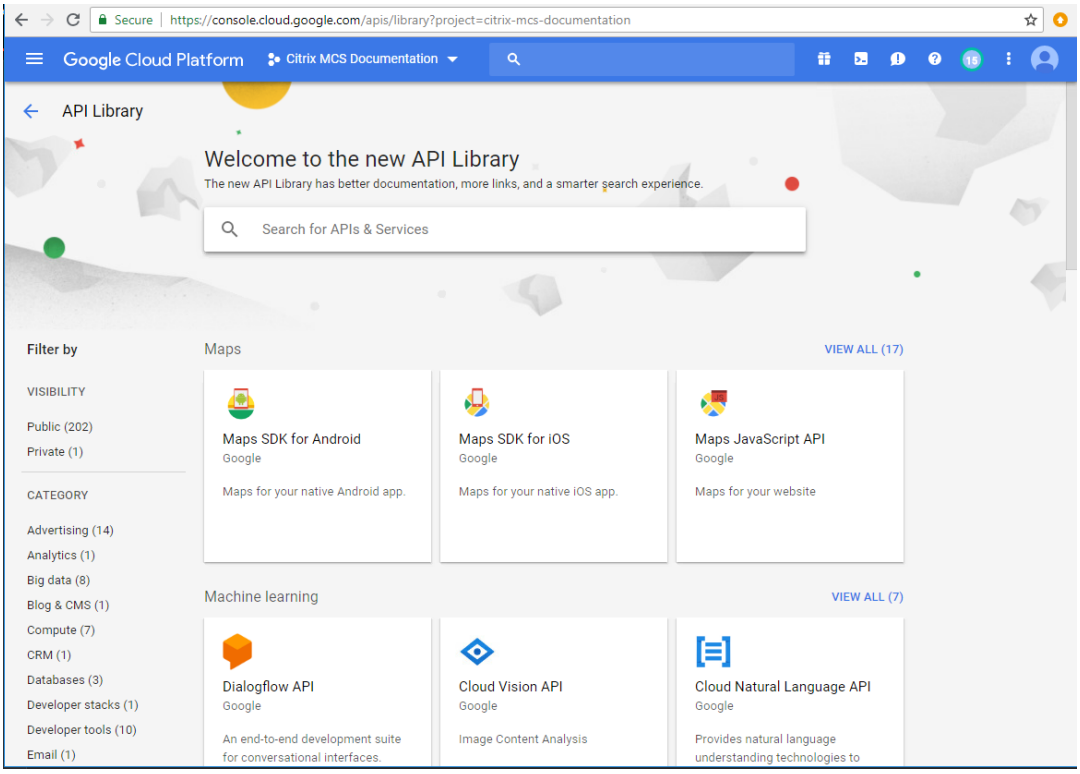
À partir de la console Google Cloud, procédez comme suit :

1. Dans le menu supérieur gauche, sélectionnez **API et Services > Tableau de bord**.



2. Dans l'écran **Tableau de bord**, assurez-vous que l'API Compute Engine est activée. Si ce n'est pas le cas, procédez comme suit :

    a) Accédez à **API et Services > Bibliothèque**.



b) Dans la zone de recherche, tapez *Compute Engine*.

c) Dans les résultats de la recherche, sélectionnez **API Compute Engine**.

d) Sur la page **API Compute Engine**, sélectionnez **Activer**.

3. Activez l'API Cloud Resource Manager.

   a) Accédez à **API et Services > Bibliothèque**.

   b) Dans le champ de recherche, tapez *Cloud Resource Manager*.

   c) Dans les résultats de la recherche, sélectionnez **Cloud Resource Manager API**.

   d) Sur la page **API Cloud Resource Manager**, sélectionnez **Activer**. L'état de l'API s'affiche.

4. Activez **API IAM (Identity and Access Management)** et **API Cloud Build** de la même façon.

Vous pouvez également utiliser Google Cloud Shell pour activer les API. Pour ce faire :

1. Ouvrez la console Google et chargez Cloud Shell.
2. Exécutez les quatre commandes suivantes dans Cloud Shell :

   - gcloud services enable compute.googleapis.com
   - gcloud services enable cloudresourcemanager.googleapis.com
   - gcloud services enable iam.googleapis.com
   - gcloud services enable cloudbuild.googleapis.com

3. Cliquez sur **Authorize** si Cloud Shell vous y invite.

Configuration et mise à jour des comptes de service

> **Remarque :**
>
> GCP apporte des modifications au comportement par défaut du service Cloud Build et à l'utilisation des comptes de service après le 29 avril 2024. Pour plus d'informations, consultez la page Modification d'un compte de service Cloud Build. Vos projets Google existants pour lesquels l'API Cloud Build a été activée avant le 29 avril 2024 ne sont pas concernés par cette modification. Toutefois, si vous souhaitez conserver le comportement existant du service Cloud Build après le 29 avril, vous pouvez créer ou appliquer la stratégie de l'organisation pour désactiver l'application des contraintes avant d'activer l'API Cloud Build. Par conséquent, le contenu suivant est divisé en deux : avant le 29 avril 2024 et après le 29 avril 2024. Si vous définissez la nouvelle stratégie de l'organisation, suivez la section Avant le 29 avril 2024.

Avant le 29 avril 2024

Citrix Cloud utilise trois comptes de service distincts dans le cadre du projet Google Cloud :

- *Compte de service Citrix Cloud* : ce compte de service permet à Citrix Cloud d'accéder au projet Google, de provisionner et de gérer des machines. Ce compte de service s'authentifie auprès de Google Cloud à l'aide d'une clé générée par Google Cloud.

  Vous devez créer ce compte de service manuellement comme indiqué ici. Pour plus d'informations, consultez Créer un compte Citrix Cloud Service.

  Vous pouvez identifier ce compte de service à l'aide d'une adresse e-mail. Par exemple, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Compte de service Cloud Build* : ce compte de service est automatiquement provisionné une fois que vous avez activé toutes les API mentionnées dans Activer les API Google Cloud. Pour afficher tous les comptes de service créés automatiquement, accédez à **IAM & Admin > IAM** dans la console **Google Cloud** et cochez la case **Include Google-provided role grants**.

  Vous pouvez identifier ce compte de service par une adresse e-mail commençant par l'**ID du projet** et le mot **cloudbuild**. Par exemple, `<project-id>@cloudbuild.gserviceaccount.com`

  Vérifiez si les rôles suivants ont été attribués au compte de service. Si vous devez ajouter des rôles, suivez les étapes décrites dans la section Ajouter des rôles au compte de service Cloud Build.

  - Compte de service Cloud Build

  - Administrateur d'instances Compute
  - Utilisateur du compte de service

- *Compte de service Cloud Compute* : ce compte de service est ajouté par Google Cloud aux instances créées dans Google Cloud une fois l'API Compute activée. Ce compte possède le rôle d'éditeur de base IAM pour effectuer les opérations. Toutefois, si vous supprimez l'autorisation par défaut pour bénéficier d'un contrôle plus précis, vous devez ajouter le rôle **Administrateur de l'espace de stockage** qui requiert les autorisations suivantes :

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

Vous pouvez identifier ce compte de service par une adresse e-mail commençant par l'**ID du projet** et le mot **compute**. Par exemple, `<project-id>-compute@developer.gserviceaccount.com`.

Créer un compte Citrix Cloud Service Pour créer un compte Citrix Cloud Service, procédez comme suit :

1. Dans la console Google Cloud, accédez à **IAM et administration > Comptes de service**.
2. Sur la page **Comptes de service**, sélectionnez **CRÉER UN COMPTE DE SERVICE**.
3. Sur la page **Créer un compte de service**, entrez les informations requises, puis sélectionnez **CRÉER ET CONTINUER**.
4. Sur la page **Autoriser ce compte de service à accéder au projet**, cliquez sur le menu déroulant **Sélectionner un rôle** et sélectionnez les rôles requis. Cliquez sur **+AJOUTER UN AUTRE RÔLE** si vous souhaitez ajouter d'autres rôles.

   Chaque compte (personnel ou service) a différents rôles définissant la gestion du projet. Attribuez les rôles suivants à ce compte de service :

   - Administrateur informatique
   - Administrateur de l'espace de stockage
   - Éditeur Cloud Build
   - Utilisateur du compte de service
   - Utilisateur de Cloud Datastore
   - Opérateur de cryptage Cloud KMS

   L'opérateur de cryptage Cloud KMS a besoin des autorisations suivantes :

   - cloudkms.cryptoKeys.get

- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **Remarque :**
>
> Activez toutes les API pour obtenir la liste complète des rôles disponibles lors de la création d'un nouveau compte de service.

5. Cliquez sur **CONTINUER**
6. Sur la page **Autoriser les utilisateurs à accéder à ce compte de service**, ajoutez des utilisateurs ou des groupes pour leur permettre d'effectuer des actions dans ce compte de service.
7. Cliquez sur **OK**.
8. Accédez à la console principale IAM.
9. Identifiez le compte de service créé.
10. Vérifiez que les rôles sont correctement assignés.

Considérations :

Lors de la création du compte de service, tenez compte des éléments suivants :

- Les étapes **Autoriser ce compte de service à accéder au projet** et **Autoriser les utilisateurs à accéder à ce compte de service** sont facultatives. Si vous choisissez d'ignorer ces étapes de configuration facultatives, le compte de service nouvellement créé ne s'affiche pas dans la page **IAM et administration > IAM**.
- Pour afficher les rôles associés à un compte de service, ajoutez les rôles sans ignorer les étapes facultatives. Ce processus garantit que les rôles apparaissent pour le compte de service configuré.

Clé de compte Citrix Cloud Service La clé de compte Citrix Cloud Service est requise pour créer une connexion dans Citrix DaaS. La clé est contenue dans un fichier d'informations d'identification (.json). Une fois la clé créée, le fichier est automatiquement téléchargé et enregistré dans le dossier **Téléchargements**. Lorsque vous créez la clé, assurez-vous de définir le type de clé sur JSON. Sinon, l'interface Configuration complète de Citrix ne peut pas l'analyser.

Pour créer une clé de compte de service, accédez à **IAM & Admin > Service accounts**, puis cliquez sur l'adresse e-mail du compte de service Citrix Cloud. Passez à l'onglet **Keys** et sélectionnez **Add Key > Create new key**. Assurez-vous de sélectionner **JSON** comme type de clé.

> **Conseil :**
>
> Créez des clés à l'aide de la page **Comptes de service** de la console Google Cloud. Nous vous recommandons de modifier régulièrement les clés pour des raisons de sécurité. Pour fournir de nouvelles clés à l'application Citrix Virtual Apps and Desktops, modifiez une connexion Google Cloud existante.

Ajouter des rôles au compte Citrix Cloud Service Pour ajouter des rôles au compte Citrix Cloud Service, procédez comme suit :

1. Dans la console Google Cloud, accédez à **IAM et administration > IAM**.
2. Sur la page **IAM > AUTORISATIONS**, recherchez le compte de service que vous avez créé, identifiable grâce à une adresse e-mail.

   Par exemple, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Sélectionnez l'icône en forme de crayon pour modifier l'accès au compte principal du compte de service.
4. Sur la page **Modifier l'accès à « identifiant du projet »** pour l'option de compte principal sélectionnée, sélectionnez **AJOUTER UN AUTRE RÔLE** pour ajouter les rôles requis à votre compte de service un par un, puis sélectionnez **ENREGISTRER**.

Ajouter des rôles au compte de service Cloud Build Pour ajouter des rôles au compte de service Cloud Build :

1. Dans la console Google Cloud, accédez à **IAM et administration > IAM**.
2. Sur la page **IAM**, recherchez le compte de service Cloud Build, identifiable par une adresse e-mail commençant par l'**ID du projet** et le mot **cloudbuild**.

   Par exemple, `<project-id>@cloudbuild.gserviceaccount.com`
3. Sélectionnez l'icône en forme de crayon pour modifier les rôles du compte Cloud Build.
4. Sur la page **Modifier l'accès à « identifiant du projet »** pour l'option de compte principal sélectionnée, sélectionnez **AJOUTER UN AUTRE RÔLE** pour ajouter les rôles requis à votre compte de service Cloud Build un par un, puis sélectionnez **ENREGISTRER**.

   > **Remarque :**
   >
   > Activez toutes les API pour obtenir la liste complète des rôles.

Après le 29 avril 2024

Citrix Cloud utilise deux comptes de service distincts dans le cadre du projet Google Cloud :

- *Compte de service Citrix Cloud* : ce compte de service permet à Citrix Cloud d'accéder au projet Google, de provisionner et de gérer des machines. Ce compte de service s'authentifie auprès de Google Cloud à l'aide d'une clé générée par Google Cloud.

  Vous devez créer ce compte de service manuellement.

  Vous pouvez identifier ce compte de service à l'aide d'une adresse e-mail. Par exemple, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Compte de service Cloud Compute :* ce compte de service est automatiquement provisionné une fois que vous avez activé toutes les API mentionnées dans Activer les API Google Cloud. Pour afficher tous les comptes de service créés automatiquement, accédez à **IAM & Admin > IAM** dans la console **Google Cloud** et cochez la case **Include Google-provided role grants**. Ce compte possède le rôle d'éditeur de base IAM pour effectuer les opérations. Toutefois, si vous supprimez l'autorisation par défaut pour bénéficier d'un contrôle plus précis, vous devez ajouter le rôle **Administrateur de l'espace de stockage** qui requiert les autorisations suivantes :

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

  Vous pouvez identifier ce compte de service par une adresse e-mail commençant par l'**ID du projet** et le mot **compute**. Par exemple, `<project-id>-compute@developer.gserviceaccount.com`.

  Vérifiez si les rôles suivants ont été attribués au compte de service.

  - Compte de service Cloud Build
  - Administrateur d'instances Compute
  - Utilisateur du compte de service

Créer un compte Citrix Cloud Service Pour créer un compte Citrix Cloud Service, procédez comme suit :

1. Dans la console Google Cloud, accédez à **IAM et administration > Comptes de service**.
2. Sur la page **Comptes de service**, sélectionnez **CRÉER UN COMPTE DE SERVICE**.
3. Sur la page **Créer un compte de service**, entrez les informations requises, puis sélectionnez **CRÉER ET CONTINUER**.

4. Sur la page **Autoriser ce compte de service à accéder au projet**, cliquez sur le menu déroulant **Sélectionner un rôle** et sélectionnez les rôles requis. Cliquez sur **+AJOUTER UN AUTRE RÔLE** si vous souhaitez ajouter d'autres rôles.

   Chaque compte (personnel ou service) a différents rôles définissant la gestion du projet. Attribuez les rôles suivants à ce compte de service :

   - Administrateur informatique
   - Administrateur de l'espace de stockage
   - Éditeur Cloud Build
   - Utilisateur du compte de service
   - Utilisateur de Cloud Datastore
   - Opérateur de cryptage Cloud KMS

   L'opérateur de cryptage Cloud KMS a besoin des autorisations suivantes :

   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.get
   - cloudkms.keyRings.list

   > **Remarque :**
   >
   > Activez toutes les API pour obtenir la liste complète des rôles disponibles lors de la création d'un nouveau compte de service.

5. Cliquez sur **CONTINUER**
6. Sur la page **Autoriser les utilisateurs à accéder à ce compte de service**, ajoutez des utilisateurs ou des groupes pour leur permettre d'effectuer des actions dans ce compte de service.
7. Cliquez sur **OK**.
8. Accédez à la console principale IAM.
9. Identifiez le compte de service créé.
10. Vérifiez que les rôles sont correctement assignés.

Considérations :

Lors de la création du compte de service, tenez compte des éléments suivants :

- Les étapes **Autoriser ce compte de service à accéder au projet** et **Autoriser les utilisateurs à accéder à ce compte de service** sont facultatives. Si vous choisissez d'ignorer ces étapes de configuration facultatives, le compte de service nouvellement créé ne s'affiche pas dans la page **IAM et administration > IAM**.

- Pour afficher les rôles associés à un compte de service, ajoutez les rôles sans ignorer les étapes facultatives. Ce processus garantit que les rôles apparaissent pour le compte de service configuré.

Clé de compte Citrix Cloud Service La clé de compte Citrix Cloud Service est requise pour créer une connexion dans Citrix DaaS. La clé est contenue dans un fichier d'informations d'identification (.json). Une fois la clé créée, le fichier est automatiquement téléchargé et enregistré dans le dossier **Téléchargements**. Lorsque vous créez la clé, assurez-vous de définir le type de clé sur JSON. Sinon, l'interface Configuration complète de Citrix ne peut pas l'analyser.

Pour créer une clé de compte de service, accédez à **IAM & Admin > Service accounts**, puis cliquez sur l'adresse e-mail du compte de service Citrix Cloud. Passez à l'onglet **Keys** et sélectionnez **Add Key > Create new key**. Assurez-vous de sélectionner **JSON** comme type de clé.

> **Conseil :**
>
> Créez des clés à l'aide de la page **Comptes de service** de la console Google Cloud. Nous vous recommandons de modifier régulièrement les clés pour des raisons de sécurité. Pour fournir de nouvelles clés à l'application Citrix Virtual Apps and Desktops, modifiez une connexion Google Cloud existante.

Ajouter des rôles au compte Citrix Cloud Service Pour ajouter des rôles au compte Citrix Cloud Service, procédez comme suit :

1. Dans la console Google Cloud, accédez à **IAM et administration > IAM**.
2. Sur la page **IAM > AUTORISATIONS**, recherchez le compte de service que vous avez créé, identifiable grâce à une adresse e-mail.

   Par exemple, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Sélectionnez l'icône en forme de crayon pour modifier l'accès au compte principal du compte de service.
4. Sur la page **Modifier l'accès à « identifiant du projet »** pour l'option de compte principal sélectionnée, sélectionnez **AJOUTER UN AUTRE RÔLE** pour ajouter les rôles requis à votre compte de service un par un, puis sélectionnez **ENREGISTRER**.

Ajouter des rôles au compte de service Cloud Compute Pour ajouter des rôles au compte de service Cloud Compute :

1. Dans la console Google Cloud, accédez à **IAM et administration > IAM**.

2. Sur la page **IAM**, recherchez le compte de service Cloud Build, identifiable par une adresse e-mail commençant par l'**ID du projet** et le mot **cloudbuild**.

   Par exemple, `<project-id>-compute@developer.gserviceaccount.com`

3. Sélectionnez l'icône en forme de crayon pour modifier les rôles du compte Cloud Build.
4. Sur la page **Modifier l'accès à « identifiant du projet »** pour l'option de compte principal sélectionnée, sélectionnez **AJOUTER UN AUTRE RÔLE** pour ajouter les rôles requis à votre compte de service Cloud Build un par un, puis sélectionnez **ENREGISTRER**.

   > **Remarque :**
   >
   > Activez toutes les API pour obtenir la liste complète des rôles.

Autorisations de stockage et gestion des buckets

Citrix Virtual Apps and Desktops améliore le processus de signalement d'échecs Cloud Build pour le service Google Cloud. Ce service exécute des builds sur Google Cloud. Citrix Virtual Apps and Desktops crée un bucket de stockage nommé `citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }` dans lequel les services Google Cloud capturent les informations de journal de build. Une option qui supprime le contenu après une période de 30 jours est définie sur ce bucket. Ce processus nécessite que les autorisations Google Cloud du compte de service utilisé pour la connexion soient définies sur `storage.buckets.update`. Si le compte de service ne dispose pas de cette autorisation, Citrix Virtual Apps and Desktops ignore les erreurs et poursuit le processus de création du catalogue. Sans cette autorisation, la taille des journaux de build augmente et nécessite un nettoyage manuel.

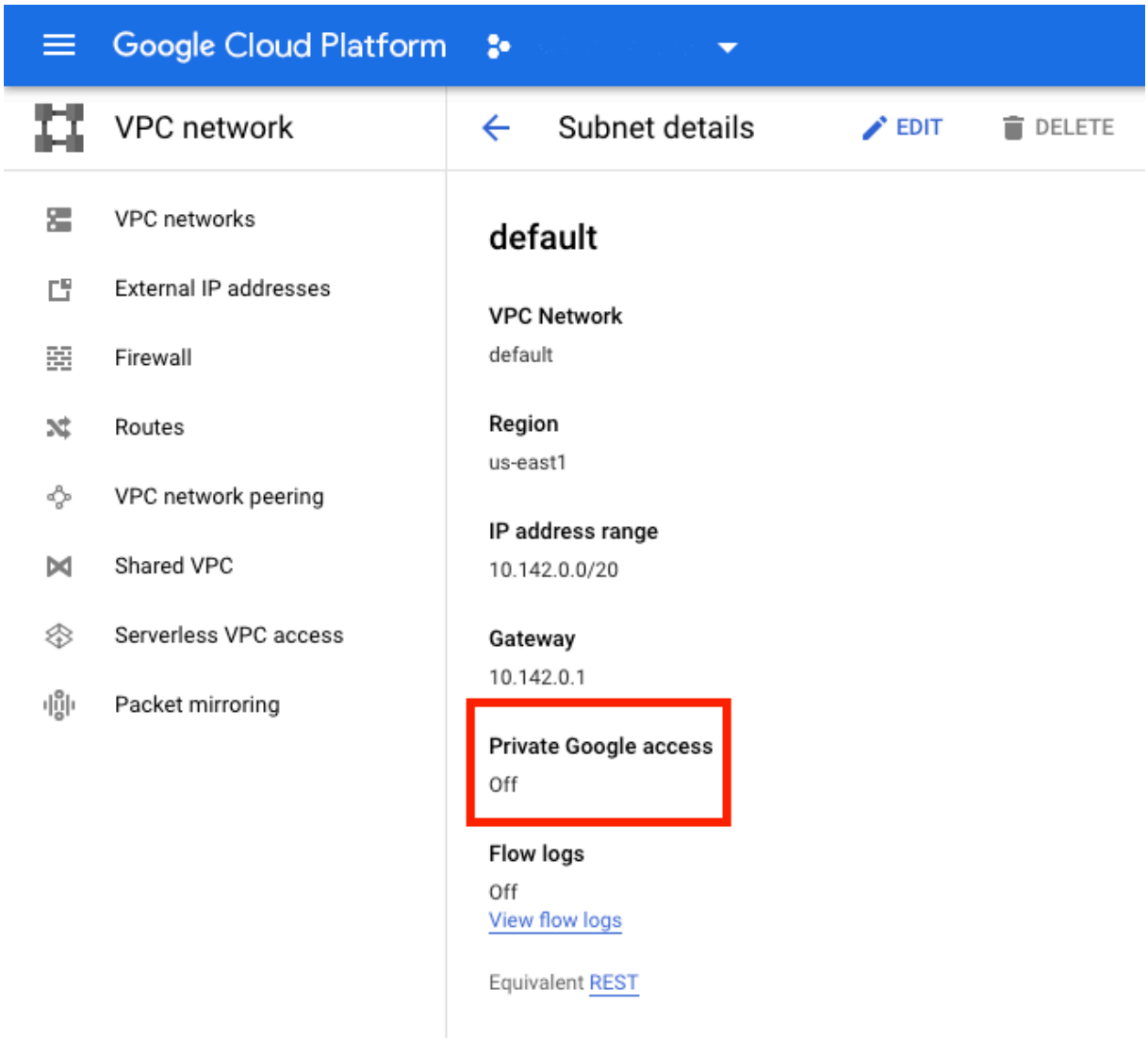
Activer l'accès privé à Google

Lorsqu'une machine virtuelle ne dispose pas d'une adresse IP externe affectée à son interface réseau, les paquets ne sont envoyés qu'à d'autres destinations d'adresses IP internes. Lorsque vous activez l'accès privé, la machine virtuelle se connecte à l'ensemble d'adresses IP externes utilisées par l'API Google et les services associés.

> **Remarque :**
>
> Que l'accès privé à Google soit activé ou non, toutes les machines virtuelles dotées ou non d'adresses IP publiques doivent pouvoir accéder aux API publiques de Google, en particulier si des appliances réseau tiers ont été installés dans l'environnement.

Pour vous assurer qu'une machine virtuelle de votre sous-réseau peut accéder aux API Google sans adresse IP publique pour le provisioning MCS :

1. Dans Google Cloud, accédez à la **configuration du réseau VPC**.
2. Dans l'écran Détails du sous-réseau, activez **Accès privé à Google**.



Pour plus d'informations, consultez Configuration de l'accès privé à Google.

> **Important :**
>
> Si votre réseau est configuré pour empêcher l'accès des machines virtuelles à Internet, assurez-vous que votre organisation assume les risques associés à l'activation de l'accès privé à Google pour le sous-réseau auquel la machine virtuelle est connectée.

Autres ressources

- Installer les composants principaux
- Installer des VDA

- Créer un site
- Pour créer et gérer une connexion dans les environnements Google Cloud, voir Connexion aux environnements Google Cloud

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de machines

Environnements de virtualisation HPE Moonshot

June 27, 2024

Citrix Virtual Apps and Desktops gère vos charges de travail HPE Moonshot via un plug-in HPE Moonshot géré par Citrix. Avec ce plug-in, vous pouvez créer des connexions à votre châssis HPE Moonshot, créer des catalogues et gérer l'alimentation des machines du catalogue.

Exigences

Installez le plug-in HPE Moonshot géré par Citrix sur le Delivery Controller.

> **Remarque :**
>
> - Si des plug-ins HPE Moonshot gérés par Citrix et HPE sont installés, le Delivery Controller utilise le plug-in HPE Moonshot géré par Citrix.
> - Si des plug-ins HPE Moonshot gérés par Citrix et HPE sont installés et que vous souhaitez utiliser le plug-in Moonshot géré par HPE, désinstallez le plug-in HPE Moonshot géré par Citrix et mettez à jour le cache `RegisterPlugin`.

Installez le plug-in HPE Moonshot géré par Citrix

Pour installer le plug-in HPE Moonshot géré par Citrix, procédez comme suit :

1. Installez `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin`.msi. `E:\` est l'image ISO.
2. Ouvrez le PowerShell en tant qu'administrateur et exécutez la commande suivante.

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins
    .exe -pluginsroot .\CitrixMachineCreation\v1.0.0.0\
<!--NeedCopy-->
```


3. Une fois le plug-in enregistré, redémarrez les services suivants depuis le **Gestionnaire des tâches** :

    a) CitrixBrokerService
    b) CitrixHostService
    c) CitrixMachineCreationService

4. Exécutez `Get-HypHypervisorPlugins` pour vérifier si le plug-in est installé sur le Delivery Controller. Le champ **DisplayName** de la sortie doit être **HPE Moonshot**.

Désinstallez le plug-in HPE Moonshot géré par Citrix et mettez à jour le cache RegisterPlugin

Si des plug-ins HPE Moonshot gérés par Citrix et HPE sont installés et que vous souhaitez utiliser le plug-in Moonshot géré par HPE, vous devez désinstaller le plug-in HPE Moonshot géré par Citrix et mettre à jour le cache `RegisterPlugin`. Pour ce faire :

1. Désinstallez le plug-in HPE Moonshot géré par Citrix.
2. Ouvrez le PowerShell en tant qu'administrateur et exécutez la commande suivante :

```
1 cd `C:\Program Files\Common Files\Citrix\HCLPlugins`
2 C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins
     .exe -PluginsRoot ` C:\Program Files\Common Files\Citrix\
     HCLPlugins\ManagedMachine\v2.5.0.0`
3 <!--NeedCopy-->
```

3. Une fois le plug-in enregistré, redémarrez les services suivants depuis le **Gestionnaire des tâches** :

    a) CitrixBrokerService
    b) CitrixHostService
    c) CitrixMachineCreationService

4. Exécutez `Get-HypHypervisorPlugins` pour vérifier si le plug-in est installé sur le Delivery Controller. Le champ **DisplayName** de la sortie doit être **HPE Moonshot Machine Manager**.

Étapes clés

1. Configurez vos environnements HPE.
2. Créez une connexion avec le châssis HPE Moonshot.
3. Créez un catalogue de machines.

> **Remarque :**
>
> Avant de créer un catalogue, assurez-vous de disposer d'un ou de plusieurs nœuds de cartouches HPE Moonshot et installez des VDA sur ces nœuds. Vous pouvez considérer le châssis HPE Moonshot comme un hyperviseur et les nœuds de cartouche comme des machines virtuelles.

4. Créez un groupe de mise à disposition.
5. Migrez le reste des nœuds HPE Moonshot non gérés vers le groupe de mise à disposition ou le catalogue géré.

Autres ressources

- Installer les composants principaux
- Installer des VDA
- Créer un site
- Pour créer et gérer une connexion dans HPE Moonshot, consultez Connexion à HPE Moonshot

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de machines

Environnements de cloud Microsoft Azure Resource Manager

June 27, 2024

Lorsque vous utilisez Microsoft Azure Resource Manager pour provisionner des machines virtuelles dans votre déploiement Citrix Virtual Apps and Desktops, familiarisez-vous avec les éléments suivants :

- Azure Active Directory : https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/
- Infrastructure Consent : https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-an-application-integration
- Principal de service : https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals/

Pour configurer votre Microsoft Azure Resource Manager, consultez la section Préparer l'installation.

Autres ressources

- Installer les composants principaux
- Installer des VDA
- Créer un site
- Pour créer et gérer une connexion dans les environnements Azure, voir Connexion à Microsoft Azure.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de machines
- CTX219211: Set up a Microsoft Azure Active Directory account
- CTX219243 : Grant XenApp and XenDesktop access to your Azure subscription
- CTX219271 : Deploy hybrid cloud using site-to-site VPN

Environnements Microsoft System Center Configuration Manager

June 27, 2024

Les sites qui utilisent Microsoft System Center Configuration Manager (Configuration Manager) pour gérer l'accès aux applications et bureaux peuvent étendre cette utilisation à Citrix Virtual Apps and Desktops via ces options.

- Installez des VDA à l'aide de SCCM.
- **Fonctionnalité Configuration Manager Wake Proxy :** l'utilisation de la fonctionnalité Remote PC Access Wake on LAN est prise en charge avec Configuration Manager. Pour de plus amples informations, consultez la section Wake on LAN - Intégration SCCM.
- **Propriétés Citrix Virtual Apps and Desktops :** les propriétés vous permettent d'identifier Citrix Virtual Desktops pour la gestion via Configuration Manager. (Dans certaines versions, Configuration Manager utilise l'ancien nom de Citrix Virtual Apps and Desktops : XenApp et XenDesktop.)

Propriétés

Propriétés disponibles pour Microsoft System Center Configuration Manager pour gérer des bureaux virtuels.

Les propriétés booléennes affichées dans Configuration Manager apparaissent sous la forme de 1 ou 0 au lieu de true ou false.

Les propriétés sont disponibles pour la classe Citrix_virtualDesktopInfo dans l'espace de noms Root\Citrix\DesktopInformation. Les noms des propriétés proviennent du fournisseur WMI (Windows Management Instrumentation) :

Propriété	Description
AssignmentType	Définit la valeur de IsAssigned. Les valeurs valides sont : ClientIP, ClientName, None et User (définit IsAssigned sur True)
BrokerSiteName	Renvoie la même valeur que HostIdentifier
DesktopCatalogName	Catalogue de machines associé au bureau.
DesktopGroupName	Groupe de mise à disposition associé au bureau.
HostIdentifier	Renvoie la même valeur que BrokerSiteName.
IsAssigned	True pour attribuer le bureau à un utilisateur, False pour un bureau aléatoire
IsMasterImage	Permet de prendre des décisions sur l'environnement. Par exemple, installez des applications sur l'image et non sur les machines provisionnées. Les valeurs valides sont : True sur une machine virtuelle utilisée comme image. Cette valeur est définie lors de l'installation basée sur une sélection ou Cleared sur une VM qui est provisionnée à partir de cette image.
IsVirtualMachine	True pour une machine virtuelle, **false** pour une machine physique.
OSChangesPersist	False si l'image du système d'exploitation du bureau est réinitialisée à un nouvel état chaque fois qu'elle est redémarrée, sinon **true**.
PersistentDataLocation	Emplacement dans lequel le Gestionnaire de configuration stocke les données permanentes. Ceci n'est pas accessible aux utilisateurs.
BrokerSiteName, DesktopCatalogName, DesktopGroupName, HostIdentifier	Déterminé quand le bureau s'enregistre auprès du contrôleur. La valeur est null pour un bureau qui n'est pas entièrement enregistré.

Pour collecter les propriétés, exécutez un inventaire matériel dans Configuration Manager. Pour afficher les propriétés, utilisez l'Explorateur de ressources Configuration Manager. Dans ce cas, les noms incluent des espaces ou varient légèrement des noms de propriété. Par exemple, `BrokerSiteName` apparaît sous la forme `Broker Site Name`.

- Configurer Configuration Manager pour collecter les propriétés Citrix WMI du VDA Citrix
- Créer des collections de machines basées sur une requête à l'aide des propriétés Citrix WMI
- Créer des conditions globales basées sur les propriétés Citrix WMI
- Utilisez les conditions globales pour définir les spécifications du type de déploiement de l'application

Vous pouvez également utiliser les propriétés Microsoft dans la classe Microsoft `CCM_DesktopMachine` dans l'espace de noms `Root\ccm_vdi`. Pour de plus amples informations, consultez la documentation de Microsoft.

Environnements de virtualisation Microsoft System Center Virtual Machine Manager

June 27, 2024

Suivez ce guide si vous utilisez Hyper-V avec Microsoft System Center Virtual Machine Manager (VMM) pour fournir des machines virtuelles.

Cette version prend en charge les versions de VMM indiquées dans la section Configuration système requise.

> **Remarque :**
>
> Les clusters Hyper-V mixtes (contenant des serveurs exécutant différentes versions de Hyper-V) ne sont pas pris en charge.

Vous pouvez utiliser Machine Creation Services et Citrix Provisioning (anciennement Provisioning Services) pour provisionner :

- La génération 1 prend en charge les machines virtuelles avec OS de serveur ou de bureau.
- La génération 2 prend en charge les machines virtuelles avec OS de serveur ou de bureau, y compris la prise en charge du démarrage sécurisé.

Installer et configurer un hyperviseur

> **Important :**
>
> Tous les Delivery Controller doivent se trouver dans la même forêt que les serveurs VMM.

1. Installez Microsoft Hyper-V Server et VMM sur vos serveurs.
2. Installez la console System Center Virtual Machine Manager Console sur tous les Controller. La version de la console doit correspondre à la version du serveur de gestion. Bien qu'une console antérieure puisse se connecter au serveur de gestion, le provisioning des VDA échoue si les versions diffèrent.
3. Vérifiez les informations de compte suivantes :

   Le compte que vous utilisez pour spécifier des hôtes dans Studio est un administrateur VMM ou un administrateur VMM délégué pour les machines Hyper-V appropriées. Si ce compte possède uniquement le rôle d'administrateur délégué dans VMM, les données de stockage ne sont pas répertoriées dans Studio lors du processus de création de l'hôte.

   Le compte d'utilisateur utilisé pour l'intégration de Studio doit également être un membre du groupe de sécurité Administrateurs local sur chaque serveur Hyper-V. Cette configuration prend en charge la gestion du cycle de vie des VM, comme la création, la mise à jour et la suppression de VM.

   L'installation du Controller sur un serveur exécutant Hyper-V n'est pas prise en charge.

Dans les déploiements importants où un seul SCVMM gère plusieurs clusters dans différents centres de données, vous pouvez limiter la portée des groupes d'hôtes des administrateurs délégués.

Pour limiter la portée des groupes d'hôtes, utilisez le rôle d'administrateur délégué dans la console Microsoft System Center Virtual Machine Manager (VMM) :

1. Dans **Create User Roles Wizard**, sélectionnez Fabric Administrator (administrateur délégué) comme rôle utilisateur.
2. Dans **Members**, ajoutez le compte utilisateur de l'annuaire Active Directory que vous souhaitez utiliser en tant qu'administrateur délégué.
3. Dans **Scope**, sélectionnez les groupes d'hôtes auxquels vous souhaitez que l'administrateur délégué ait accès.
4. Créez un nouveau compte **Run As Account** en utilisant les informations d'identification utilisateur de l'administrateur délégué. Utilisez ces informations d'identification pour créer une connexion à l'hyperviseur ultérieurement. N'utilisez pas les comptes de rôle d'administrateur principaux.

Provisionner Azure Stack HCI via SCVMM

Azure Stack HCI est une solution de cluster d'infrastructure hyperconvergée (HCI) qui héberge des charges de travail Windows et Linux virtualisées et leur stockage dans un environnement hybride sur

site.

Les services hybrides Azure améliorent le cluster avec des fonctionnalités telles que la surveillance basée sur le cloud, la restauration de site et les sauvegardes de machines virtuelles. Vous avez également accès à une vue centralisée de tous vos déploiements Azure Stack HCI sur le portail Azure.

Intégrer Azure Stack HCI à SCVMM

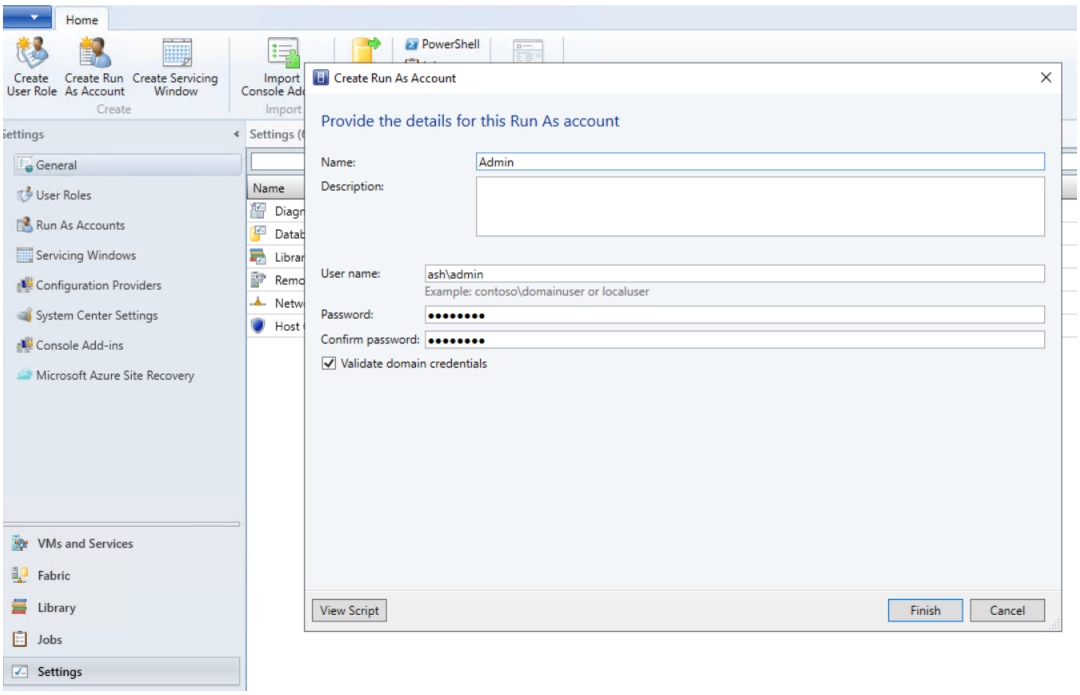
Pour intégrer Azure Stack HCI à SCVMM, vous devez d'abord créer un cluster Azure Stack HCI, puis intégrer ce cluster à SCVMM.

1. Pour créer le cluster Azure Stack HCI, consultez le document Microsoft Connecter Azure Stack HCI à Azure.
2. Pour intégrer le cluster Azure Stack HCI à SCVMM, procédez comme suit :

   a) Connectez-vous à la machine qui est prête à héberger le serveur SCVMM et installez SCVMM 2019 UR3 ou version ultérieure.

   > **Remarque :**
   >
   > Installez la console d'administration SCVMM 2019 UR3 ou version ultérieure sur tous les contrôleurs.

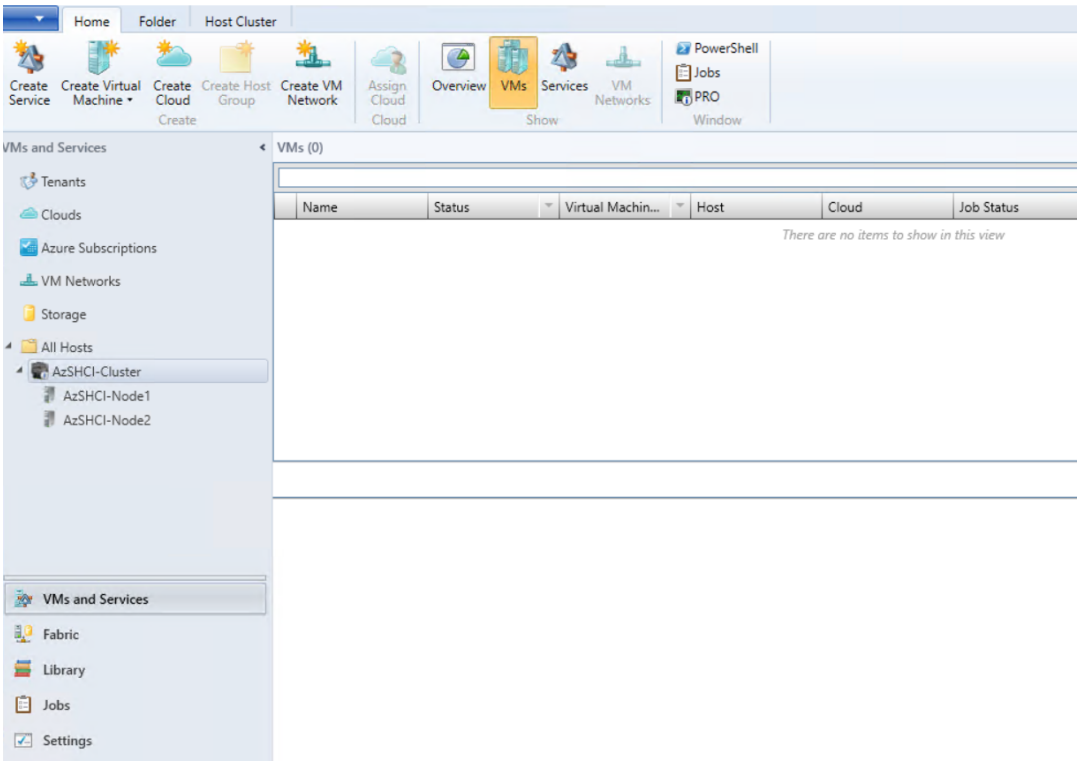
   b) Sur la page **Paramètres** de la console VMM, créez un compte Exécuter en tant que.



   c) Exécutez les commandes PowerShell suivantes avec des privilèges d'administration sur le serveur SCVMM pour ajouter le cluster Azure Stack HCI en tant qu'hôte :


```
$runAsAccountName = 'Admin'
$runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
$hostGroupName = 'All Hosts'
$hostGroup = Get-SCVMHostGroup -Name $hostGroupName
$hostCluster = 'FQDN of Azure Stack HCI cluster'
Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
    VMHostGroup
$hostGroup -Credential $runAsAccount -RemoteConnectEnabled
    $true
<!--NeedCopy-->
```

d) Vous pouvez désormais voir le cluster Azure Stack HCI ainsi que les nœuds dans la console VMM.



e) Créez la connexion d'hébergement SCVMM dans Web Studio.

Autres ressources

- Installer les composants principaux
- Installer des VDA
- Créer un site
- Pour créer et gérer une connexion dans SCVMM, consultez Connexion à Microsoft System Center Virtual Machine Manager.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de machines

Environnements de virtualisation Nutanix

June 27, 2024

Suivez ces instructions lors de l'utilisation de Nutanix Acropolis pour fournir des machines virtuelles dans votre déploiement Citrix Virtual Apps and Desktops. Le processus d'installation comprend les tâches suivantes :

- Installer et enregistrer le plug-in Nutanix dans votre environnement Citrix Virtual Apps and Desktops.
- Créer une connexion à l'hyperviseur Nutanix Acropolis.
- Créer un catalogue de machines qui utilise un instantané d'une image principale que vous avez créée sur l'hyperviseur Nutanix.

Pour de plus amples informations, consultez le Guide d'installation du plugin Nutanix Acropolis MCS, disponible sur le portail d'assistance de Nutanix.

Installer et enregistrer le plug-in Nutanix

Réalisez la procédure suivante pour installer et enregistrer le plug-in Nutanix sur tous vos Delivery Controller. Utilisez Citrix Studio pour créer une connexion à Nutanix. Créez ensuite un catalogue de machines qui utilise un instantané d'une image principale que vous avez créée dans l'environnement Nutanix.

> **Conseil :**
>
> Nous vous recommandons d'arrêter, puis de redémarrer Citrix Host Service, Citrix Broker Service et Machine Creation Services lorsque vous installez ou mettez à jour le plug-in Nutanix.

Pour de plus amples informations sur l'installation du plug-in Nutanix, consultez le site de documentation de Nutanix.

Autres ressources

- Installer les composants principaux

- Installer des VDA
- Créer un site
- Pour créer et gérer une connexion dans les environnements Nutanix, voir Connexion à Nutanix.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de machines

Solutions partenaires et cloud Nutanix

June 27, 2024

Citrix Virtual Apps and Desktops prend en charge les solutions cloud Nutanix et partenaires suivantes :

- Nutanix Cloud Clusters sur AWS

Nutanix Cloud Clusters sur AWS

Citrix Virtual Apps and Desktops prend en charge Nutanix Cloud Clusters sur AWS. Les clusters Nutanix simplifient la façon dont les applications sont exécutées sur des clouds privés ou sur plusieurs clouds publics. Pour plus d'informations sur Nutanix Cloud Clusters sur AWS, consultez le Guide de déploiement et d'utilisation de Nutanix Cloud Clusters sur AWS.

> **Conseil :**
>
> Cette prise en charge fournit les mêmes fonctionnalités qu'un cluster sur site Nutanix. Un seul cluster est pris en charge, *Prism Element*. Pour plus d'informations, veuillez consulter cette section.

Exigences

Pour utiliser les clusters Nutanix sur AWS, vous avez besoin des éléments suivants :

- Un compte Nutanix.
- Un compte AWS avec les autorisations suivantes :
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Créer un cluster Nutanix

Pour créer un cluster Nutanix :

1. Connectez-vous à votre compte Nutanix.
2. Recherchez l'option **Nutanix Cluster**, puis cliquez sur **Launch**. La **console Nutanix** s'ouvre. Pour plus d'informations, consultez Get Started with Nutanix Cluster on AWS.
3. Choisissez de créer un **nouveau VPC**.

Le processus de création du cluster peut échouer avec les erreurs suivantes :

- Le cluster n'a pas pu être créé dans un délai donné. Suppression du cluster.
- `Cluster Nutanix hôte - Nœud XXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`
- `Cluster Nutanix hôte - Nœud XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`

Si le cluster n'a pas pu être créé :

- Essayez d'en recréer un dans une autre région.
- Assurez-vous de supprimer la pile Nutanix CloudFormation (CFS) avant de réessayer.

En plus d'autres ressources, Nutanix CFS crée :

- 1 VPC nommé *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16
- 2 sous-réseaux 10.0.128.0/24 et 10.0.129.0/24
- 1 passerelle Internet
- 1 passerelle NAT

Une fois le cluster créé, récupérez l'adresse de **Nutanix Prism** :

1. Accédez à la **console Nutanix**.
2. Dans l'angle supérieur droit de la console, passez la souris sur le lien **Launch Prism Element** et copiez l'URL.

Autres ressources

- Installer les composants principaux
- Installer des VDA
- Créer un site
- Pour créer et gérer une connexion avec les solutions cloud et partenaires Nutanix, voir Connexion aux solutions partenaires et cloud Nutanix.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de machines

Environnements de virtualisation VMware

June 27, 2024

Suivez ce guide si vous utilisez VMware pour fournir des machines virtuelles.

Installez vCenter Server et les outils de gestion appropriés. (Aucune prise en charge n'est fournie pour l'opération vSphere vCenter Linked Mode.)

Si vous prévoyez d'utiliser MCS, ne désactivez pas la fonctionnalité de navigateur de banque de données dans vCenter Server (décrite dans https://kb.vmware.com/s/article/2101567). Si vous désactivez cette fonctionnalité, MCS ne fonctionne pas correctement.

Autres ressources

- Installer les composants principaux
- Installer des VDA
- Créer un site
- Pour créer et gérer une connexion dans les environnements VMware, voir Connexion à VMware.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de machines

Solutions VMware Cloud et partenaires

June 27, 2024

Citrix Virtual Apps and Desktops prend en charge les solutions VMware Cloud et partenaires suivantes :

- Azure VMware Solution (AVS)

- Google Cloud VMware Engine
- VMware Cloud sur Amazon Web Services (AWS)

Intégration de la solution Azure VMware (AVS)

Citrix Virtual Apps and Desktops Service prend en charge AVS. AVS fournit une infrastructure cloud contenant des clusters vSphere créés par l'infrastructure Azure. Tirez parti de Citrix Virtual Apps and Desktop Service pour utiliser AVS pour provisionner votre charge de travail VDA de la même manière que vous utiliseriez vSphere dans des environnements locaux.

Configurer le cluster AVS

Pour permettre à Citrix Virtual Apps and Desktop Service d'utiliser AVS, effectuez les opérations suivantes dans Azure :

- Demander un quota d'hôtes
- Enregistrer le fournisseur de ressources Microsoft.AVS
- Liste de contrôle du réseau
- Créer un cloud privé pour la solution Azure VMware
- Accéder à un cloud privé avec la solution Azure VMware
- Configurer la mise en réseau de votre cloud privé VMware dans Azure
- Configurer DHCP pour la solution Azure VMware
- Ajouter un segment réseau dans la solution Azure VMware
- Vérifier l'environnement de la solution Azure VMware

Demander un quota d'hôte pour les clients Azure Enterprise Agreement Dans la page **Aide + Support** du portail Azure, sélectionnez **Nouvelle demande de support**et incluez les informations suivantes :

- Type de problème : technique
- Abonnement : sélectionnez votre abonnement
- Service :Tous les services > Solution Azure VMware
- Ressource : Question générale
- Résumé : Besoin de capacité
- Type de problème : problèmes de gestion de la capacité
- Sous-type de problème : demande client de quota/capacité d'hôte supplémentaire

Dans la **description** du ticket d'assistance, incluez les informations suivantes dans l'onglet **Détails** :

- POC ou Production

- Nom de la région
- Nombre d'hôtes
- Tout autre détail

> **Remarque :**
>
> AVS nécessite un minimum de trois hôtes et vous recommande d'utiliser la redondance d'hôtes N+1.

Après avoir spécifié les détails du ticket de support, sélectionnez **Examiner et créer** pour envoyer la demande à Azure.

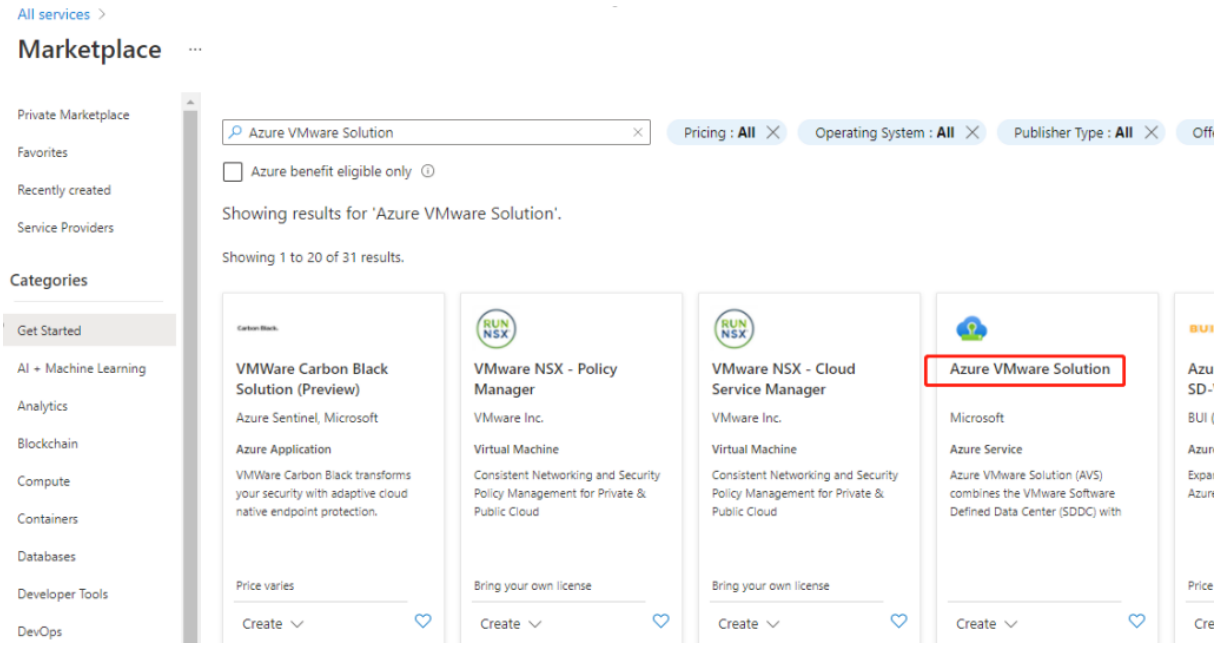
Enregistrer le fournisseur de ressources Microsoft.AVS Après avoir demandé le quota d'hôte, enregistrez le fournisseur de ressources :

1. Connectez-vous au portail Azure.
2. Dans le menu du portail Azure, sélectionnez **Tous les services**.
3. Dans le menu **Tous les services**, saisissez l'abonnement, puis sélectionnez **Abonnements**.
4. Sélectionnez l'abonnement dans la liste des abonnements.
5. Sélectionnez **Fournisseurs de ressources** et saisissez **Microsoft.AVS** dans la barre de recherche.
6. Si le fournisseur de ressources n'est pas enregistré, sélectionnez **Enregistrer**.

Considérations sur le réseau AVS propose des services de mise en réseau nécessitant des plages d'adresses réseau et des ports de pare-feu spécifiques. Pour plus d'informations, consultez la liste de contrôle de planification de la mise en réseau pour la solution Azure VMware.

Créer un cloud privé pour la solution Azure VMware Après avoir pris en compte les exigences réseau de votre environnement, créez un cloud privé ASV :

1. Connectez-vous au portail Azure.
2. Sélectionnez **Créer une nouvelle ressource**.
3. Dans la zone de texte **Rechercher dans le marketplace**, tapez *Solution Azure VMware*, puis sélectionnez **Solution Azure VMware** dans la liste.



Image

Dans la fenêtre **Solution Azure VMware** :

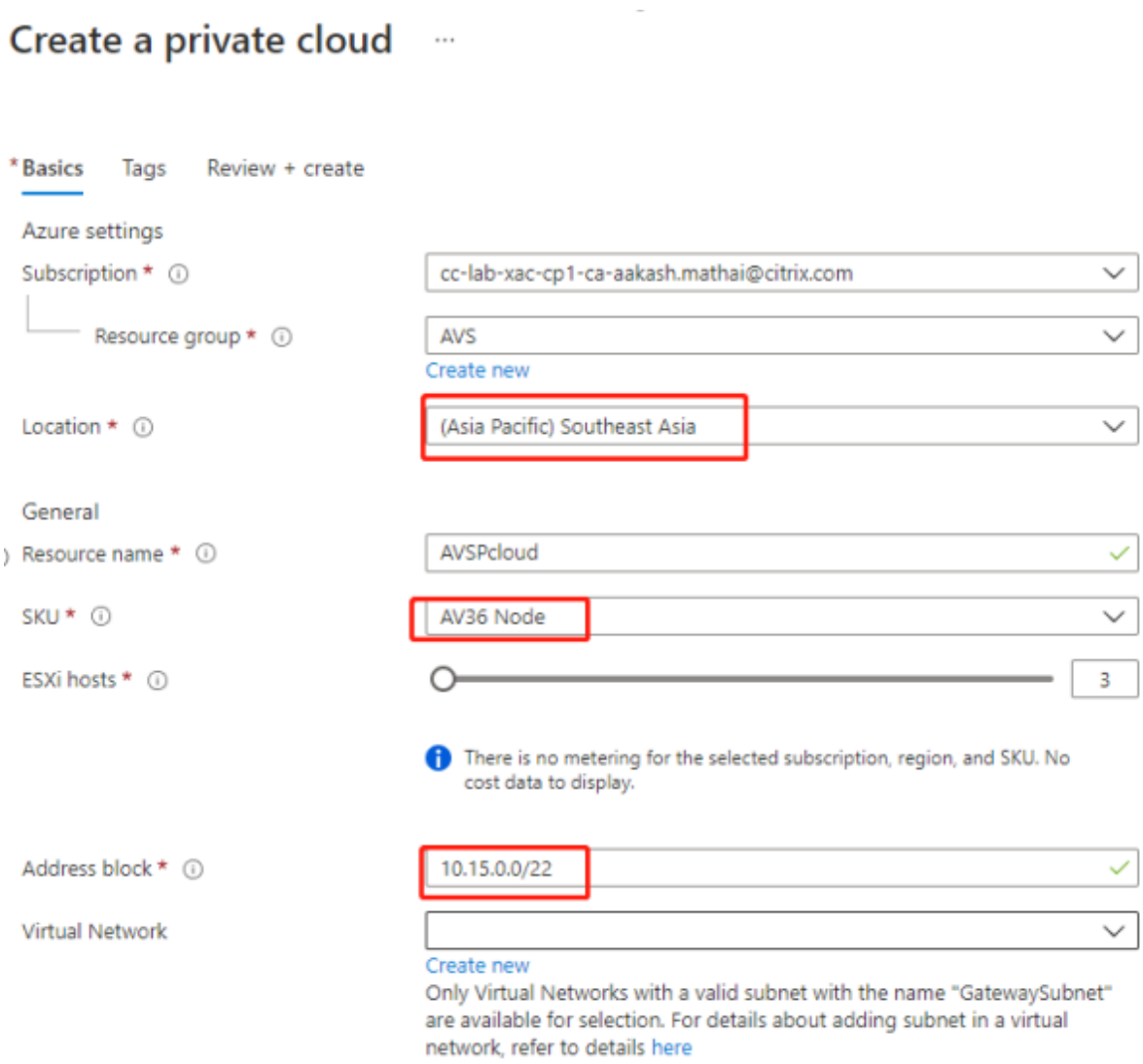
1. Sélectionnez **Créer**.
2. Cliquez sur l'onglet **Options de base**.
3. Entrez des valeurs pour les champs, en utilisant les informations du tableau ci-dessous :

Champ	Valeur
Abonnement	Sélectionnez l'abonnement que vous prévoyez d'utiliser pour le déploiement. Toutes les ressources d'un abonnement Azure sont facturées ensemble.
Groupe de ressources	Sélectionnez le groupe de ressources de votre cloud privé. Un groupe de ressources Azure est un conteneur logique dans lequel les ressources Azure sont déployées et gérées. Vous pouvez également créer un nouveau groupe de ressources pour votre cloud privé.
Emplacement	Sélectionnez un emplacement, par exemple East US. Il s'agit de la région que vous avez définie au cours de la phase de planification.
Nom de la ressource	Indiquez le nom de votre cloud privé pour la solution Azure VMware.
SKU	Sélectionnez AV36.

Champ	Valeur
Hôtes	Affiche le nombre d'hôtes alloués au cluster de cloud privé. La valeur par défaut est 3, qui peut être augmentée ou réduite après le déploiement.
Bloc d'adresses	Fournissez un bloc d'adresses IP pour le cloud privé. Le CIDR représente le réseau de gestion du cloud privé et sera utilisé pour les services de gestion de cluster, tels que vCenter Server et NSX-T Manager. Utilisez l'espace d'adressage /22, par exemple 10.175.0.0/22. L'adresse doit être unique et ne pas chevaucher d'autres réseaux virtuels Azure ni des réseaux locaux.
Réseau virtuel	Laissez ce champ vide car le circuit ExpressRoute de la solution Azure VMware est établi en tant qu'étape de post-déploiement.

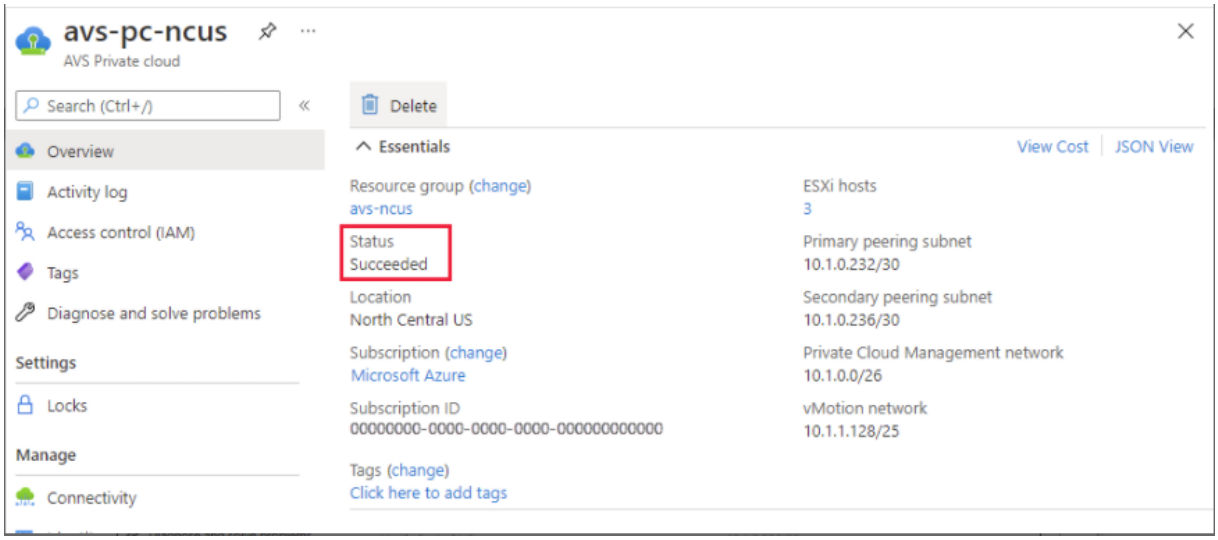
Dans l'écran **Créer un cloud privé** :

1. Dans le champ **Emplacement**, sélectionnez la région qui contient l'AVS. La région du groupe de ressources est identique à la région AVS.
2. Dans le champ **SKU**, sélectionnez **AV36 Node**.
3. Spécifiez une adresse IP dans le champ **Bloc d'adresses**. Par exemple, 10.15.0.0/22.
4. Sélectionnez **Réviser+Créer**.
5. Après avoir examiné les informations, cliquez sur **Créer**.



> **Conseil :**
>
> La création d'un cloud privé peut prendre 3 à 4 heures. L'ajout d'un seul hôte au cluster peut prendre de 30 à 45 minutes.

Vérifiez que le déploiement a réussi. Accédez au groupe de ressources que vous avez créé et sélectionnez votre cloud privé. Lorsque l'**état** indique **Réussi**, le déploiement est terminé.



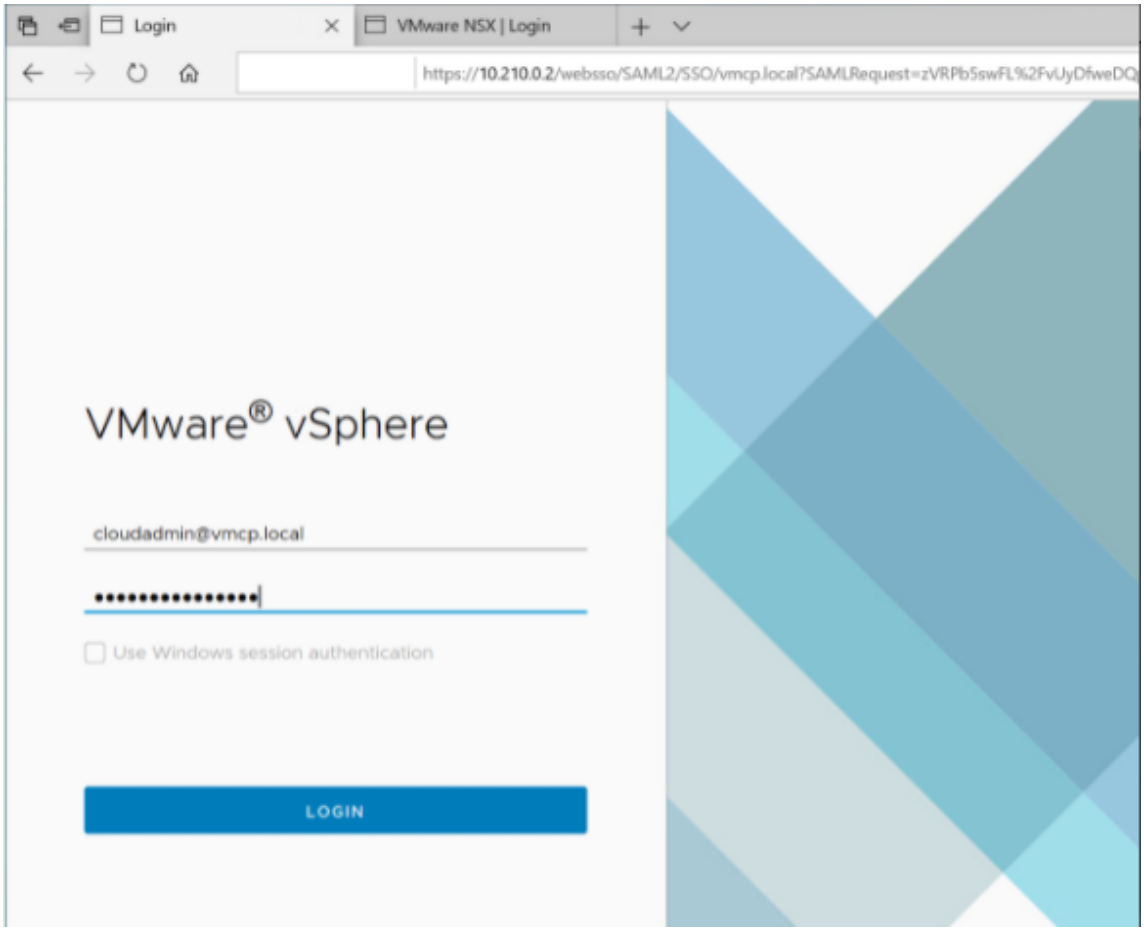
Accéder à un cloud privé avec la solution Azure VMware Une fois que vous avez créé un cloud privé, créez une machine virtuelle Windows et connectez-vous au vCenter local de votre cloud privé.

Créer une machine virtuelle Windows

1. Dans le groupe de ressources, sélectionnez **+ Ajouter**, puis recherchez et sélectionnez **Microsoft Windows 10/2016/2019**.
2. Cliquez sur **Créer**.
3. Saisissez les informations requises, puis sélectionnez **Réviser+Créer**.
4. Une fois la validation terminée, sélectionnez **Créer** pour lancer le processus de création de machine virtuelle.

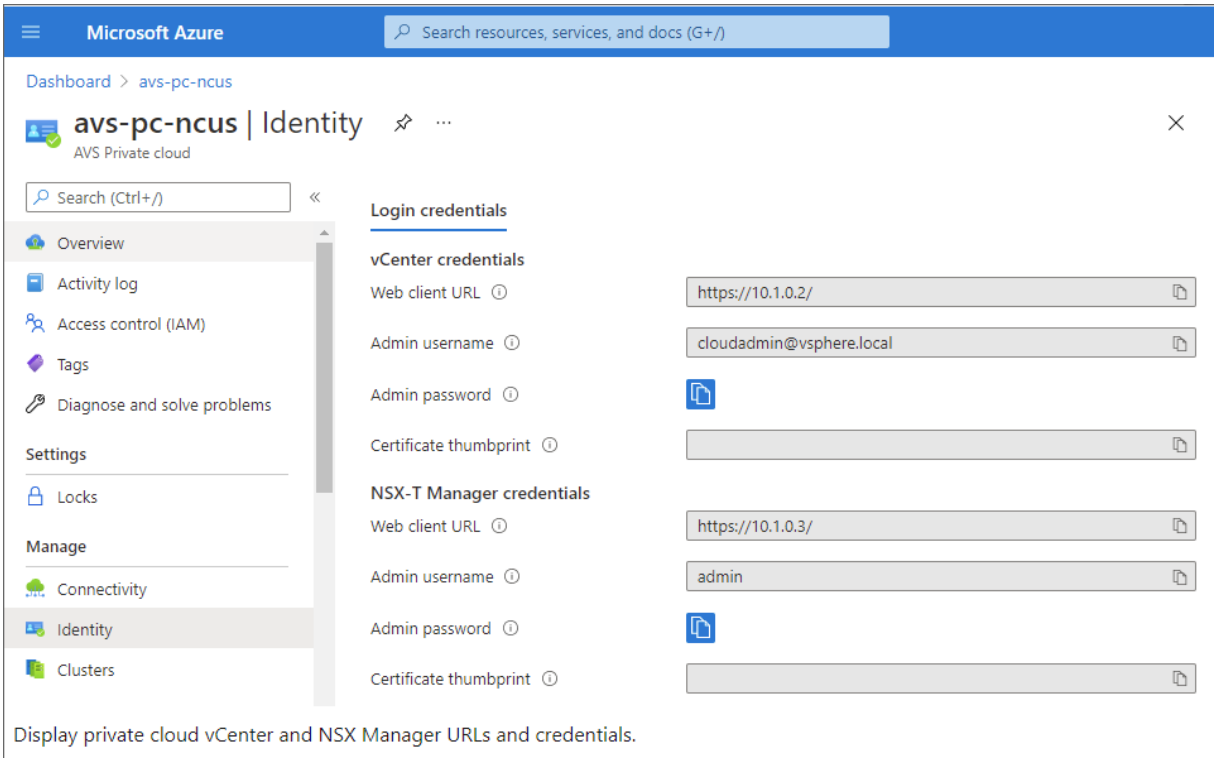
Se connecter au vCenter local de votre cloud privé

1. Connectez-vous à **vSphere Client avec VMware vCenter SSO** en tant qu'administrateur cloud.



2. Dans le portail Azure, sélectionnez votre cloud privé, puis **Gérer > Identité**.

Les URL et informations d'identification de l'utilisateur pour vCenter et NSX-T Manager dans le cloud privé s'affichent :



Display private cloud vCenter and NSX Manager URLs and credentials.

Après avoir confirmé les URL et les informations d'identification de l'utilisateur :

1. Accédez à la machine virtuelle que vous avez créée à l'étape précédente et connectez-vous à la machine virtuelle.
2. Dans la machine virtuelle Windows, ouvrez un navigateur et accédez aux URL du vCenter et de NSX-T Manager dans deux onglets de navigateur. Dans l'onglet vCenter, saisissez les informations d'identification de l'utilisateur, *cloudadmin@vmcp.local*, de l'étape précédente.

Configurer la mise en réseau de votre cloud privé VMware dans Azure Après avoir accédé à un cloud privé ASV, configurez la mise en réseau en créant un réseau virtuel et une passerelle.

Créer un réseau virtuel

1. Connectez-vous au portail Azure.
2. Accédez au groupe de ressources créé précédemment.
3. Sélectionnez **+ Ajouter** pour définir une nouvelle ressource.
4. Dans la zone de texte **Rechercher dans le marketplace**, tapez *réseau virtuel*. Recherchez la ressource de réseau virtuel et sélectionnez-la.
5. Sur la page **Réseau virtuel**, sélectionnez **Créer** pour configurer le réseau virtuel pour votre cloud privé.
6. Sur la page **Créer un réseau virtuel**, saisissez les détails de votre réseau virtuel.

7. Dans l'onglet **Options de base**, saisissez un nom pour le réseau virtuel, sélectionnez la région appropriée, puis cliquez sur **Suivant : Adresses IP**.
8. Dans l'onglet **Adresses IP**, sous Espace d'adressage IPv4, saisissez l'adresse créée précédemment.

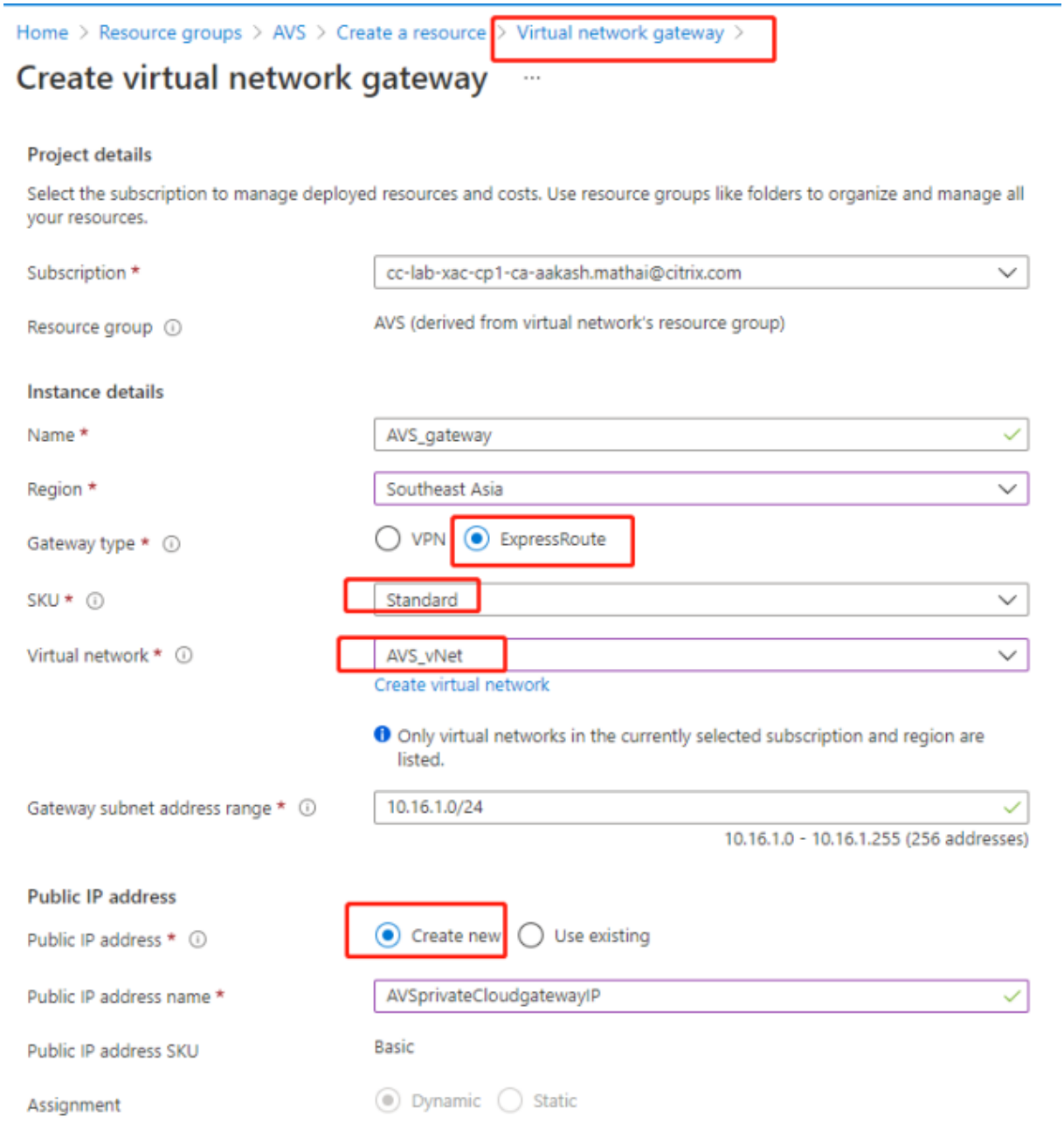
> **Important :**
>
> Utilisez une adresse qui ne chevauche pas l'espace d'adressage que vous avez utilisé lors de la création de votre cloud privé.

Après avoir entré l'espace d'adressage :

1. Sélectionnez **+ Ajouter un sous-réseau**.
2. Sur la page **Ajouter un sous-réseau**, attribuez au sous-réseau un nom et une plage d'adresses appropriée.
3. Cliquez sur **Ajouter**.
4. Sélectionnez **Réviser+Créer**.
5. Vérifiez les informations et cliquez sur **Créer**. Une fois le déploiement terminé, le réseau virtuel apparaît dans le groupe de ressources.

Créer une passerelle de réseau virtuel Après avoir créé un réseau virtuel, créez une passerelle de réseau virtuel.

1. Dans votre groupe de ressources, sélectionnez **+ Ajouter** pour ajouter une nouvelle ressource.
2. Dans la zone de texte **Rechercher dans le marketplace**, tapez *passerelle de réseau virtuel*. Recherchez la ressource de réseau virtuel et sélectionnez-la.
3. Sur la page **Passerelle de réseau virtuel**, cliquez sur **Créer**.
4. Dans l'onglet **Options de base** de la page **Créer une passerelle de réseau virtuel**, indiquez des valeurs pour les champs.
5. Cliquez sur **Réviser + Créer**.

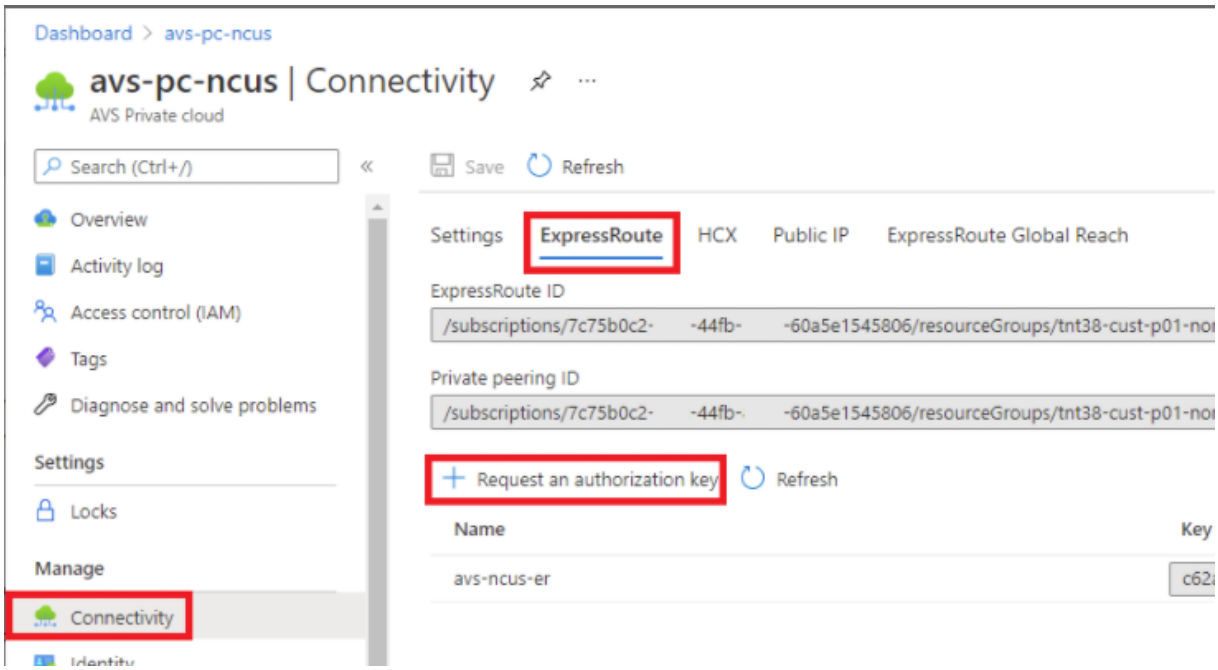


Après avoir examiné la configuration de la passerelle du réseau virtuel, cliquez sur **Créer** pour déployer votre passerelle de réseau virtuel.
Une fois le déploiement terminé, connectez votre connexion **ExpressRoute** à la passerelle de réseau virtuel contenant votre cloud privé Azure AVS.

Connecter ExpressRoute à la passerelle de réseau virtuel Après avoir déployé une passerelle de réseau virtuel, ajoutez une connexion entre celle-ci et votre cloud privé Azure AVS :

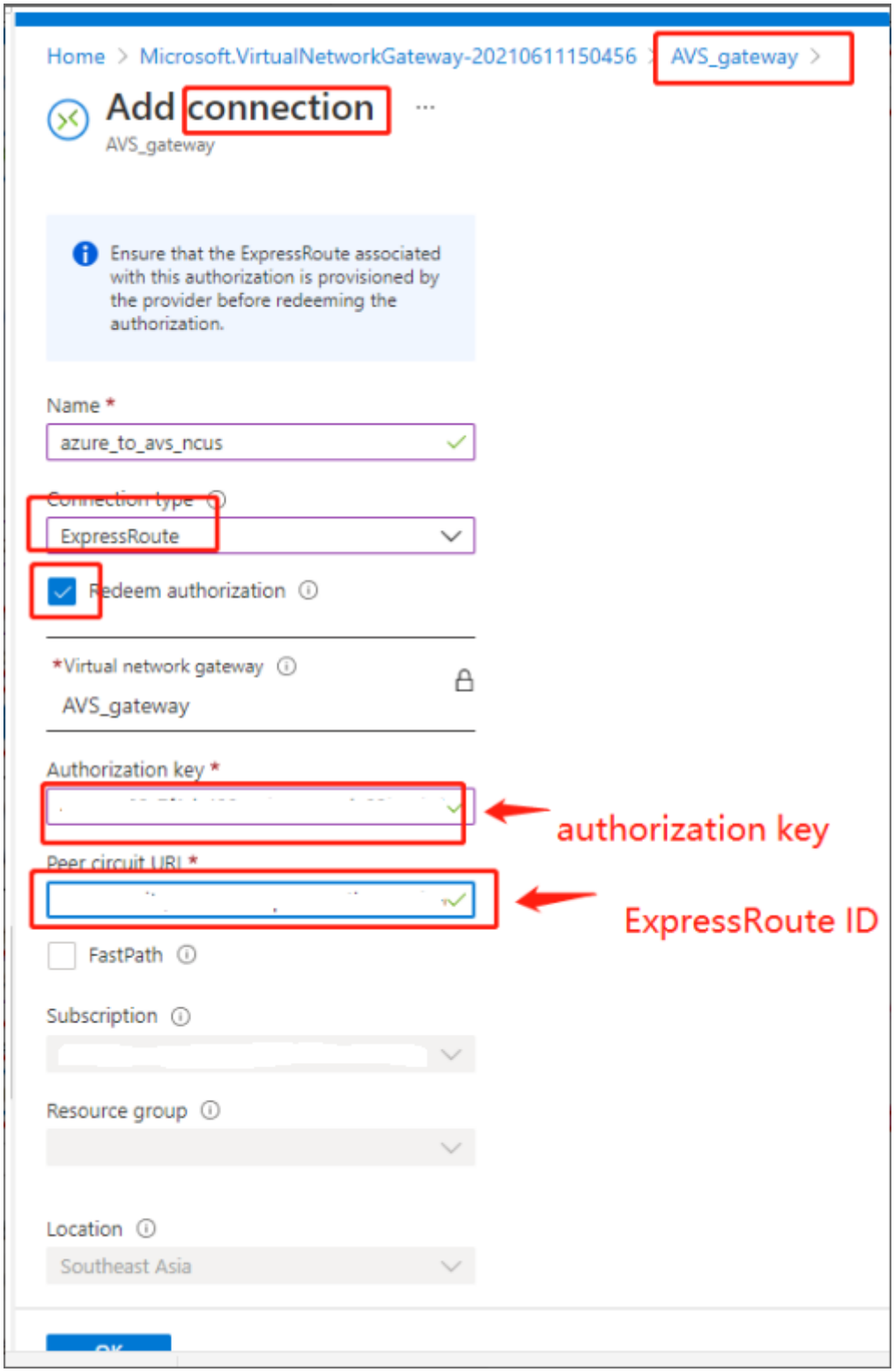
1. Demandez une clé d'autorisation ExpressRoute.

2. Dans le portail Azure, accédez au **cloud privé de la solution Azure VMware**. Sélectionnez **Gérer > Connectivité > ExpressRoute**, puis sélectionnez **+ Demander une clé d'autorisation**.

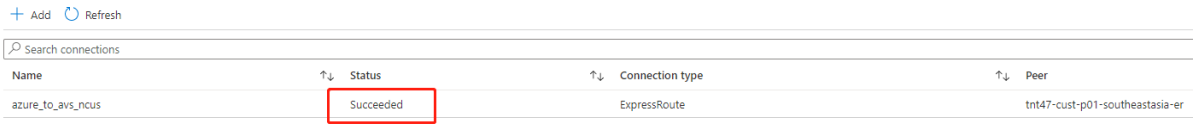


Après avoir demandé une clé d'autorisation :

1. Entrez un nom pour la clé et cliquez sur **Créer**. La création de la clé peut prendre environ 30 secondes. Une fois créée, la nouvelle clé apparaît dans la liste des clés d'autorisation du cloud privé.
2. Copiez la **clé d'autorisation** et l'**ID ExpressRoute**. Vous en aurez besoin pour terminer le processus d'appairage. La clé d'autorisation disparaît après un certain temps, alors copiez-la dès qu'elle apparaît.
3. Accédez à la **passerelle de réseau virtuel** que vous prévoyez d'utiliser et sélectionnez **Connexions > + Ajouter**.
4. Sur la page **Ajouter une connexion**, indiquez des valeurs pour les champs, puis sélectionnez **OK**.



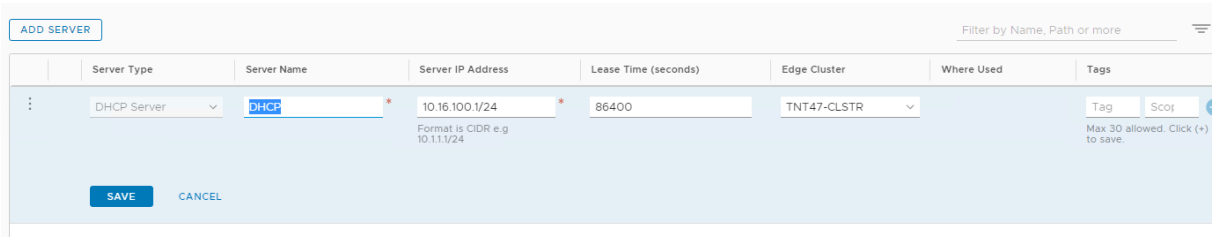
La connexion est établie entre votre circuit ExpressRoute et votre réseau virtuel :



Configurer DHCP pour la solution Azure VMware Après avoir connecté ExpressRoute à la passerelle virtuelle, configurez DHCP.

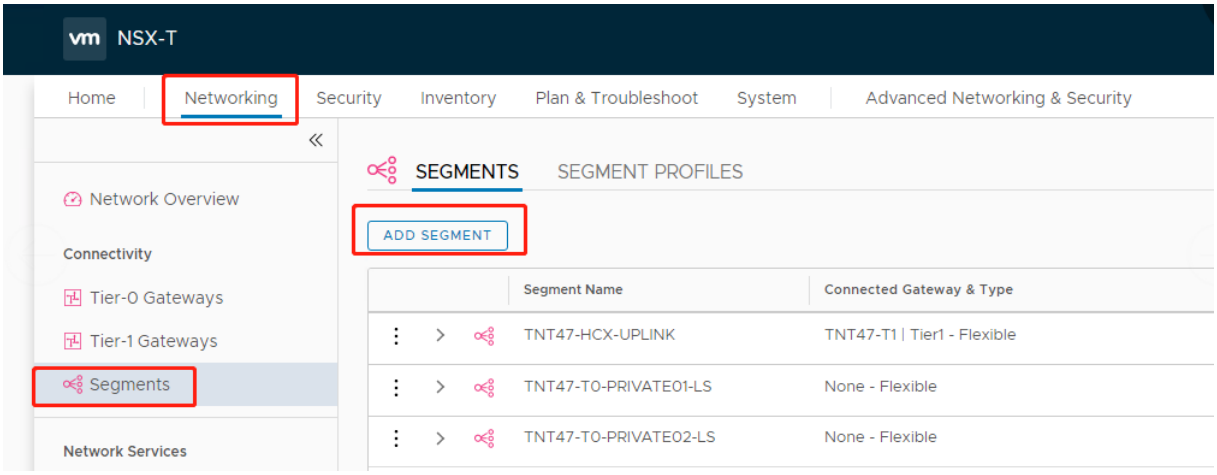
Utiliser NSX-T pour héberger votre serveur DHCP Dans NSX-T Manager :

1. Sélectionnez **Networking> DHCP**, puis **Add Server**.
2. Sélectionnez **DHCP** pour **Server Type**, indiquez le nom et l'adresse IP du serveur.
3. Cliquez sur **Enregistrer**.
4. Sélectionnez **Tier 1 Gateways**, sélectionnez les points de suspension verticaux sur la passerelle de niveau 1, puis sélectionnez **Edit**.
5. Sélectionnez **No IP Allocation Set** pour ajouter un sous-réseau.
6. Sélectionnez **DHCP Local Server** pour **Type**.
7. Pour **DHCP Server**, sélectionnez **Default DHCP**, puis cliquez sur **Save**.
8. Cliquez à nouveau sur **Save**, puis sélectionnez **Close Editing**.



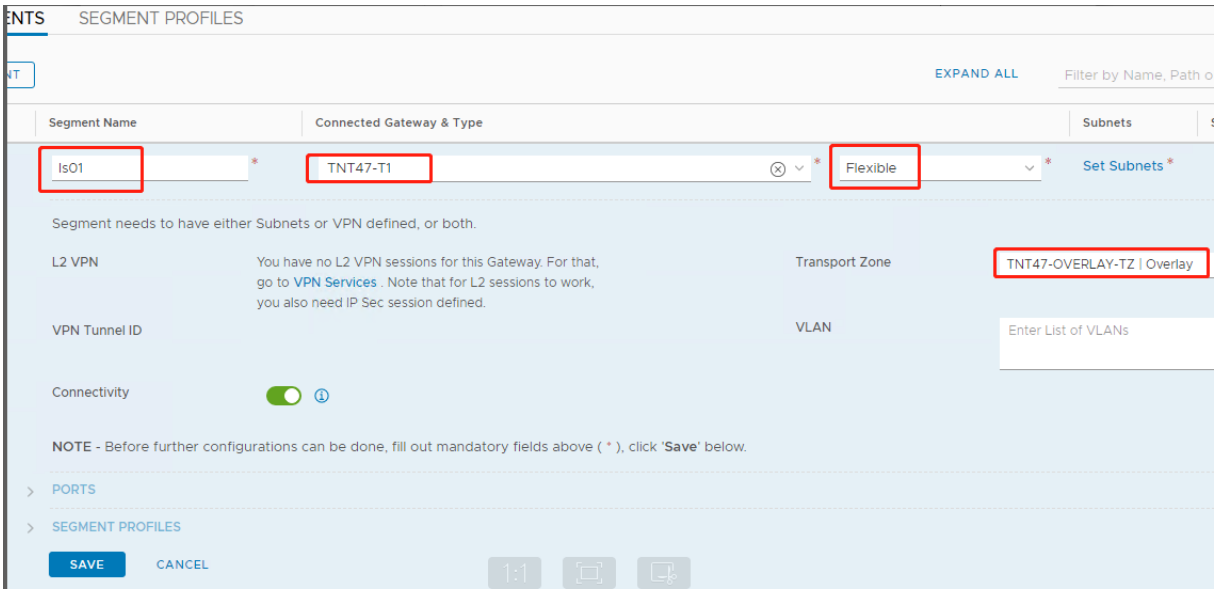
Ajouter un segment réseau dans la solution Azure VMware Après avoir configuré DHCP, ajoutez un segment de réseau.

Pour ajouter un segment de réseau, dans NSX-T Manager, sélectionnez **Networking > Segments**, puis cliquez sur **Add Segment**.



Dans l'écran **Segments profile** :

1. Entrez un **nom** pour le segment.
2. Sélectionnez **Tier-1 Gateway (TNTxx-T1)** pour **Connected Gateway** et laissez **Type** défini sur**Flexible**.
3. Sélectionnez la superposition préconfigurée **Transport Zone(TNTxx-OVERLAY-TZ)**.
4. Cliquez sur **Set Subnets**.



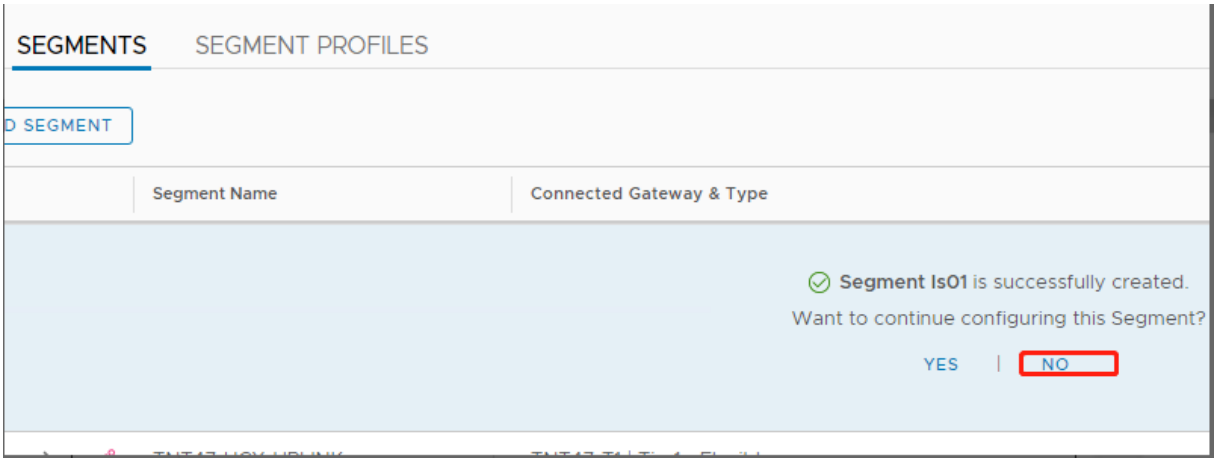
Dans la section **Subnets** :

1. Entrez l'adresse IP de la passerelle.
2. Sélectionnez **Add**.

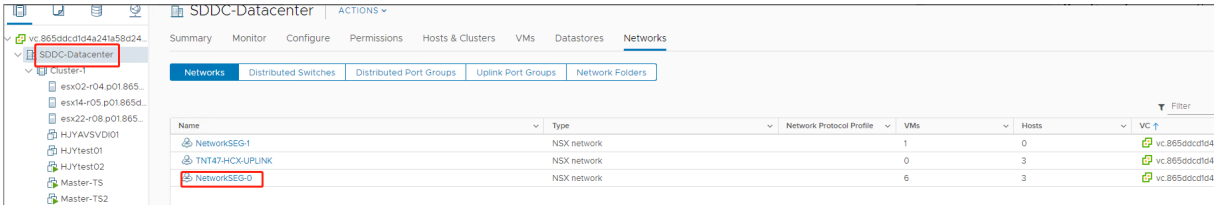
> **Important :**
>
> Cette adresse IP de segment doit appartenir à l'adresse IP de la passerelle Azure, 10.15.0.0/22.

La plage DHCP doit appartenir à l'adresse IP de segment :

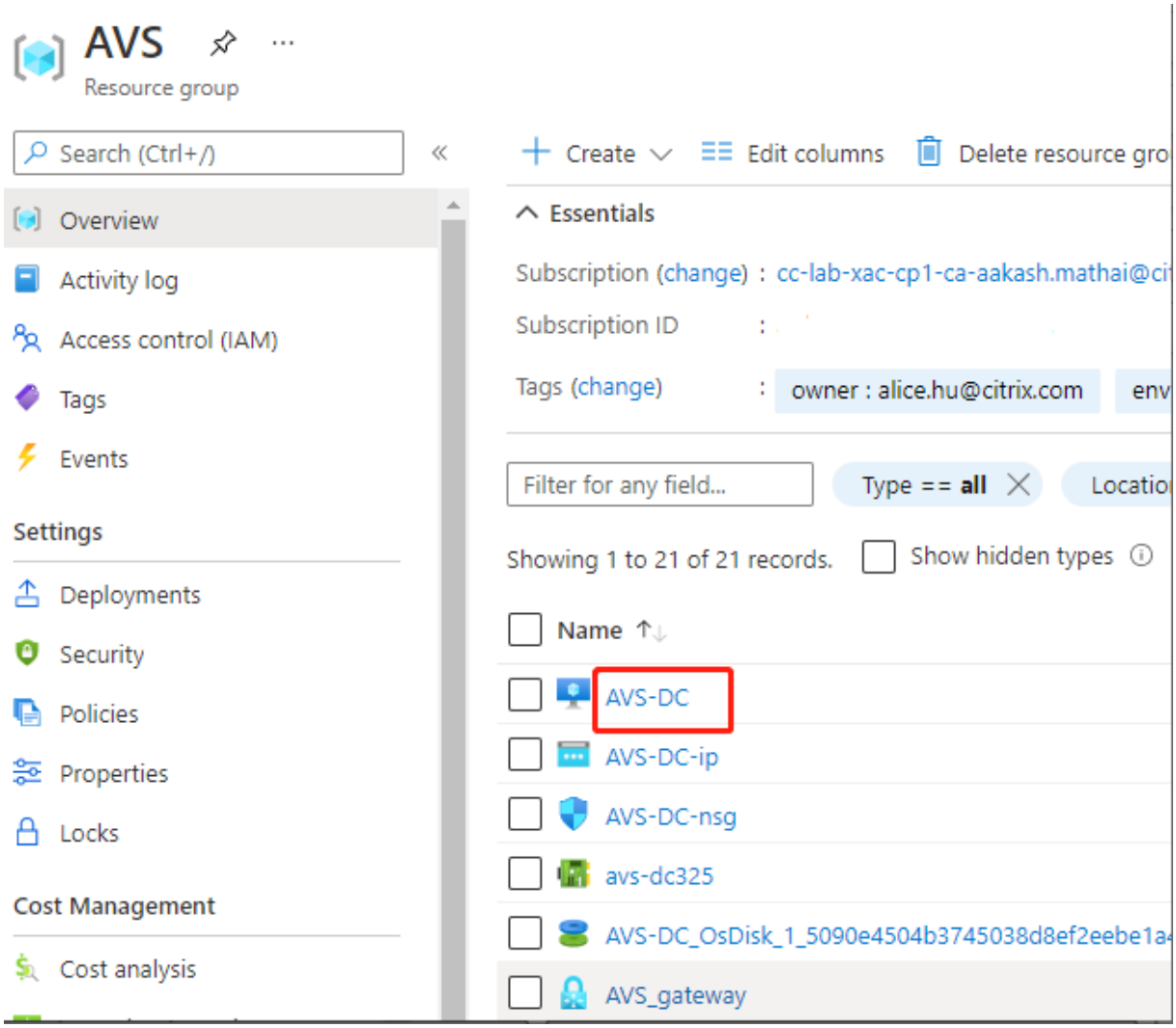
Sélectionnez **No** pour refuser l'option de continuer à configurer le segment :



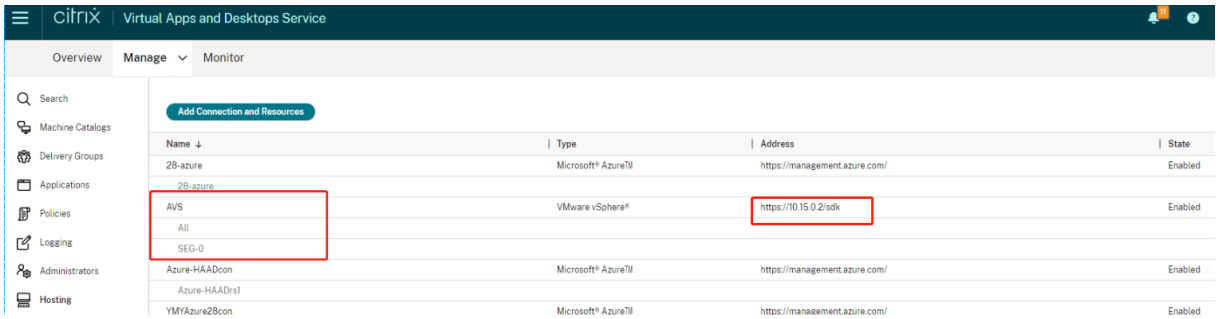
Dans vCenter, sélectionnez **Networking > SDDC-Datacenter** :



Vérifier l'environnement Azure AVS Configurez une connexion directe et un connecteur dans le groupe de ressources Azure :



Vérifiez la connexion avec les informations d'identification de vCenter :



Google Cloud VMware Engine

Citrix Virtual Apps and Desktops vous permet de migrer des charges de travail Citrix locales basées sur VMware vers Google Cloud VMware Engine.

Configurer Google Cloud VMware Engine

La procédure suivante explique comment acquérir et configurer un cluster sur Google Cloud VMware Engine.

Accéder au portail VMware Engine

1. Dans **Google Cloud Console**, cliquez sur le menu de navigation.
2. Dans la section **Compute**, cliquez sur **VMware Engine** pour ouvrir VMware Engine dans un nouvel onglet de navigateur.

Conditions requises pour créer le premier cloud privé Vous devez avoir accès à Google Cloud VMware Engine, au quota de nœuds VMware Engine disponible et à un rôle IAM approprié. Préparez les conditions suivantes avant de continuer à créer votre cloud privé :

1. Demandez un accès à l'API et un quota de nœuds. Pour plus d'informations, consultez Demande d'accès à l'API et de quota.
2. Notez les plages d'adresses que vous souhaitez utiliser pour les dispositifs de gestion VMware et le réseau de déploiement HCX. Pour plus d'informations, consultez la section Configuration réseau requise.
3. Obtenez le rôle IAM d'administrateur de service VMware Engine.

Créer votre premier cloud privé

1. Accédez au portail VMware Engine.
2. Sur la page d'accueil de VMware Engine, cliquez sur **Créer un cloud privé**. L'emplacement d'hébergement et les types de nœuds matériels sont répertoriés.
3. Sélectionnez le nombre de nœuds pour le cloud privé. Au moins trois nœuds sont nécessaires.
4. Entrez une plage CIDR (Classless Inter-Domain Routage) pour le réseau de gestion VMware.
5. Entrez une plage CIDR pour le réseau de déploiement HCX.

   > **Important :**
   >
   > La plage CIDR ne doit chevaucher aucun de vos sous-réseaux locaux ou cloud. La plage CIDR doit être supérieure ou égale à /27.

6. Sélectionnez **Vérifier et créer**.
7. Vérifiez les paramètres. Pour modifier les paramètres, cliquez sur **Précédent**.
8. Cliquez sur **Créer** pour commencer à créer le cloud privé.

Au fur et à mesure que VMware Engine crée votre nouveau cloud privé, il déploie plusieurs composants VMware et définit des stratégies d'autoscaling automatique initiales pour les clusters dans le cloud privé. La création d'un cloud privé peut prendre de 30 minutes à 2 heures. Une fois le provisioning terminé, vous recevez un e-mail.

Configurer la passerelle VPN Google Cloud VMware Engine Pour établir une connectivité initiale à Google Cloud VMware Engine, vous pouvez utiliser une passerelle VPN. Il s'agit d'un VPN client basé sur OpenVPN à l'aide duquel vous pouvez vous connecter à votre vCenter VMware Software Defined Data Center (SDDC) et effectuer toute configuration initiale requise.

Avant de déployer la passerelle VPN, configurez la plage **Services Edge** pour la région où votre SDDC est déployé. Pour ce faire :

1. Ouvrez une session sur le portail **Google Cloud VMware Engine** et accédez à **Réseau > Paramètres régionaux**. Cliquez sur **Ajouter une région**.
2. Choisissez la région où votre SDDC est déployé et activez **Accès Internet** et **Service IP public**.
3. Indiquez la plage Services Edge notée lors de la planification et cliquez sur **Soumettre**. L'activation de ces services prend 10 à 15 minutes.

   Une fois l'opération terminée, les services Edge s'affichent comme **activés** sur la page Paramètres régionaux. L'activation de ces paramètres permet d'allouer des adresses IP publiques à votre SDDC, ce qui est une condition requise pour déployer une passerelle VPN.

Pour déployer une passerelle VPN :

1. Sur le portail **Google Cloud VMware Engine**, accédez à **Network > VPN Gateways**. Cliquez sur **Create New VPN Gateway**.
2. Indiquez le nom de la passerelle VPN et du sous-réseau client réservés lors de la planification. Cliquez sur **Suivant**.
3. Sélectionnez les utilisateurs auxquels accorder l'accès VPN. Cliquez sur **Suivant**.
4. Spécifiez les réseaux qui doivent être accessibles via VPN. Cliquez sur **Suivant**.
5. Un écran récapitulatif s'affiche. Vérifiez les sélections, puis cliquez sur **Submit** pour créer la passerelle VPN. La page VPN Gateways s'affiche avec l'état de la nouvelle passerelle VPN défini sur **Creating**.
6. Une fois que l'état passe à **Operational**, cliquez sur la nouvelle passerelle VPN.
7. Cliquez sur **Download my VPN configuration** pour télécharger un fichier ZIP contenant des profils OpenVPN préconfigurés pour la passerelle VPN. Des profils pour la connexion via UDP/1194 et TCP/443 sont disponibles. Choisissez votre préférence et importez-la dans Open VPN, puis connectez-vous.
8. Accédez à **Resources** et sélectionnez votre SDDC.

Connecter le VPN

1. Établissez une connexion point à site entre votre réseau sur site et le cloud privé via la configuration de la passerelle VPN. Consultez Configurer la passerelle VPN Google Cloud VMware Engine.
2. Chargez la configuration VPN téléchargée lors de l'étape décrite dans Configurer la passerelle VPN Google Cloud VMware Engine.
3. Importez le fichier vers votre client VPN, par exemple, OpenVPN Connect.

Pour plus d'informations, consultez la section Se connecter à l'aide d'un VPN.

Créer le premier sous-réseau

Accéder à NSX-T Manager à partir du portail VMware Engine Le processus de création d'un sous-réseau se déroule dans NSX-T, auquel vous accédez via VMware Engine. Procédez comme suit pour accéder à NSX-T Manager.

1. Ouvrez une session sur le portail **Google Cloud VMware Engine**.
2. Dans le menu de navigation principal, accédez à **Resources**.
3. Sous **Private cloud name**, cliquez sur le nom du cloud privé correspondant au cloud privé sur lequel vous souhaitez créer le sous-réseau.
4. Sur la page de détails de votre cloud privé, cliquez sur l'onglet **vSphere Management Network**.
5. Sous **FQDN**, cliquez sur le nom de domaine complet correspondant à NSX-T Manager.
6. Lorsque vous y êtes invité, saisissez vos informations d'identification de connexion. Si vous avez configuré vIDM et que vous l'avez connecté à une source d'identité, telle qu'Active Directory, utilisez vos informations d'identification de source d'identité à la place.

   > **Rappel :**
   >
   > Vous pouvez récupérer les informations d'identification générées à partir de la page de détails du cloud privé.

Configurer le service DHCP pour le sous-réseau Avant de créer un sous-réseau, configurez un service DHCP :

Dans NSX-T Manager :

1. Accédez à **Networking > DHCP**. Le tableau de bord réseau indique que le service DHCP crée une passerelle de niveau 0 et une passerelle de niveau 1.
2. Pour commencer à provisionner un serveur DHCP, cliquez sur **Add Server**.
3. Sélectionnez **DHCP** pour **Server Type**, indiquez le nom et l'adresse IP du serveur.
4. Cliquez sur **Save** pour créer le service DHCP.

Procédez comme suit pour attacher ce service DHCP à la passerelle de niveau 1 appropriée. Une passerelle de niveau 1 par défaut est déjà configurée par le service DHCP :

1. Sélectionnez **Tier 1 Gateways**, sélectionnez les points de suspension verticaux sur la passerelle de niveau 1, puis sélectionnez **Edit**.
2. Dans le champ **No IP Allocation Set**, sélectionnez **No IP Allocation Set**.
3. Sélectionnez **DHCP Local Server** pour **Type**.
4. Sélectionnez le serveur DHCP que vous avez créé pour **DHCP Server**.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Close Editing**.

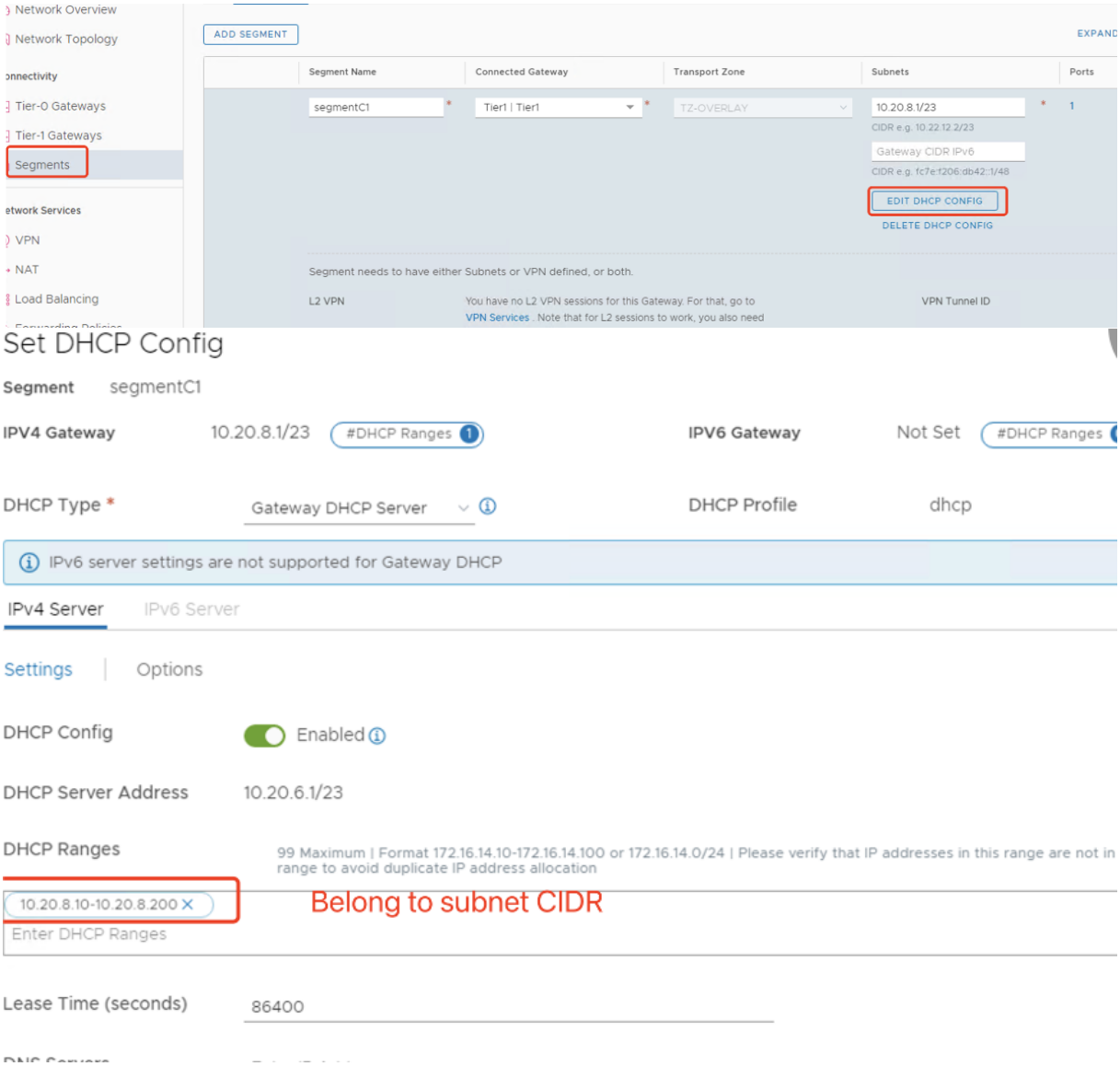
Vous pouvez désormais créer un segment de réseau dans NSX-T. Pour plus d'informations sur DHCP dans NSX-T, consultez la documentation VMware relative à DHCP.

Créer un segment de réseau dans NSX-T Pour les machines virtuelles de charge de travail, vous créez des sous-réseaux en tant que segments de réseau NSX-T pour votre cloud privé :

1. Dans NSX-T Manager, accédez à **Network > Segments**.
2. Cliquez sur **Add Segment**.
3. Entrez un nom pour le segment.
4. Sélectionnez **Tier-1** pour **Connected Gateway** et laissez Type défini sur **Flexible**.
5. Cliquez sur **Set Subnets**.
6. Cliquez sur **Add Subnets**.
7. Entrez la plage de sous-réseaux dans **Gateway IP/Prefix Length**. Spécifiez la plage de sous-réseau avec **.1** comme dernier octet. Par exemple, **10.12.2.1/24**.
8. Spécifiez les plages DHCP et cliquez sur **ADD**.
9. Dans **Transport Zone**, sélectionnez **TZ-OVERLAY** dans la liste déroulante.
10. Cliquez sur **Enregistrer**. Vous pouvez désormais sélectionner ce segment de réseau dans vCenter lors de la création d'une machine virtuelle.

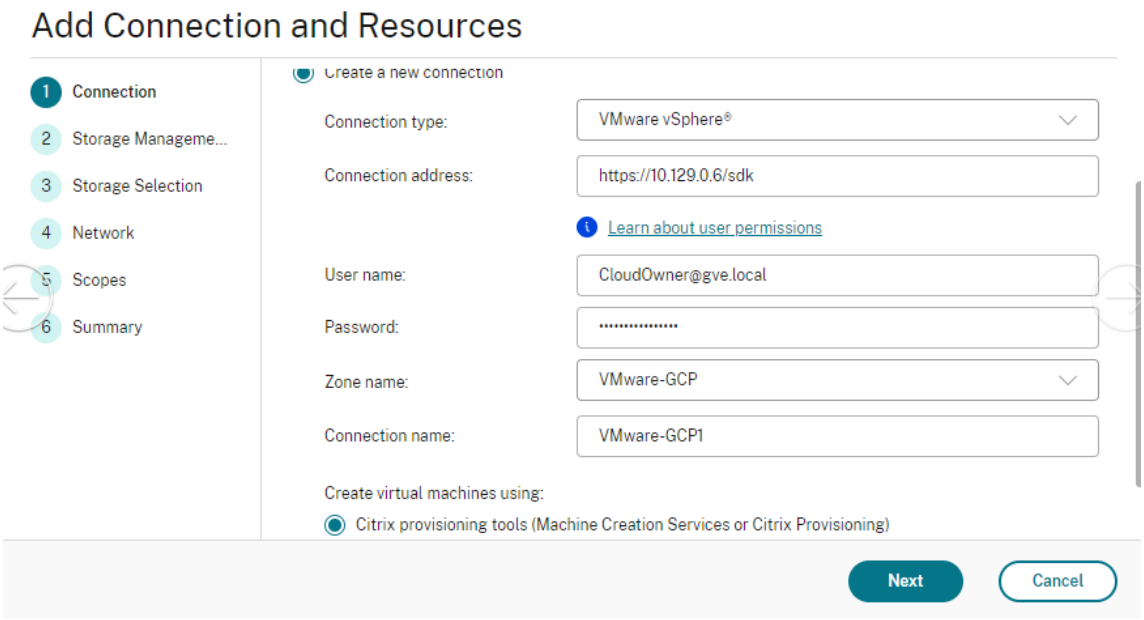
Dans une région donnée, vous pouvez configurer au plus 100 itinéraires uniques entre VMware Engine et votre réseau VPC à l'aide d'un accès aux services privés. Cela inclut, par exemple, les plages d'adresses IP de gestion du cloud privé, les segments de réseau de charge de travail NSX-T et les plages d'adresses IP du réseau HCX. Cette limite inclut tous les clouds privés de la région.

> **Remarque :**
>
> Un problème de configuration Google Cloud vous force à configurer le paramètre de plage DHCP plusieurs fois. Par conséquent, assurez-vous de configurer le paramètre de plage DHCP après la configuration Google Cloud. Cliquez sur **EDIT DHCP CONFIG** pour configurer les plages DHCP.



Créez la connexion Google Cloud VMware dans Citrix Studio

1. Créez une machine dans vCenter.
2. Lancez Citrix Studio.
3. Sélectionnez le nœud d'hébergement, puis cliquez sur **Ajouter une connexion et des ressources**.
4. Sur l'écran **Connexion**, sélectionnez **Créer une nouvelle connexion** et les détails suivants :



a) Sélectionnez **VMware vSphere** comme **Type de connexion**.
b) Dans la zone **Adresse de connexion**, entrez l'adresse IP privée de vCenter.
c) Entrez les informations d'identification de vCenter.
d) Entrez un nom pour la connexion.
e) Choisissez l'outil pour créer des machines virtuelles.

5. Sur l'écran **Réseau**, sélectionnez le sous-réseau créé dans le serveur NSX-T.
6. Suivez les instructions de l'assistant.

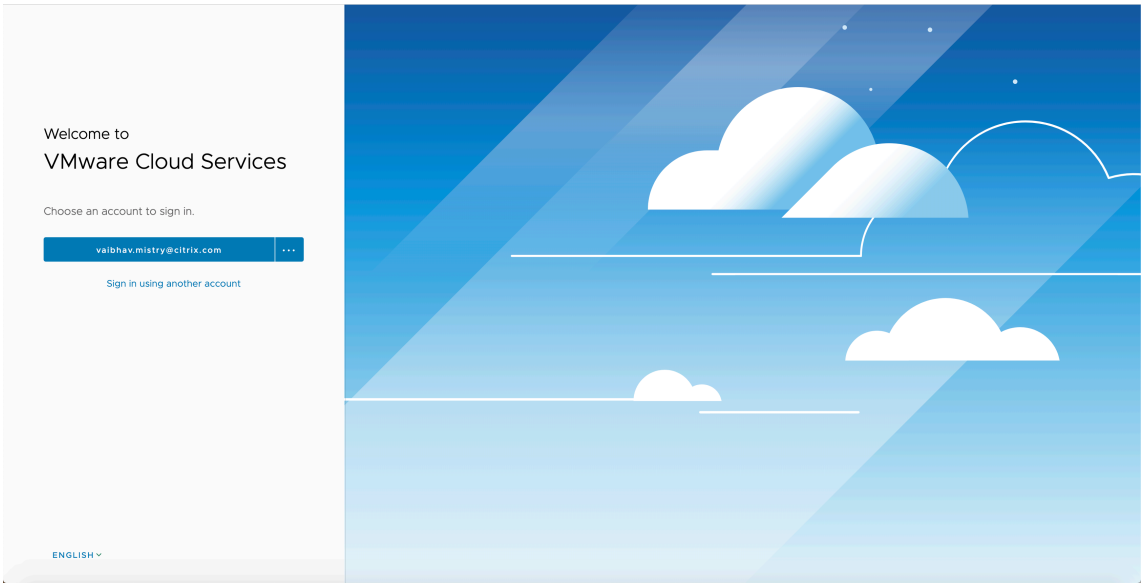
Cloud VMware sur Amazon Web Services (AWS)

Cloud VMware sur Amazon Web Services (AWS) vous permet de migrer des charges de travail Citrix sur site basées sur VMware vers AWS Cloud.

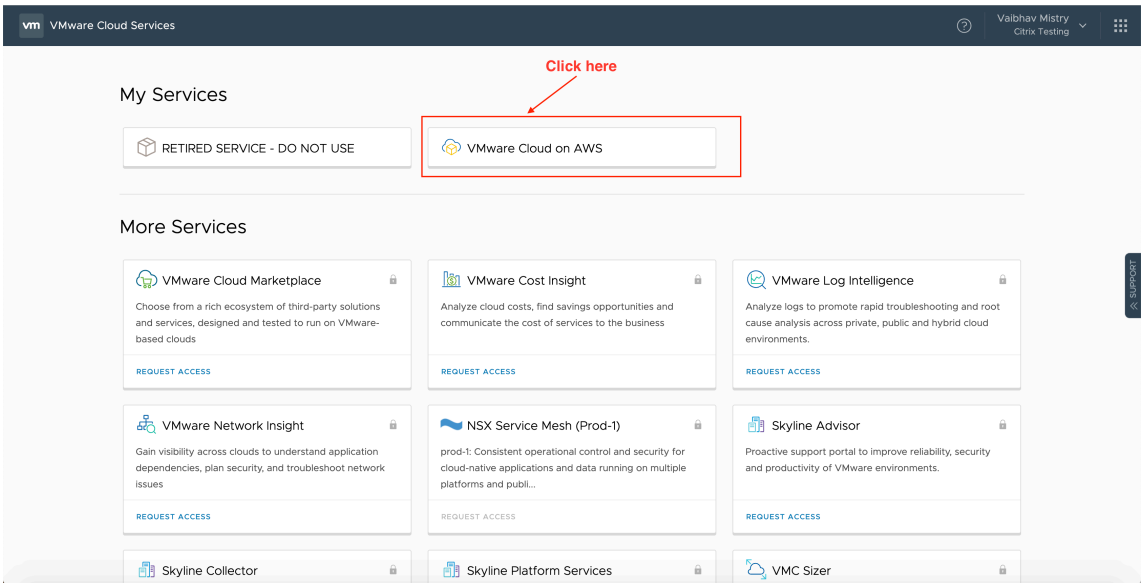
Cet article décrit la procédure à suivre pour configurer un cloud VMware sur AWS.

Accéder à l'environnement cloud VMware

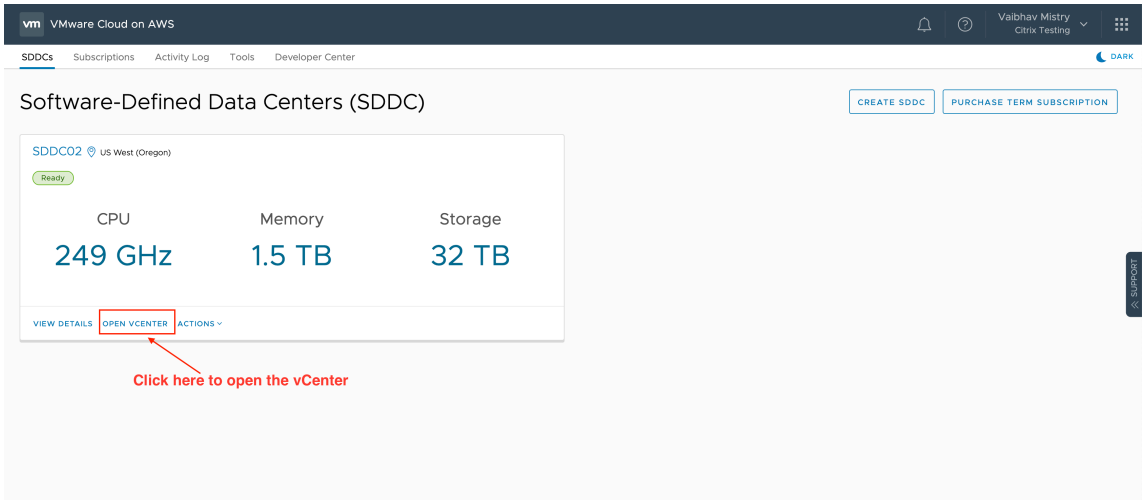
1. Connectez-vous aux services cloud VMware à l'aide de l'URL https://console.cloud.vmware.com/.

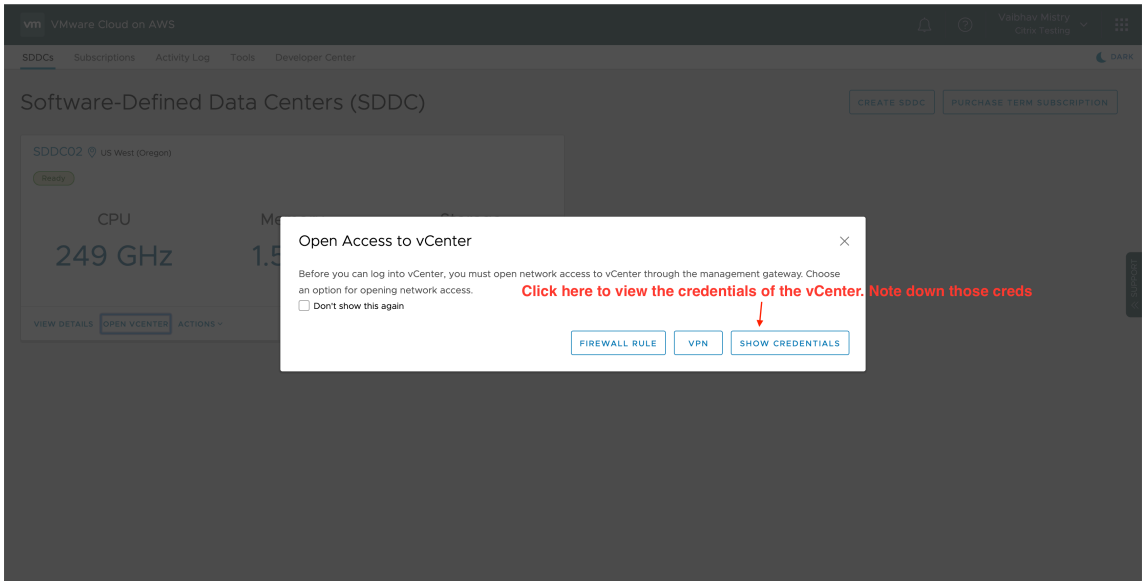


2. Cliquez sur **VMware Cloud on AWS**. La page Software-Defined Data Centers (SDDC) s'affiche.

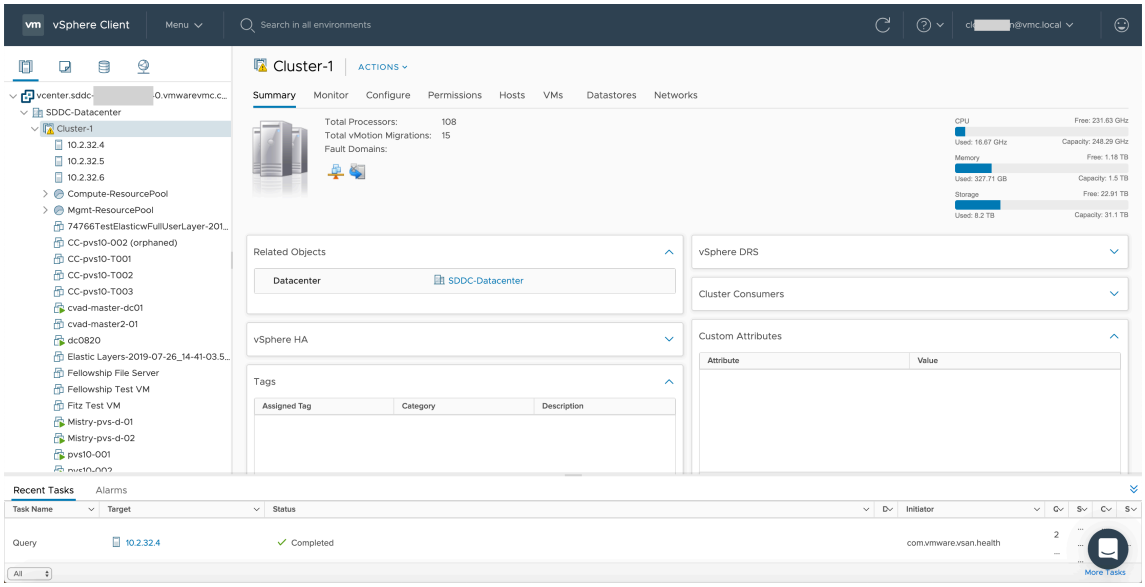


3. Cliquez sur **OPEN VCENTER**, puis sur **SHOW CREDENTIALS**. Notez les informations d'identification pour une utilisation ultérieure.





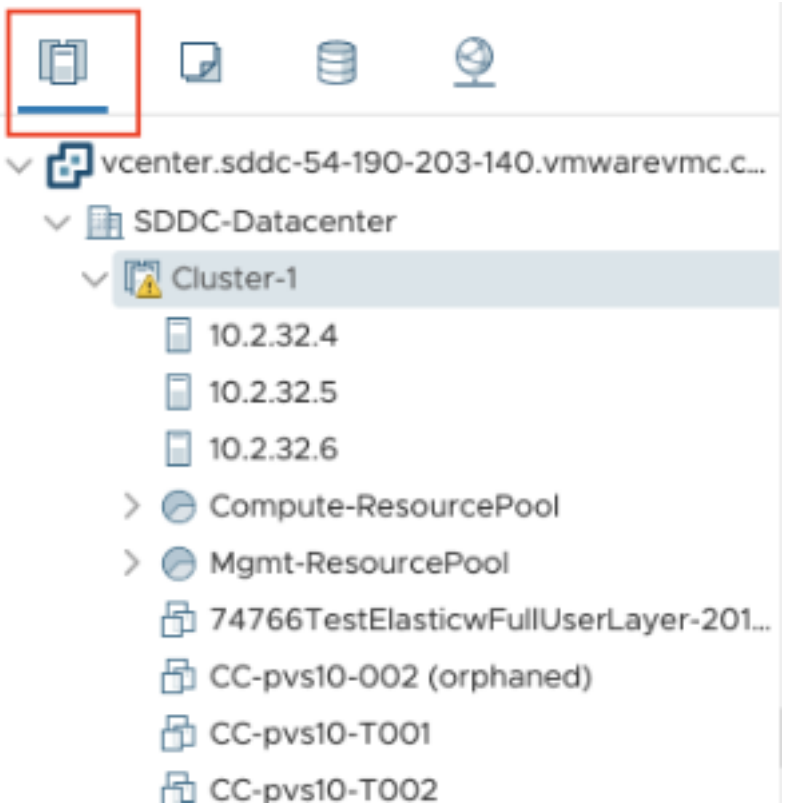
4. Ouvrez un navigateur Web et entrez l'URL de vSphere Web Client.
5. Entrez les informations d'identification que vous avez notées et cliquez sur **Login**. La page Web du client vSphere est similaire à l'environnement local.



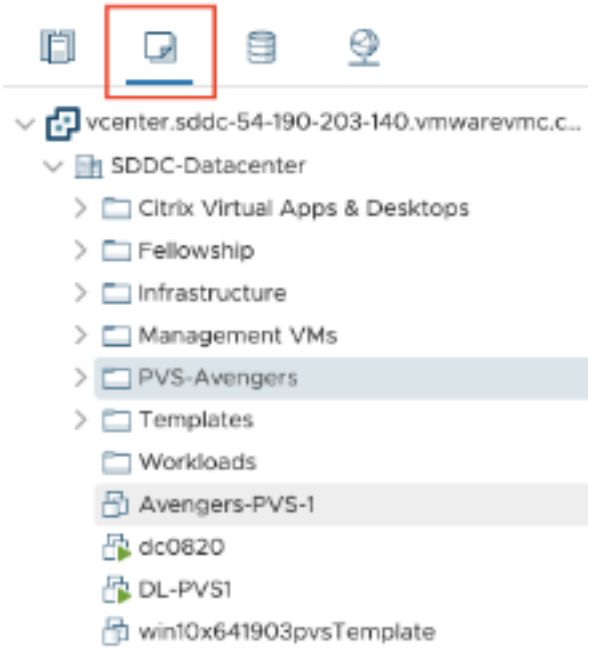
À propos de l'environnement cloud VMware

La page Web du client vSphere propose quatre vues.

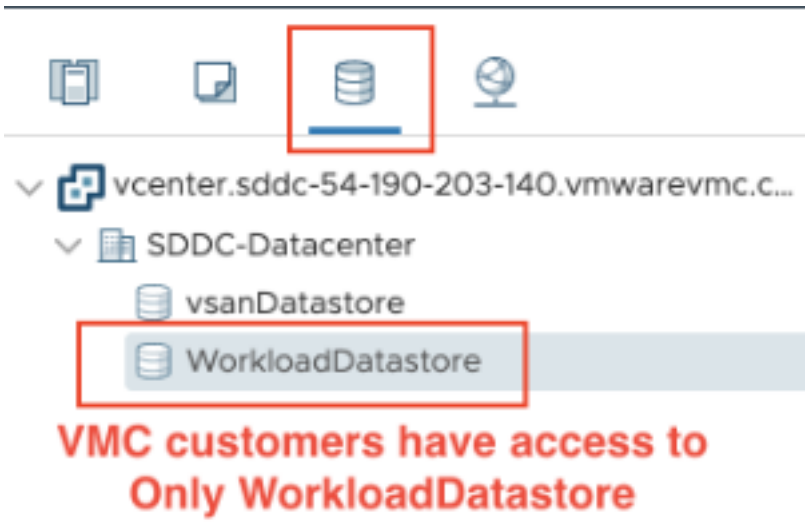
- Vue Hôte et cluster : vous ne pouvez pas créer de nouveau cluster, mais l'administrateur du cloud peut créer plusieurs pools de ressources.



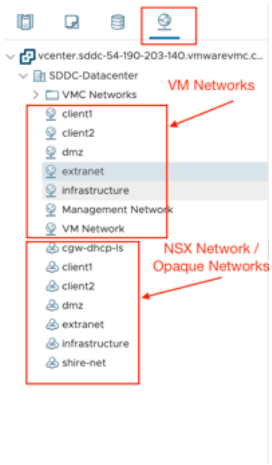
- Vue VM et modèle : l'administrateur du cloud peut créer de nombreux dossiers.



- Vue Stockage : sélectionnez le stockage **WorkloadDatastore** lorsque vous ajoutez une unité d'hébergement dans Citrix Studio, car vous n'avez accès qu'à Workload Datastore.



- Vue Réseau : les icônes sont différentes pour les réseaux cloud VMware et les réseaux opaques.



Après avoir configuré le cluster, reportez-vous à la section Environnements de virtualisation VMware pour l'ajout de connexions et de ressources.

Autres ressources

- Installer les composants principaux
- Installer des VDA
- Créer un site

- Pour créer et gérer une connexion, consultez la section Connexion aux solutions partenaires et cloud VMware.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de machines

Installer les composants principaux

June 27, 2024

> **Important :**
>
> Citrix collecte les données de licence de base nécessaires pour le respect de ses intérêts légitimes, y compris la conformité des licences. Pour plus d'informations, consultez Données du système de licences Citrix.

Les composants principaux incluent Citrix Delivery Controller, Citrix Studio, Web Studio, Citrix Director et le serveur de licences Citrix.

> **Remarque :**
>
> Citrix Studio est une console de gestion Windows qui vous permet de configurer et de gérer votre déploiement Citrix Virtual Apps and Desktops sur site. Web Studio est la nouvelle génération de Citrix Studio, une console de gestion Web offrant la même fonctionnalité que Citrix Studio. Pour plus d'informations sur Web Studio, voir Installer Web Studio.

(Dans les versions antérieures à 2003, les composants principaux incluaient Citrix StoreFront. Vous pouvez toujours installer StoreFront en cliquant sur la vignette **Citrix StoreFront** ou en exécutant la commande disponible sur le support d'installation.)

Avant de commencer l'installation, consultez cet article et Préparer l'installation.

Cet article décrit la séquence de l'assistant d'installation lors de l'installation des composants principaux. Des lignes de commande équivalentes sont fournies. Pour de plus amples informations, consultez la section Installer à l'aide de la ligne de commande.

Étape 1. Télécharger le logiciel du produit et démarrer l'assistant

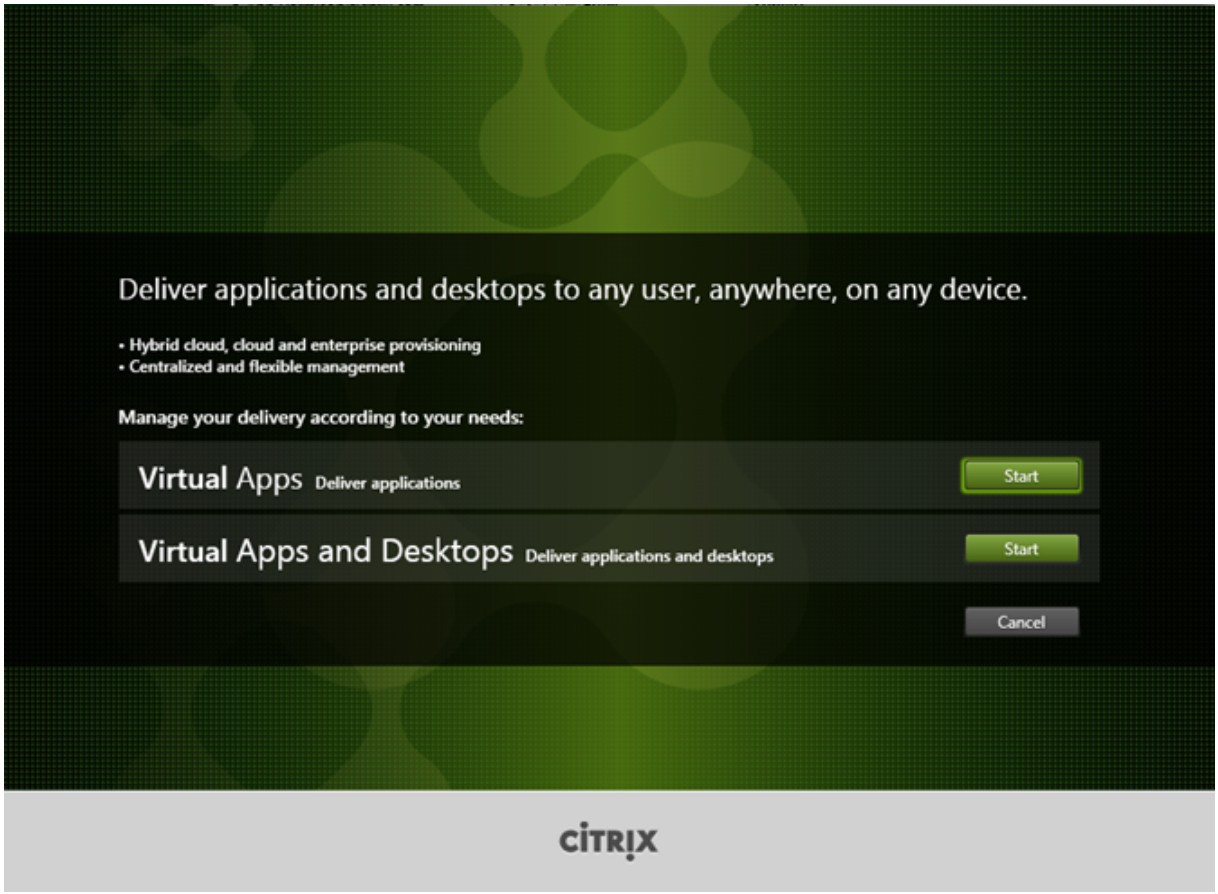
Utilisez vos informations d'identification de compte Citrix pour accéder à la page de téléchargement de Citrix Virtual Apps and Desktops. Téléchargez le fichier ISO du produit.

Décompressez le fichier. Éventuellement, gravez un DVD du fichier ISO.

Ouvrez une session sur la machine sur lequel vous installez les composants principaux, à l'aide d'un compte d'administrateur local.

Insérez le DVD dans le lecteur ou montez le fichier ISO. Si le programme d'installation ne se lance pas automatiquement, double-cliquez sur l'application **AutoSelect** ou sur le lecteur monté.

Étape 2. Choisir le produit à installer

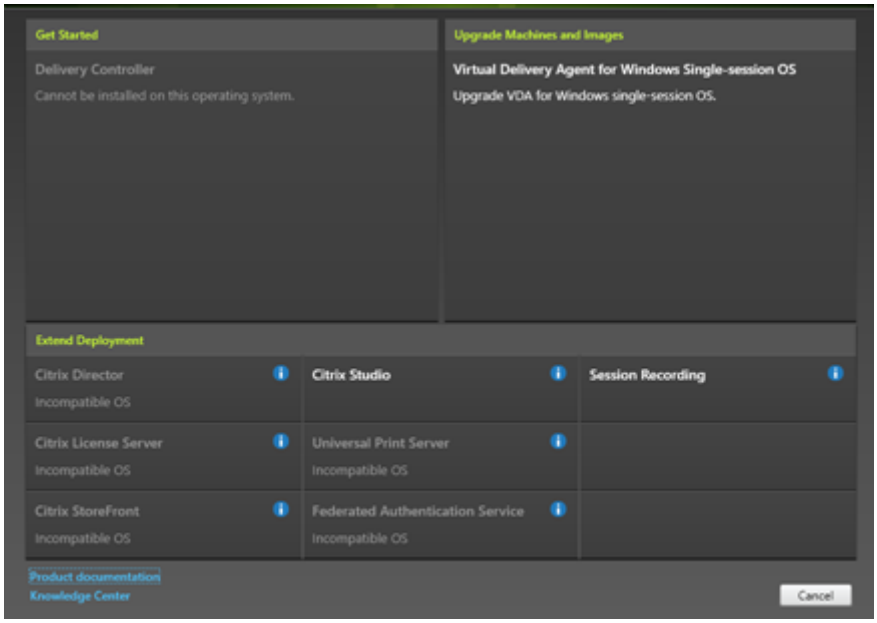


Cliquez sur **Démarrer** à côté du produit à installer : Virtual Apps ou Virtual Apps and Desktops.

(si la machine dispose déjà d'un composant Citrix Virtual Apps and Desktops, cette page ne s'affiche pas).

Option de ligne de commande : `/xenapp` pour installer Citrix Virtual Apps. Citrix Virtual Apps and Desktops est installé si l'option est omise

Étape 3. Choisir les composants à installer

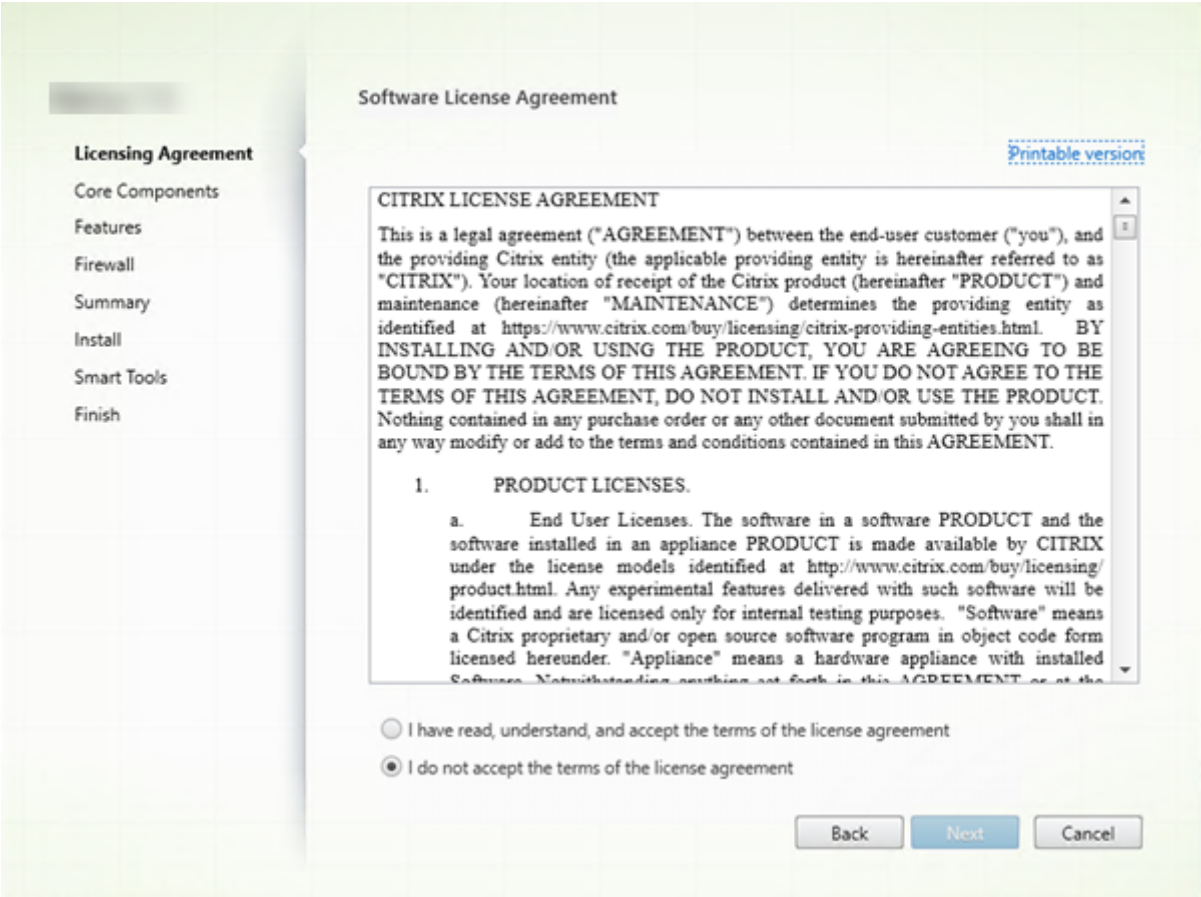


Si vous venez juste de démarrer, sélectionnez **Delivery Controller**. (vous sélectionnerez les composants spécifiques à installer sur cette machine dans une page ultérieure).

Si vous avez déjà installé un Controller (sur cette machine ou une autre) et souhaitez installer un autre composant, sélectionnez-le dans la section **Étendre le déploiement**.

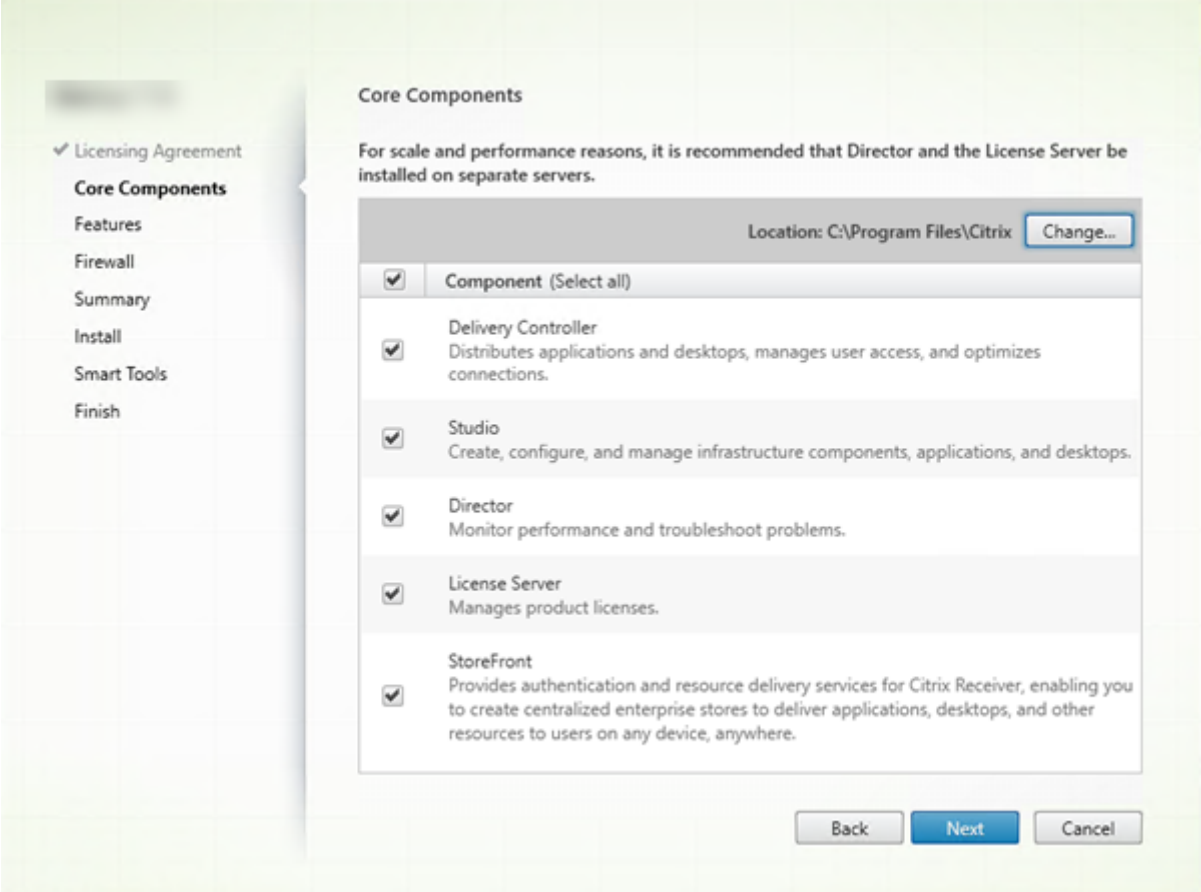
Option de ligne de commande : `/components`

Étape 4. Lire puis accepter le contrat de licence



Sur la page **Contrat de licence**, après avoir lu le contrat de licence, indiquez que vous l'avez lu et accepté. Cliquez ensuite sur **Suivant**.

Étape 5. Sélectionner les composants à installer et l'emplacement d'installation



Sur la page **Composants principaux** :

- **Emplacement :** par défaut, les composants sont installés dans `C:\Program Files\Citrix`. Le paramètre par défaut convient à la plupart des déploiements. Si vous spécifiez un autre emplacement, ce dernier doit disposer d'autorisations d'exécution pour le service réseau.
- **Composants :** par défaut, les cases à cocher pour tous les composants principaux sont sélectionnées. L'installation de tous les composants principaux sur un seul serveur convient aux déploiements d'évaluation, de test ou de production de petite taille. Pour les environnements de production, Citrix vous recommande d'installer Director, StoreFront, Citrix Secure Private Access et le serveur de licences sur des serveurs distincts.

  > **Remarque :**
  >
  > Si vous installez des composants sur plusieurs serveurs, installez le serveur de licences Citrix et les licences d'abord, avant d'installer d'autres composants sur d'autres serveurs. Pour plus d'informations, consultez la section Installation automatique du Guide de ges-

> tion des licences pour Citrix Virtual Apps and Desktops.

Une icône vous avertit lorsque vous choisissez de ne pas installer des composants principaux requis sur cette machine. Cette alerte vous rappelle d'installer ce composant, mais pas nécessairement sur cette machine.

Cliquez sur **Suivant**.

Option de ligne de commande : `/installdir`, `/components`, `/exclude`

Vérification du matériel

Lorsque vous installez ou mettez à niveau un Delivery Controller, le matériel est vérifié. Le programme d'installation vous avertit si la machine dispose d'une quantité de RAM inférieure à la quantité recommandée (5 Go), ce qui peut affecter la stabilité du site. Pour plus d'informations, consultez la section Configuration matérielle requise.

Interface graphique : une boîte de dialogue apparaît.

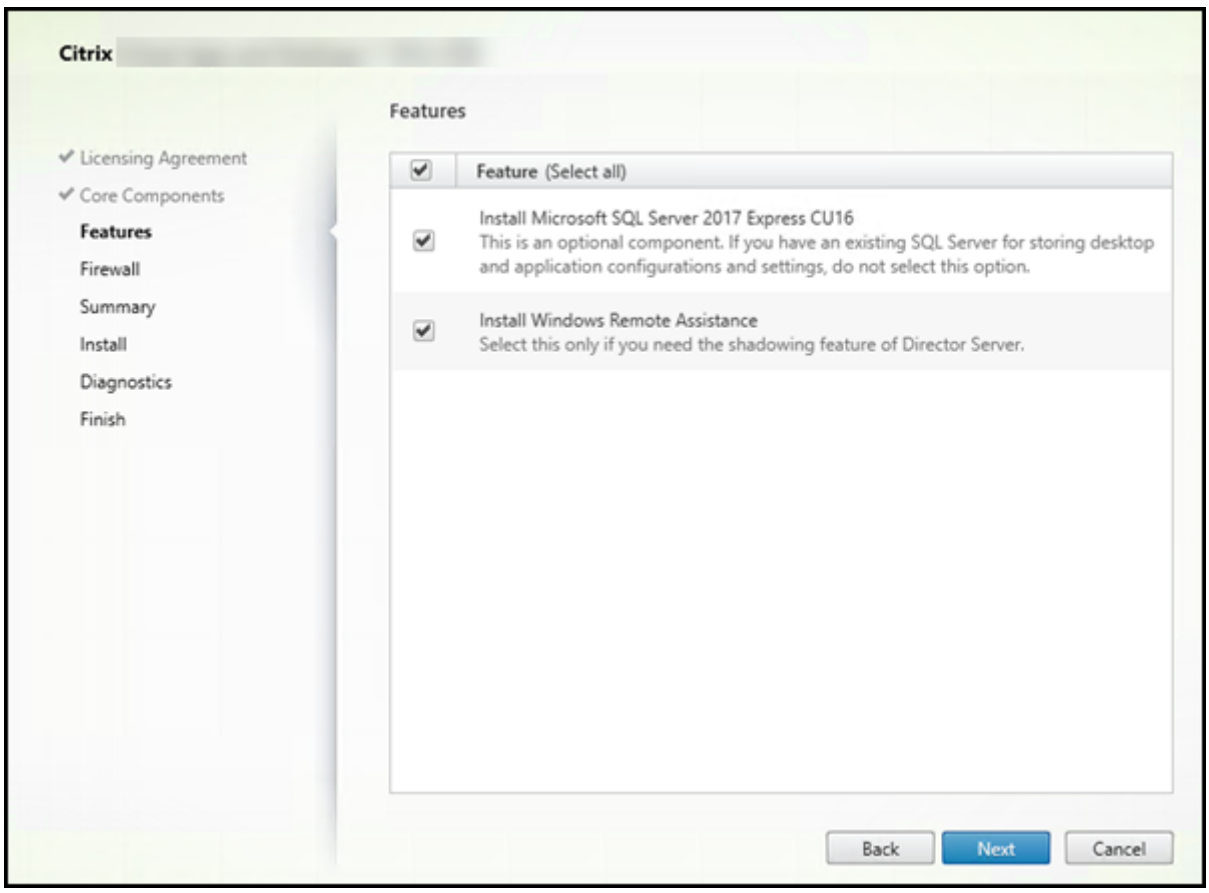
- Recommandé : cliquez sur **Annuler** pour arrêter l'installation. Ajoutez plus de RAM à la machine, puis recommencez l'installation.
- Vous pouvez également cliquer sur **Suivant** pour poursuivre l'installation. Le site peut présenter des problèmes de stabilité.

Interface de ligne de commande : l'installation ou la mise à niveau se termine. Les journaux d'installation contiennent un message décrivant ce qui a été trouvé et les options disponibles.

- Recommandé : ajoutez plus de RAM à la machine, puis exécutez à nouveau la commande.
- Sinon, exécutez à nouveau la commande avec l'option `/ignore_hw_check_failure` pour remplacer l'avertissement. Votre site peut présenter des problèmes de stabilité.

Lors de la mise à niveau, vous êtes également averti si le système d'exploitation ou la version de SQL Server n'est plus pris en charge. Voir Mettre un déploiement à niveau.

Étape 6. Activer ou désactiver des fonctionnalités



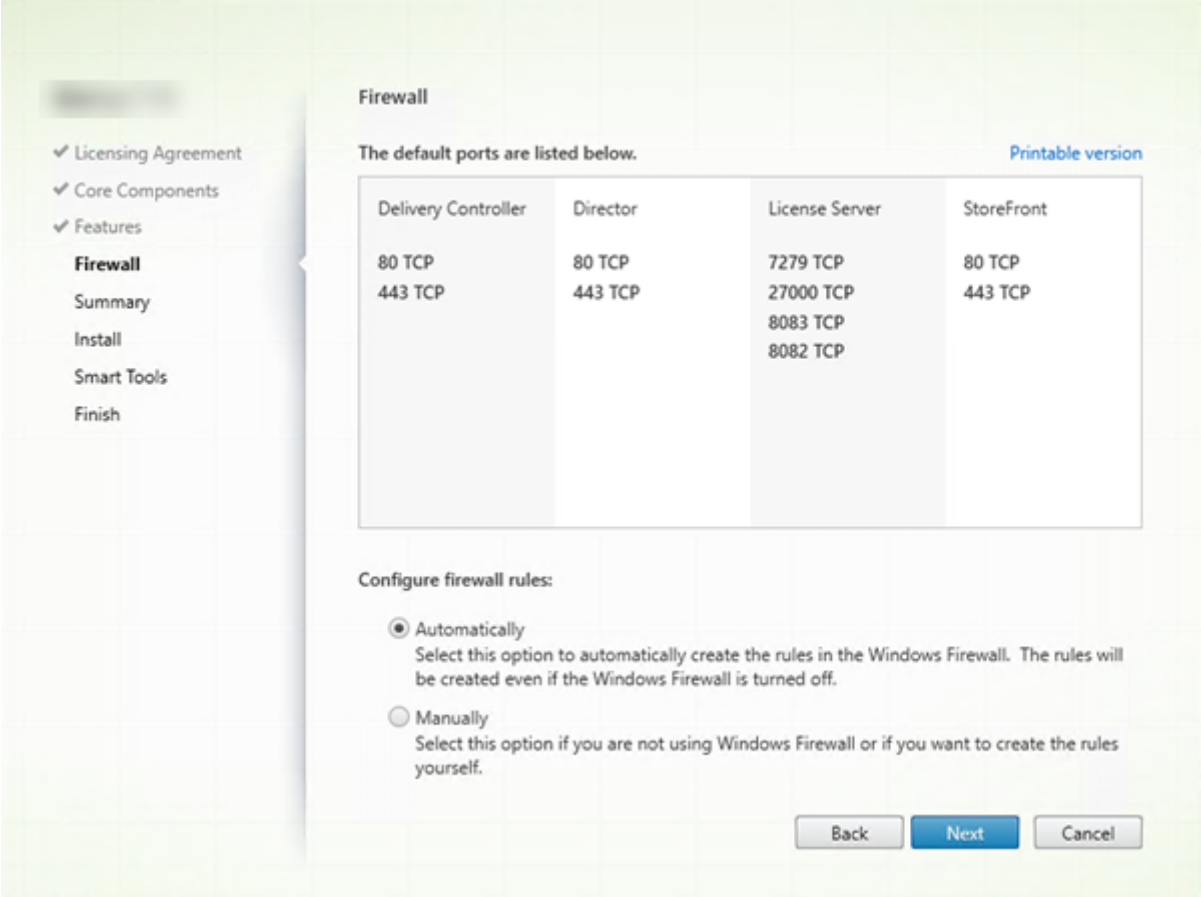
Sur la page **Fonctionnalités** :

- Sélectionnez si vous souhaitez installer Microsoft SQL Server Express pour l'utiliser en tant que base de données du site. Par défaut, cette option est activée. Si vous n'avez pas d'expérience avec les bases de données Citrix Virtual Apps and Desktops, consultez la section Bases de données.
- Lorsque vous installez Director, l'Assistance à distance Windows est installée automatiquement. Vous pouvez choisir d'activer l'observation dans l'Assistance à distance Windows pour l'utiliser avec l'observation utilisateur de Director. L'activation de l'observation ouvre le port TCP 3389. Cette fonctionnalité est activée par défaut. Le paramètre par défaut convient à la plupart des déploiements. Cette fonction s'affiche uniquement lors de l'installation de Director.

Cliquez sur **Suivant**.

Options de ligne de commande : `/nosql` (pour empêcher l'installation), `/no_remote_assistance` (pour empêcher l'activation)

Étape 7. Ouvrir les ports du pare-feu Windows



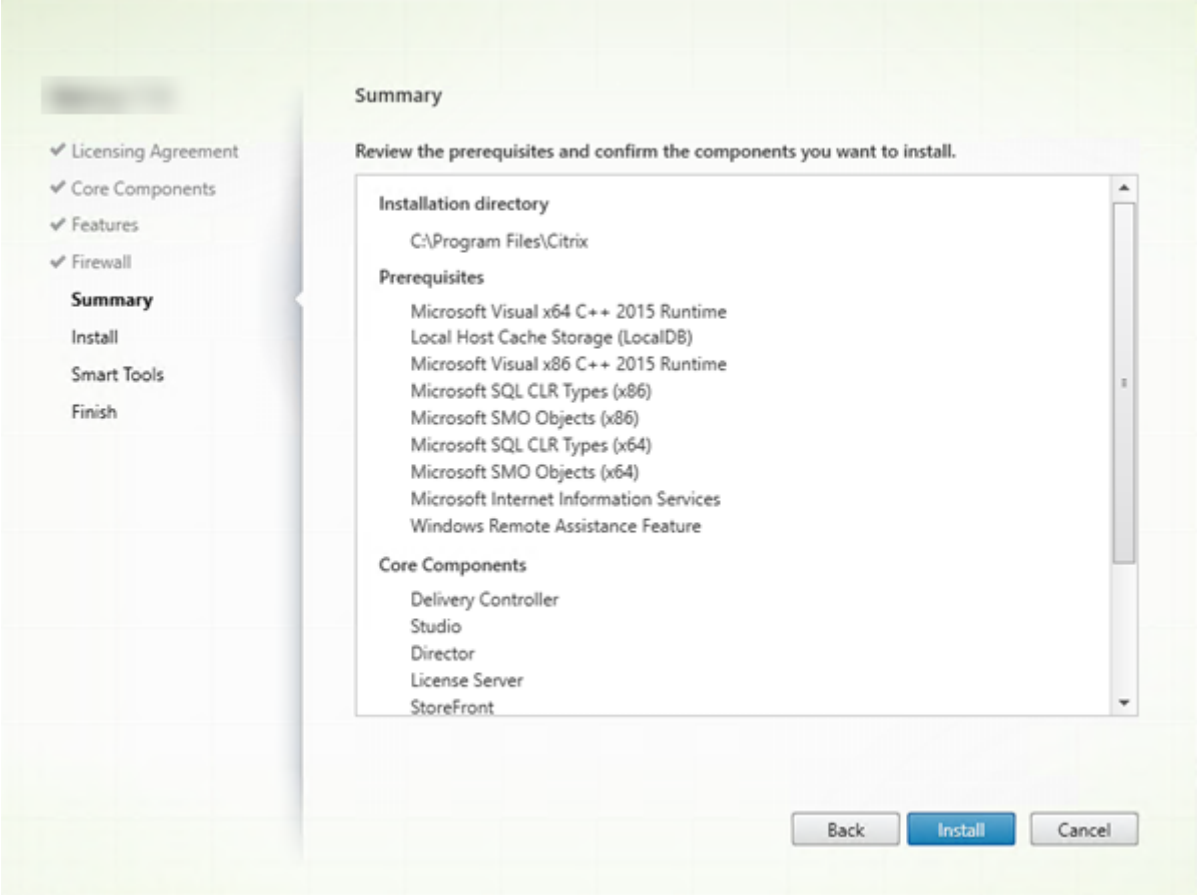
Par défaut, les ports répertoriés sur la page **Pare-feu** sont ouverts automatiquement si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Le paramètre par défaut convient à la plupart des déploiements. Pour obtenir des informations sur le port, consultez la section Ports réseau.

Cliquez sur **Suivant**.

(Le graphique présente la liste des ports si vous avez choisi d'installer tous les composants principaux sur cette machine. Ce type d'installation est généralement effectué uniquement pour les déploiements test.)

Option de ligne de commande : `/configure_firewall`

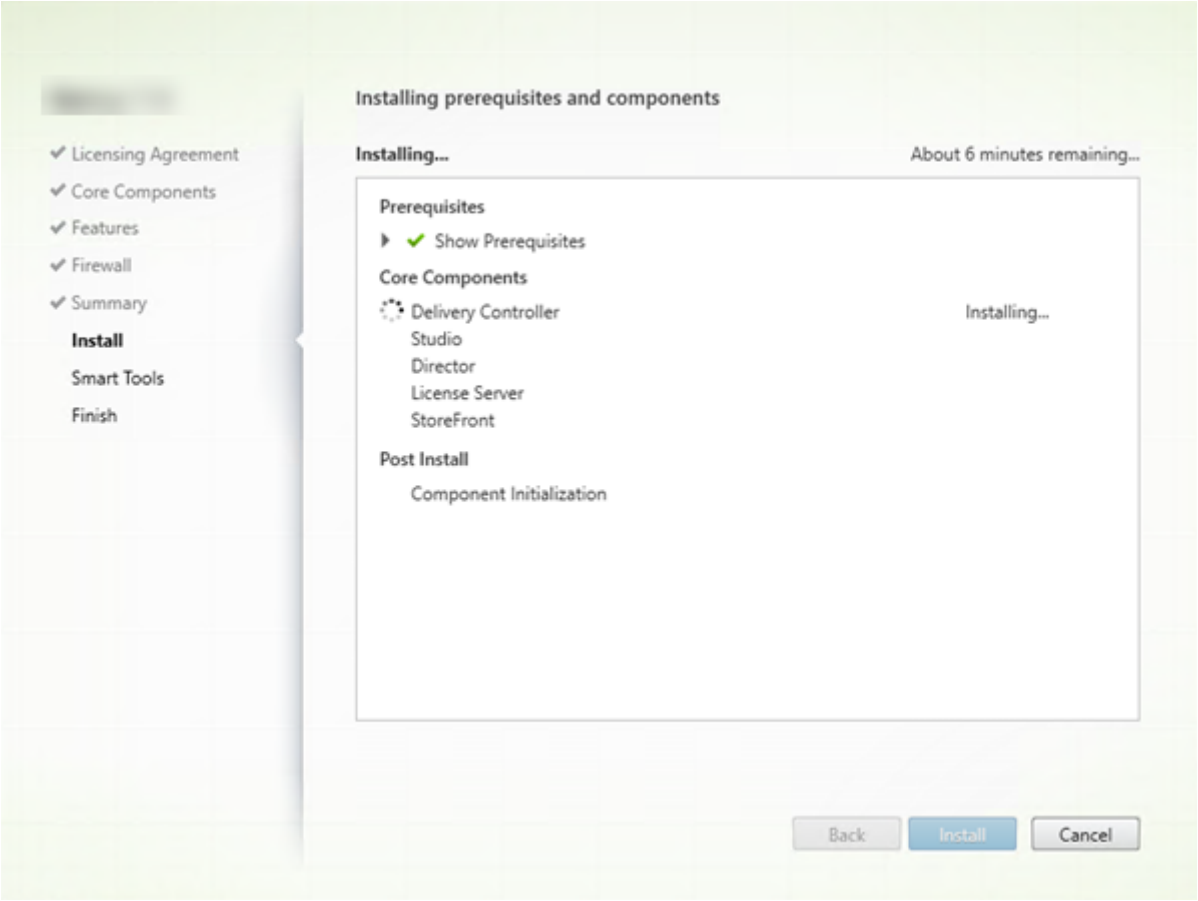
Étape 8. Vérifier les composants requis et confirmer l'installation



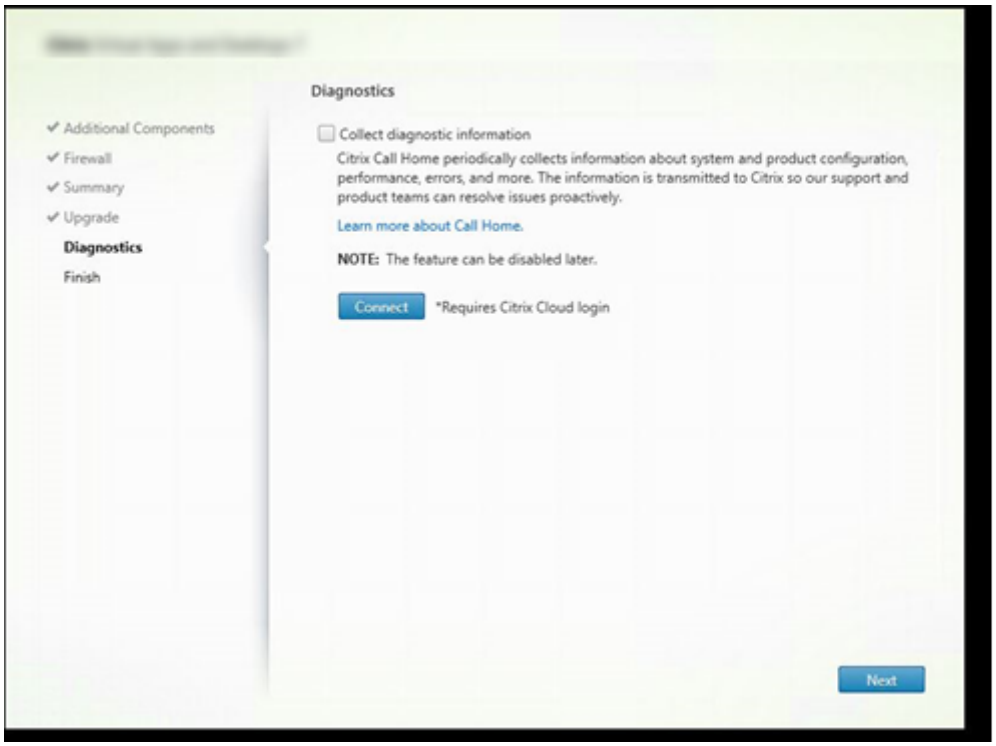
La page **Résumé** répertorie les éléments qui seront installés. Utilisez le bouton **Précédent** pour revenir sur les pages précédentes de l'assistant et modifier les réglages, le cas échéant.

Lorsque vous êtes prêt, cliquez sur **Installer**.

L'écran indique la progression de l'installation :



Étape 9 –Partager les informations de diagnostic avec Cloud Software Group



Sur la page **Diagnostics**, indiquez si vous souhaitez participer au programme Citrix Call Home.

Cette page apparaît lors de l'installation d'un Delivery Controller à l'aide de l'interface graphique. Lorsque vous installez StoreFront (mais pas un Controller), l'assistant affiche cette page. Si vous installez d'autres composants principaux (mais pas un Controller ou StoreFront), l'Assistant n'affiche pas cette page.

Durant une mise à niveau, cette page ne s'affiche pas si Call Home est déjà activé ou si le programme d'installation rencontre une erreur liée au service de télémétrie Citrix (Citrix Telemetry Service).

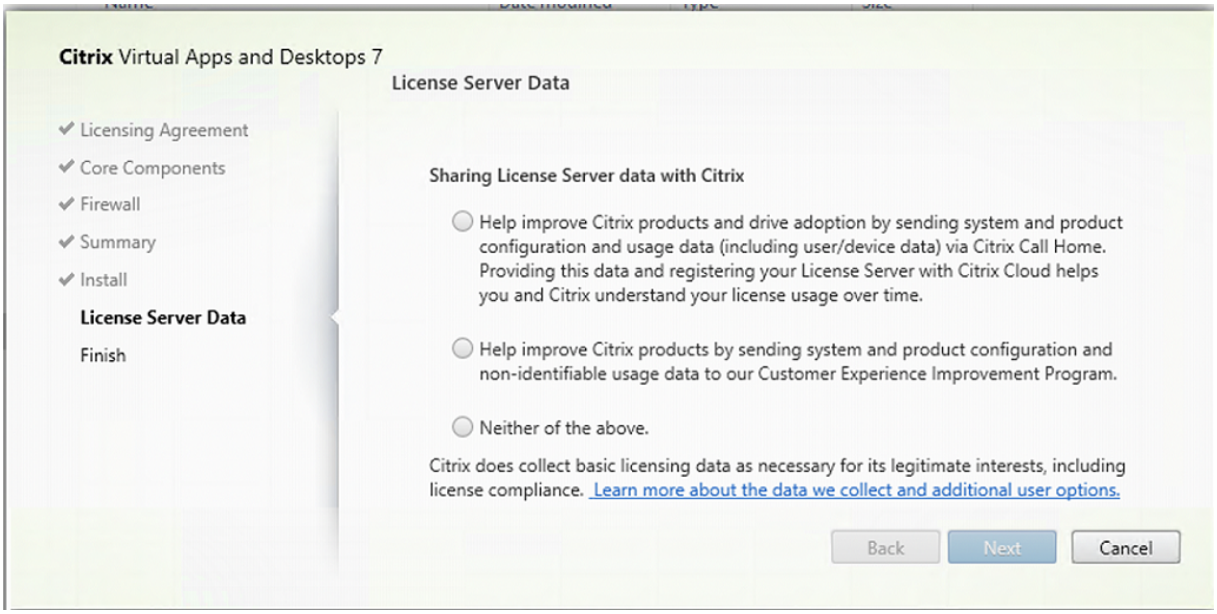
Si vous choisissez de participer (valeur par défaut), cliquez sur **Connecter**. Lorsque vous y êtes invité, saisissez vos informations d'identification de compte Citrix. Vous pouvez modifier votre choix d'inscription ultérieurement, après l'installation.

Une fois que vos informations d'identification sont validées (ou si vous choisissez de ne pas participer au programme), cliquez sur **Suivant**.

Si vous cliquez sur **Se connecter** sur la page **Diagnostics** sans sélectionner d'abord **Collecter des informations de diagnostic**, après avoir fermé la boîte de dialogue **Se connecter à Citrix Insight Services**, le bouton **Suivant** est désactivé. Vous ne pouvez pas passer à la page suivante. Pour réactiver le bouton **Suivant**, sélectionnez et désélectionnez immédiatement **Collecter des informations de diagnostic**.

Pour plus d'informations, consultez Call Home.

Étape 10. Partager les données du serveur de licences avec Cloud Software Group



Sur la page **Données du serveur de licences**, nous vous demandons de partager les données Call Home ou les données du Programme d'amélioration de l'expérience utilisateur (CEIP) pour nous aider. En outre, Cloud Software Group requiert également la collecte de données de base sur les licences, y compris la conformité des licences, dans la mesure nécessaire à ses intérêts légitimes.

La page **Données du serveur de licences** apparaît lorsque vous avez installé le serveur de licences :

- En tant que solution autonome.
- En tant que composant principal, lors de l'installation d'un Delivery Controller.

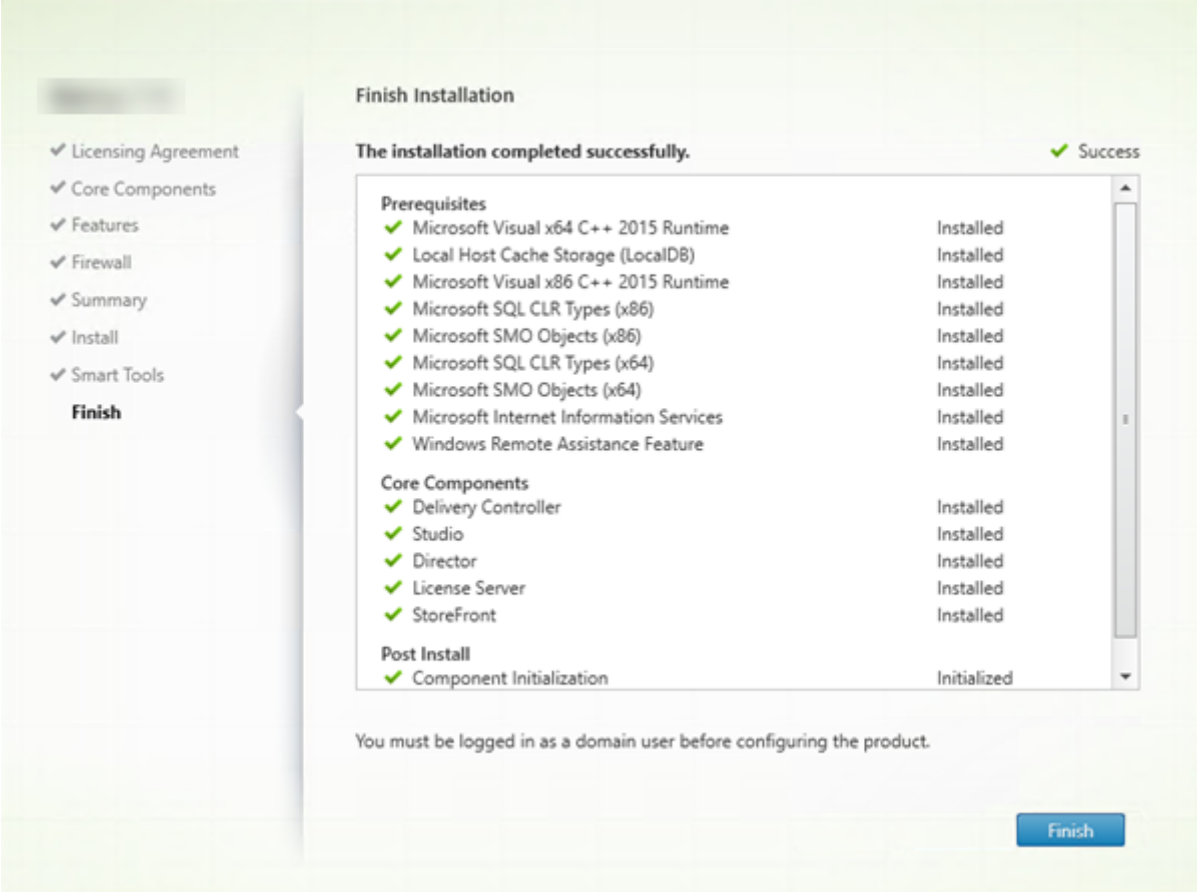
Lors d'une mise à niveau, cette page n'apparaît pas si la configuration est déjà définie dans le fichier `/CITRIX.opt:.`

Le serveur de licences surveille plusieurs types de données utilisateur, telles que les données de licence, les données Call Home et les données CEIP. Pour activer la collecte des données Call Home et CEIP, vous devez choisir de participer.

Pour plus d'informations sur la manière d'activer la collecte de données Call Home et CEIP lors de l'installation à l'aide de la ligne de commande, voir Options de ligne de commande pour l'installation des composants principaux.

Pour plus d'informations sur la collecte des données de licences Cloud Software Group, consultez la section Programmes de collecte de données de licences Citrix.

Étape 11. Fin de l'installation



La page **Terminer** contient des coches vertes pour tous les éléments pré-requis et composants installés et initialisés avec succès.

Cliquez sur **Terminer**.

Étape 12. Installer les autres composants principaux sur d'autres machines

Si vous avez installé tous les composants principaux sur une machine, passez aux étapes suivantes. Sinon, exécutez le programme d'installation sur d'autres machines pour installer d'autres composants. Vous pouvez également installer des Controller supplémentaires sur d'autres serveurs.

Étapes suivantes

Une fois que vous avez installé tous les composants requis, utilisez Studio pour créer un site.

Après avoir créé le site, installez les VDA.

À tout moment, vous pouvez utiliser le programme d'installation du produit entier pour étendre votre déploiement avec les composants suivants :

- **Composant serveur d'impression universelle** : exécutez le programme d'installation sur votre serveur d'impression.

  1. Sélectionnez **Serveur d'impression universelle** dans la section **Étendre le déploiement**.
  2. Acceptez le contrat de licence.
  3. Sur la page **Pare-feu**, par défaut, les ports TCP 7229 et 8080 sont ouverts dans le pare-feu si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Vous pouvez désactiver cette action par défaut si vous souhaitez ouvrir les ports manuellement.

  Pour installer ce composant à partir de la ligne de commande, consultez Options de ligne de commande pour l'installation d'un serveur d'impression universelle.

- Service d'authentification fédérée.
- Enregistrement de session.
- Workspace Environment Management.

Installer à l'aide de la ligne de commande

June 27, 2024

> **Important :**
>
> - Si vous effectuez une mise à niveau et que votre version actuelle utilise ou est dotée du logiciel Personal vDisk ou AppDisks, reportez-vous à la section Suppression de PvD, AppDisks et d'hôtes non pris en charge.
> - Citrix collecte les données de licence de base nécessaires pour le respect de ses intérêts légitimes, y compris la conformité des licences. Pour plus d'informations, consultez Données du système de licences Citrix.

Introduction

Cet article s'applique à l'installation de composants sur des machines avec systèmes d'exploitation Windows. Pour de plus amples informations sur les VDA pour systèmes d'exploitation Linux, consultez Linux Virtual Delivery Agents.

Cet article explique comment émettre des commandes d'installation du produit. Avant de procéder à une installation, consultez la section Préparer l'installation. Cet article contient des descriptions des programmes d'installation disponibles.

Pour pouvoir suivre la progression de l'exécution de la commande en cours et des valeurs de retour, vous devez être l'administrateur d'origine ou utiliser l'option **Exécuter en tant qu'administrateur**. Pour plus d'informations, veuillez consulter la documentation des commandes Microsoft.

En complément des commandes d'installation directes, des exemples de scripts sont fournis sur le fichier ISO du produit que vous pouvez utiliser pour installer, mettre à niveau ou supprimer des VDA dans Active Directory. Pour de plus amples informations, consultez Installer les VDA à l'aide de scripts.

Si vous tentez d'installer ou de mettre à niveau sur une version de Windows non prise en charge par cette version de Citrix Virtual Apps and Desktops, un message vous renvoie vers des informations décrivant vos options. Voir Systèmes d'exploitation antérieurs.

Pour en savoir plus sur la façon dont Citrix présente le résultat de l'installation des composants, consultez Codes de retour de l'installation Citrix.

Utiliser le programme d'installation du produit entier

Pour accéder à l'interface de la ligne de commande du programme d'installation du produit complet :

1. Téléchargez le pack du produit auprès de Citrix. Des informations d'identification de compte Citrix sont requises pour accéder au site de téléchargement.
2. Décompressez le fichier. Éventuellement, gravez un DVD du fichier ISO.
3. Ouvrez une session sur le serveur sur lequel vous installez les composants, à l'aide d'un compte d'administrateur local.
4. Insérez le DVD dans le lecteur ou montez le fichier ISO.
5. À partir du répertoire `\x64\XenDesktop Setup` du support d'installation, exécutez la commande appropriée.

   Pour installer les composants principaux : exécutez `XenDesktopServerSetup.exe` avec les options répertoriées dans la section Options de ligne de commande pour l'installation des composants principaux.

   Pour installer un VDA : exécutez `XenDesktopVDASetup.exe` avec les options répertoriées dans Options de ligne de commande pour l'installation d'un VDA.

   Pour installer StoreFront : exécutez `CitrixStoreFront-x64.exe` dans le dossier `x64 > StoreFront` sur le support d'installation.

Pour installer le serveur d'impression universelle : suivez les instructions de la section Options de ligne de commande pour l'installation d'un serveur d'impression universelle.

Pour installer le service d'authentification fédérée : Citrix vous recommande d'utiliser l'interface graphique.

Pour installer l'enregistrement de session : suivez les instructions de la section Enregistrement de session.

Pour installer Workspace Environment Management : suivez les instructions de la section Workspace Environment Management.

Pour installer Secure Private Access : exécutez `XenDesktopSPASetup.exe` dans le dossier de configuration `x64` > `XenDesktop` du support d'installation. Suivez les instructions des Options de ligne de commande pour installer Secure Private Access.

Options de ligne de commande pour l'installation des composants principaux

Les options de paramètres suivantes sont valides lors de l'installation des composants principaux à l'aide de la commande `XenDesktopServerSetup.exe`. Pour de plus amples informations sur les options disponibles, consultez la section Installer les composants principaux.

- **/ceipoptin** *ceipoptin* [,*ceipoptin*] …

  Permet de collecter les données Call Home et les données du programme d'amélioration de l'expérience utilisateur (CEIP). Les valeurs autorisées sont :

  - `DIAGNOSTIC` : choisissez cette valeur pour permettre à Citrix Licensing de collecter les données Call Home.
  - `ANONYMOUS` : choisissez cette valeur pour permettre à Citrix Licensing de collecter les données CEIP non identifiées (qui n'identifient pas les utilisateurs).
  - `NONE` : choisissez cette valeur pour désactiver la collecte de données CEIP par Citrix Licensing.

  Pour plus d'informations sur la collecte des données Call Home, consultez Programme Call Home du système de licences Citrix.

  Pour plus de détails sur la collecte des données CEIP, consultez Programme d'amélioration de l'expérience utilisateur du système de licences Citrix.

  Pour plus de détails sur les données CEIP, consultez la section Éléments de données CEIP du système de licences Citrix.

  Pour plus de détails sur les données de licence du serveur de licences, consultez la section Données de licences Citrix.

- **/components** *composant* [,*composant*]…

  Liste séparée par des virgules des composants à installer ou supprimer. Les valeurs autorisées sont :

  - `CONTROLLER`: Controller
  - `DESKTOPSTUDIO`: Studio
  - `WEBSTUDIO`: Web Studio
  - `DESKTOPDIRECTOR`: Director
  - `LICENSESERVER`: Serveur de licences Citrix
  - `SECUREPRIVATEACCESS`: Secure Private Access

  Si cette option est omise, tous les composants sont installés (ou supprimés, si l'option `/remove` est également spécifiée).

  (Dans les versions antérieures à 2003, les valeurs valides incluaient `STOREFRONT`. Pour les versions 2003 et ultérieures, utilisez la commande d'installation dédiée de StoreFront indiquée à la section Utiliser le programme d'installation du produit entier.

- **/configure_firewall**

  Ouvre tous les ports du pare-feu Windows utilisés par les composants installés, si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Si vous utilisez un pare-feu tiers ou aucun pare-feu, vous devez ouvrir les ports manuellement.

- **/disableexperiencemetrics**

  Empêche l'envoi automatique des analyses collectées au cours de l'installation, de la mise à niveau ou de la suppression à Citrix.

- **/exclude** "*feature*"[,"*feature*"]

  Empêche l'installation de fonctions, services ou technologies séparés par des virgules, entourés de guillemets droits. Les valeurs autorisées sont :

  - `"Local Host Cache Storage (LocalDB)"`: empêche l'installation de la base de données utilisée pour le cache d'hôte local. Cette option n'a aucun effet sur l'installation de SQL Server Express pour une utilisation en tant que base de données du site.

- **/help** ou **/h**

  Affiche la commande d'aide.

- **/ignore_hw_check_failure**

  Permet à l'installation ou à la mise à niveau de Delivery Controller de continuer, même si les vérifications matérielles échouent (par exemple, en raison d'une mémoire RAM insuffisante). Pour plus d'informations, consultez la section Vérification du matériel.

- **/ignore_site_test_failure**

  Valable uniquement pendant la mise à niveau du Controller. En général, les échecs de test de site sont ignorés et la mise à niveau continue. Si cette commande est omise (ou définie sur false), tout échec de test de site entraîne l'échec du programme d'installation, sans effectuer la mise à niveau. Valeur par défaut = false

  Lors d'une mise à niveau, cette option est ignorée si une version de SQL Server non prise en charge est détectée. Pour plus d'informations, consultez la section Vérification de la version de SQL Server.

- **/installdir *directory***

  Répertoire vide existant où les composants seront installés. Valeur par défaut : c:\Program Files\Citrix.

- **/logpath *path***

  Emplacement du fichier journal. Le dossier spécifié doit exister. Le programme d'installation ne le crée pas. Valeur par défaut = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  Valide uniquement lors de l'installation de Director. Désactive la fonctionnalité d'observation utilisateur qui utilise l'Assistance à distance Windows.

- **/noreboot**

  Empêche un redémarrage après l'installation. (Pour la plupart des composants principaux, aucun redémarrage n'est activé par défaut).

- **/noresume**

  Par défaut, lorsqu'un redémarrage de la machine est nécessaire pendant une installation, le programme d'installation reprend automatiquement une fois le redémarrage terminé. Pour remplacer la valeur par défaut, spécifiez `/noresume`. Cela peut être utile si vous devez réinstaller le support ou si vous souhaitez capturer des informations lors d'une installation automatisée.

- **/nosql**

  Empêche l'installation de Microsoft SQL Server Express sur le serveur sur lequel vous installez Controller. Si cette option est omise, SQL Server Express est installé pour être utilisé en tant que base de données du site.

  Cette option n'a aucun effet sur l'installation de SQL Server Express LocalDB utilisé pour le cache d'hôte local.

- **/quiet** ou **/passive**

Aucune interface utilisateur ne s'affiche lors de l'installation. La seule preuve de l'installation est dans le Gestionnaire des tâches Windows. Si cette option n'est pas utilisée, l'interface graphique démarre.

- **/remove**

  Supprime les composants principaux spécifiés avec l'option /components.

- **/removeall**

  Supprime tous les principaux composants installés.

- **/sendexperiencemetrics**

  Envoie automatiquement les analyses collectées au cours de l'installation, de la mise à niveau ou de la suppression à Citrix. Si cette option est omise (ou que /disableexperiencemetrics est spécifié), les analyses sont collectées localement, mais pas envoyées automatiquement.

- **/tempdir** *directory*

  Répertoire qui contient les fichiers temporaires durant l'installation. Valeur par défaut = c:\Windows\Temp.

- **/xenapp**

  Installe Citrix Virtual Apps. Si cette option est omise, Citrix Virtual Apps and Desktops est installé.

Exemples d'installation des composants principaux

La commande suivante installe un Delivery Controller, Studio, le système de licences Citrix et SQL Server Express sur un serveur. Les ports de pare-feu requis pour les communications de composants sont ouverts automatiquement.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller
,desktopstudio,licenseserver /configure_firewall
```

La commande suivante installe un contrôleur Citrix Virtual Apps, Studio, et SQL Server Express sur le serveur. Les ports de pare-feu requis pour les communications de composants seront ouverts automatiquement.

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components
controller,desktopstudio /configure_firewall
```

La commande suivante installe un Delivery Controller, un Secure Private Access et SQL Server Express sur un serveur. Les ports de pare-feu requis pour les communications de composants seront ouverts automatiquement.

```
\x64\XenDesktop Setup XenDesktopServerSetup.exe /xenapp /components
controller,secureprivateaccess /configure_firewall
```


Utiliser le programme d'installation de VDA autonome

Des informations d'identification de compte Citrix sont requises pour accéder au site de téléchargement. vous devez soit disposer de privilèges d'administrateur avant de démarrer l'installation, soit utiliser l'option **Exécuter en tant qu'administrateur**.

1. Téléchargez le pack approprié auprès de Citrix :

   - VDA pour OS multi-session : `VDAServerSetup_xxxx.exe`
   - VDA pour OS mono-session : `VDAWorkstationSetup_xxxx.exe`
   - VDA pour services de base OS mono-session : `VDAWorkstationCoreSetup_xxxx.exe`

2. Vous pouvez extraire les fichiers du pack dans un répertoire existant, puis exécuter la commande d'installation, ou uniquement exécuter le pack.

   Pour extraire les fichiers avant de les installer, utilisez `/extract` avec le chemin d'accès absolu, par exemple : `C:\YourExtractFolder\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`. Le répertoire doit exister. Sinon, l'extraction échoue. Ensuite, dans une commande séparée, exécutez la commande appropriée, en utilisant les options valides répertoriées dans cet article.

   - Pour `VDAServerSetup_XXXX.exe`, exécutez `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
   - Pour `VDAWorkstationCoreSetup_XXXX.exe`, exécutez `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
   - Pour `VDAWorkstationSetup_XXXX.exe`, exécutez `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

   Pour exécuter le package téléchargé, exécutez son nom : `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` ou `VDAWorkstationCoreSetup.exe`. Utilisez les options valides répertoriées dans cet article.

Si vous connaissez le programme d'installation de la version complète du produit :

- Exécutez le programme d'installation autonome `VDAServerSetup.exe` ou `VDAWorkstationSetup.exe` comme s'il s'agissait de la commande `XenDesktopVdaSetup.exe` sauf pour le nom.
- Le programme d'installation `VDAWorkstationCoreSetup.exe` est différent, car il prend en charge un sous-ensemble des options disponibles avec les autres programmes d'installation.

Options de ligne de commande pour l'installation d'un VDA

Les options suivantes sont valides avec une ou plusieurs des commandes suivantes (programmes d'installation) : `VDAServerSetup_xxxx.exe`, `VDAWorkstationSetup_xxxx.exe` et `VDAWorkstationCoreSetup_xxxx.exe`.

Pour en savoir plus sur les options disponibles, consultez Installer des VDA.

- **/components** *component*[,*component*]

  Liste séparée par des virgules des composants à installer ou supprimer. Les valeurs autorisées sont :

  - `VDA`: Virtual Delivery Agent
  - `PLUGINS`: Application Citrix Workspace pour Windows

  Pour installer le VDA et l'application Citrix Workspace pour Windows, spécifiez `/components vda,plugins`.

  Si cette option est omise, seul le VDA est installé (pas l'application Citrix Workspace).

  Cette option n'est pas valide lors de l'utilisation du programme d'installation `VDAWorkstationCoreSetu .exe`. Ce programme d'installation ne peut pas installer l'application Citrix Workspace.

- **/controllers** "*controller* [*controller*]"

  Noms de domaines complets (FQDN) des Controller avec lesquels le VDA peut communiquer, séparés par des espaces et entourés de guillemets droits. Ne spécifiez pas à la fois les options `/site_guid` et `/controllers`.

- **/disableexperiencemetrics**

  Envoie automatiquement les analyses collectées au cours de l'installation, de la mise à niveau ou de la suppression à Citrix.

- **/enable_hdx_ports**

  Ouvre les ports du pare-feu Windows requis par le VDA et les fonctionnalités activées (sauf l'assistance à distance Windows), si le service Pare-feu Windows est détecté, même si le pare-feu n'est pas activé. Si vous utilisez un autre pare-feu ou aucun pare-feu, vous devez configurer le pare-feu manuellement. Pour obtenir des informations sur le port, consultez la section Ports réseau.

  Pour ouvrir les ports UDP utilisés par le transport adaptatif HDX, spécifiez l'option `/enable_hdx_udp_ports`, en plus de l'option `/enable_hdx_ports`.

- **/enable_hdx_udp_ports**

  Ouvre les ports UDP, dans le pare-feu Windows, que le transport adaptatif HDX utilise, si le Service pare-feu Windows est détecté, même si le pare-feu n'est pas activé. Si vous utilisez un autre

pare-feu ou aucun pare-feu, vous devez configurer le pare-feu manuellement. Pour obtenir des informations sur le port, consultez la section Ports réseau.

Pour ouvrir les ports supplémentaires utilisés par le VDA, spécifiez l'option /`enable_hdx_ports` , en plus de l'option /`enable_hdx_udp_ports`.

- **/enable_hdx_tls_dtls**

  Ouvre les ports TCP et UDP 443 pour HDX Direct V1.

- **/enable_real_time_transport**

  Active ou désactive l'utilisation d'UDP pour les paquets audio (RealTime Audio Transport pour l'audio). L'activation de cette fonctionnalité peut améliorer les performances audio. Incluez l'option /`enable_hdx_ports` si vous souhaitez que les ports UDP soient ouverts automatiquement si le service Pare-feu Windows est détecté.

- **/enable_remote_assistance**

  Active la fonctionnalité d'observation dans l'Assistance à distance Windows pour l'utiliser avec Director. Si vous spécifiez cette option, l'Assistance à distance Windows ouvre les ports dynamiques dans le pare-feu.

- **/enablerestore** ou **/enablerestorecleanup**

  (Valide uniquement pour les VDA mono-session) Active le retour automatique au point de restauration, en cas d'échec de l'installation ou de la mise à niveau du VDA.

  Si l'installation ou la mise à niveau se termine avec succès :

  - /`enablerestorecleanup` indique au programme d'installation de supprimer le point de restauration.
  - /`enablerestore` indique au programme d'installation de conserver le point de restauration, même s'il n'a pas été utilisé.

  Pour plus d'informations, consultez la section Restauration en cas d'échec de l'installation ou de la mise à niveau.

- **/enable_ss_ports**

  Ouvre les ports, dans le pare-feu Windows, qui sont requis pour le partage d'écran, si le Service pare-feu Windows est détecté, même si le pare-feu n'est pas activé. Si vous utilisez un autre pare-feu ou aucun pare-feu, vous devez configurer le pare-feu manuellement.

- **/exclude** "*component*"[,"*component*"]

  Empêche l'installation d'un ou de plusieurs composants facultatifs séparés par des virgules et entourés de guillemets droits. Par exemple, l'installation ou la mise à niveau d'un VDA sur une image qui n'est pas gérée par MCS ne nécessite pas le composant Machine Identity Service. Les valeurs valides sont les suivantes :

OS multi-session	OS mono-session	Services de base d'OS mono-session
Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in
Citrix Backup and Restore	Citrix Backup and Restore	Citrix Browser Content Redirection
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Personalization **for** App-V - VDA
Citrix MCS IODriver	Citrix MCS IODriver	Citrix Telemetry Service
Citrix Personalization **for** App-V - VDA	Citrix Personalization **for** App-V - VDA	Citrix Universal Print Client
Citrix Profile Management	Citrix Profile Management	Citrix Vda Log Capture Service
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	CSE Component
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	VDA WMI Proxy Plug-in
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	
Director VDA Plug-in	Director VDA Plug-in	
Machine Identity Service	Machine Identity Service	

OS multi-session	OS mono-session	Services de base d'OS mono-session
`Machine Management Provider`	`Machine Management Provider`	
`VDA Monitor Plug-in`	`User Personalization Layer`	
`VDA WMI Proxy Plug-in`	`VDA Monitor Plug-in`	
	`VDA WMI Proxy Plug-in`	
`Citrix App Protection Component`	`Citrix App Protection Component`	`Citrix App Protection Component`
`Citrix HyperV Filter Driver`	`Citrix HyperV Filter Driver`	
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`

L'exclusion de Citrix Profile Management de l'installation (`/exclude "Citrix Profile Management"`) affecte la surveillance et la résolution des problèmes des VDA avec Citrix Director. Sur les pages **Détails de l'utilisateur** et **Point de terminaison**, les panneaux Personnalisation et Durée de l'ouverture de session échouent. Sur les pages **Tableau de bord** et **Tendances**, le panneau Durée moyenne d'ouverture de session affiche les données uniquement pour les machines sur lesquelles Profile Management est installé.

Même si vous n'utilisez pas une solution de gestion de profils utilisateur tierce, Citrix vous recommande d'installer et d'exécuter Citrix Profile Management Service. L'activation de Citrix Profile Management Service n'est pas nécessaire.

Si vous spécifiez à la fois `/exclude` et `/includeadditional` avec le même nom de composant, ce composant n'est pas installé.

Cette option n'est pas valide lors de l'utilisation du programme d'installation `VDAWorkstationCoreSetup.exe`. Ce programme d'installation exclut automatiquement un grand nombre de ces éléments.

- **/h** ou **/help**

  Affiche la commande d'aide.

- **/includeadditional** "*component*"[,"*component*"]

Inclut l'installation d'un ou de plusieurs composants facultatifs séparés par des virgules et entourés de guillemets droits. Cette option peut être utile lorsque vous créez un déploiement Remote PC Access et souhaitez installer d'autres composants qui ne sont pas inclus par défaut. Les valeurs valides sont les suivantes :

OS multi-session	OS mono-session
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

Si vous spécifiez à la fois `/exclude` et `/includeadditional` avec le même nom de composant, ce composant n'est pas installé.

- **/installdir** *directory*

  Répertoire vide existant où les composants seront installés. Valeur par défaut : c:\Program Files\Citrix.

- **/install_mcsio_driver**

  Ne pas utiliser. Utiliser plutôt `/includeadditional "Citrix MCS IODriver"` ou `/exclude "Citrix MCS IODriver"`

- **/logpath** *path*

  Emplacement du fichier journal. Le dossier spécifié doit exister. Le programme d'installation ne le crée pas. Valeur par défaut = "%TEMP%\Citrix\XenDesktop Installer"

  Cette option n'est pas disponible dans l'interface graphique.

- **/masterimage**

Valide uniquement lors de l'installation de VDA sur une machine virtuelle. Configure le VDA en tant qu'image à utiliser pour créer d'autres machines. Cette option est équivalente à /mastermcsimage.

Cette option n'est pas valide lors de l'utilisation du programme d'installation VDAWorkstationCoreSetu .exe.

- **/mastermcsimage**

  Indique que cette machine sera utilisée comme image avec Machine Creation Services. Cette option est équivalente à /masterimage.

- **/masterpvsimage**

  Indique que cette machine sera utilisée comme image avec Citrix Provisioning ou un outil de provisioning tiers (tel que Microsoft System Center Configuration Manager) pour provisionner les machines virtuelles.

- **/websockettoken** *WebSocketToken*

  Crée un VDA Web Socket. Le WebSocketToken est destiné au jeton requis.

- **/no_mediafoundation_ack**

  Reconnaît que Microsoft Media Foundation n'est pas installé, et que plusieurs fonctionnalités multimédias de HDX ne seront pas installées et ne fonctionneront pas. Si cette option est omise et que Media Foundation n'est pas installé, l'installation du VDA s'arrête, car les conditions préalables ne sont pas remplies. La plupart des éditions Windows prises en charge sont fournies avec Media Foundation, à l'exception des éditions N. Si vous activez Windows Features > Media Features *manuellement*, la clé de registre recherchée par le méta-installateur Citrix peut ne pas avoir de valeur définie. Vérifiez la clé de registre SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion avant de démarrer le processus d'installation pour vous assurer que la valeur existe et qu'elle n'est pas vide.

- **/nodesktopexperience**

  La fonctionnalité Enhanced Desktop Experience n'est plus disponible. Cette option (et ce paramètre de stratégie) est ignorée, si spécifiée.

  Valide uniquement lors de l'installation d'un VDA pour OS multi-session. Empêche l'activation de la fonctionnalité Expérience de bureau améliorée. Cette fonctionnalité est contrôlée par le paramètre de stratégie Citrix Expérience de bureau améliorée.

- **/noreboot**

  Empêche un redémarrage après l'installation. Le VDA ne peut être utilisé qu'après un redémarrage.

- **/noresume**

  Par défaut, lorsqu'un redémarrage de la machine est nécessaire pendant une installation, le programme d'installation reprend automatiquement une fois le redémarrage terminé. Pour remplacer la valeur par défaut, spécifiez `/noresume`. Cela peut être utile si vous devez réinstaller le support ou si vous souhaitez capturer des informations lors d'une installation automatisée.

- **/physicalmachine**

  Utilisez cet argument en même temps que `/remotepc` pour l'installation de RemotePC. Sinon, le VDA risque de ne pas se comporter comme prévu dans certains scénarios utilisateur.

- **/portnumber** *port*

  Valide uniquement si l'option `/reconfig` est spécifiée. Numéro de port à activer pour les communications entre le VDA et le Controller. Le port configuré précédemment est désactivé, à moins qu'il s'agisse du port 80.

- **/proxyconfig** « *adresse ou chemin d'accès au fichier PAC* »

  Si vous prévoyez d'utiliser le protocole Rendezvous avec Gateway Service, VDA Upgrade Service, etc., dans votre environnement et que vous disposez d'un proxy non transparent sur votre réseau pour les connexions sortantes, indiquez ici le proxy. Seuls les proxys HTTP sont pris en charge. Adresse ou chemin d'accès au fichier PAC du proxy à utiliser avec le protocole Rendezvous. Pour plus d'informations sur les fonctionnalités, consultez Protocole Rendezvous.

  - Format d'adresse du proxy : `http://<url-or-ip>:<port>`
  - Format du fichier PAC : `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** ou **/passive**

  Aucune interface utilisateur ne s'affiche lors de l'installation. La seule preuve de l'installation et de la configuration est dans le Gestionnaire des tâches Windows. Si cette option n'est pas utilisée, l'interface graphique démarre.

- **/reconfigure**

  Personnalise les paramètres VDA précédemment configurés lorsqu'il est utilisé avec les options `/portnumber`, `/controllers` ou `/enable_hdx_ports`. Si vous spécifiez cette option sans spécifier également l'option `/quiet`, l'interface graphique de personnalisation de VDA démarre.

- **/remotepc**

  Valide uniquement pour les déploiements Remote PC Access (OS mono-session) ou les connexions négociées (OS multi-session). Exclut l'installation de tout composant supplémentaire (consultez les listes de composants avec l'option `/exclude` et `/includeadditional`).

Cette option n'est pas valide lors de l'utilisation du programme d'installation VDAWorkstationCoreSetup.exe. Ce programme d'installation exclut automatiquement l'installation de ces composants.

/remotepc n'est pas compatible avec l'option /servervdi.

- **/remove**

  Supprime les composants spécifiés avec l'option /components.

- **/remove_appdisk_ack**

  Autorise le programme d'installation du VDA à désinstaller le plug-in AppDisks VDA s'il est installé.

- **/remove_pvd_ack**

  Autorise le programme d'installation du VDA à désinstaller Personal vDisk s'il est installé.

- **/removeall**

  Supprime le VDA. Ne supprime pas l'application Citrix Workspace (si elle est installée).

- **/REMOVEALLWITHCWA**

  Supprime l'application Citrix Workspace ainsi que le VDA.

- **/sendexperiencemetrics**

  Envoie automatiquement les analyses collectées au cours de l'installation, de la mise à niveau ou de la suppression à Citrix. Si cette option est omise (ou que /disableexperiencemetrics est spécifié), les analyses sont collectées localement, mais pas envoyées automatiquement.

- **/servervdi**

  Installe un VDA pour OS mono-session sur une machine multi-session Windows prise en charge. Omettez cette option lors de l'installation d'un VDA pour OS multi-session sur une machine Windows multi-session.

  Avant d'utiliser cette option, consultez la section Server VDI.

  Utilisez cette option uniquement avec le programme d'installation du produit entier VDA.

- **/site_guid** *guid*

  Identificateur global unique (GUID) de l'unité d'organisation Active Directory du site. Associe un bureau virtuel à un site lorsque vous utilisez Active Directory pour la découverte (la mise à jour automatique est la méthode recommandée et la méthode de découverte par défaut). Le GUID du site est une propriété de site affichée dans Studio. Ne spécifiez pas à la fois les options /site_guid et /controllers.

- **/tempdir** *directory*

  Répertoire sur lequel stocker les fichiers temporaires durant l'installation. Valeur par défaut = c:\Windows\Temp.

Cette option n'est pas disponible dans l'interface graphique.

- **/virtualmachine**

  Valide uniquement lors de l'installation de VDA sur une machine virtuelle. Remplace la détection par le programme d'installation d'une machine physique, où les informations du BIOS transmises aux machine virtuelle les font passer pour des machines physiques.

  Cette option n'est pas disponible dans l'interface graphique.

- **/xendesktopcloud**

  Indique que le VDA est installé dans un déploiement de Citrix DaaS (Citrix Cloud).

Exemples d'installation d'un VDA

Installer un VDA avec le programme d'installation complet du produit :

La commande suivante installe un VDA pour OS mono-session et l'application Citrix Workspace à l'emplacement par défaut sur une machine virtuelle. Ce VDA sera utilisé comme image et utilisera MCS pour provisionner les machines virtuelles. Lors de sa première exécution, le VDA s'enregistrera auprès du Controller sur le serveur appelé `Contr-Main` dans le domaine `mydomain`. Le VDA utilisera la couche de personnalisation de l'utilisateur et l'Assistance à distance Windows.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda
,plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports
 /includeadditional "user personalization layer"/mastermcsimage /
enable_remote_assistance
```

Installer un VDA pour OS mono-session avec le programme d'installation autonome VDAWorkstationCoreSetup :

La commande suivante installe un VDA Core Services sur un OS mono-session à utiliser dans un déploiement VDI ou Remote PC Access. L'application Citrix Workspace et les autres services non fondamentaux ne sont pas installés. L'adresse d'un Controller est spécifiée, et les ports du Service de pare-feu Windows seront automatiquement ouverts. L'administrateur doit gérer les redémarrages.

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.
com"/enable_hdx_ports /noreboot
```

Personnaliser un VDA

Une fois que vous avez installé un VDA, vous pouvez personnaliser plusieurs paramètres. À partir du répertoire `\x64\XenDesktop Setup` du support du produit, exécutez `XenDesktopVdaSetup.exe`, à l'aide d'une ou plusieurs des options suivantes, qui sont décrites dans la section Options de ligne de commande pour l'installation d'un VDA.

- /reconfigure (option requise lors de la personnalisation d'un VDA)
- /h ou /help
- /quiet
- /noreboot
- /controllers
- /portnumber port
- /enable_hdx_ports

Dépannage des VDA

- Dans l'écran Studio d'un groupe de mise à disposition, l'entrée **Version de VDA installée** dans le panneau **Détails** peut ne pas être la version installée sur les machines. Les programmes et fonctionnalités Windows de la machine affichent la version actuelle du VDA.
- Une fois qu'un VDA est installé, il ne peut pas fournir d'applications ou de bureau aux utilisateurs tant qu'il n'est pas enregistré auprès d'un Delivery Controller.

  Pour en savoir plus sur les méthodes d'enregistrement du VDA et la résolution des problèmes d'enregistrement, consultez la section Enregistrement de VDA.

Options de ligne de commande pour l'installation d'un serveur d'impression universelle

L'option suivante est valide avec la commande XenDesktopPrintServerSetup.exe.

- **/enable_upsserver_port**

Lorsque cette option n'est pas spécifiée, le programme d'installation affiche la page **Pare-feu** à partir de l'interface graphique. Sélectionnez **Automatiquement** pour que le programme d'installation ajoute automatiquement les règles du pare-feu Windows ou **Manuellement** pour permettre à l'administrateur de configurer manuellement le pare-feu.

Après avoir installé les logiciels sur vos serveurs d'impression, configurez le serveur d'impression universelle à l'aide des instructions de la section Provisionner les imprimantes.

Options de ligne de commande pour installer un Secure Private Access

Les options suivantes sont valides avec la commande suivante (programme d'installation) : XenDesktopSPASetup.exe

- **/enable_spa_ports**

Ouvre les ports du pare-feu Windows requis par le Secure Private Access, si le service de pare-feu Windows est détecté, même si le pare-feu n'est pas activé. Si vous utilisez un autre pare-feu ou aucun pare-feu, vous devez configurer le pare-feu manuellement. Pour obtenir des informations sur le port, consultez la section Ports réseau.

- **/nosql**

  Empêche l'installation de Microsoft SQL Server Express sur le serveur sur lequel vous installez le Secure Private Access. Si cette option est omise, SQL Server Express est installé pour être utilisé en tant que base de données du site.

- **/help or /h or /?**

  Affiche la commande d'aide

- **/noreboot**

  Empêche un redémarrage après l'installation. Secure Private Access ne peut être utilisé qu'après un redémarrage.

- **/quiet ou /passive**

  Aucune interface utilisateur ne s'affiche lors de l'installation. La seule preuve de l'installation et de la configuration est dans le Gestionnaire des tâches Windows. Si cette option n'est pas utilisée, l'interface graphique démarre.

- **/remove**

  Supprime le Secure Private Access.

Pour en savoir plus sur les options, consultez le programme d'installation de Secure Private Access.

Informations supplémentaires

Pour plus d'informations sur la façon dont Citrix présente le résultat de l'installation des composants, veuillez consulter la section Codes de retour de l'installation de Citrix.

Installer Web Studio

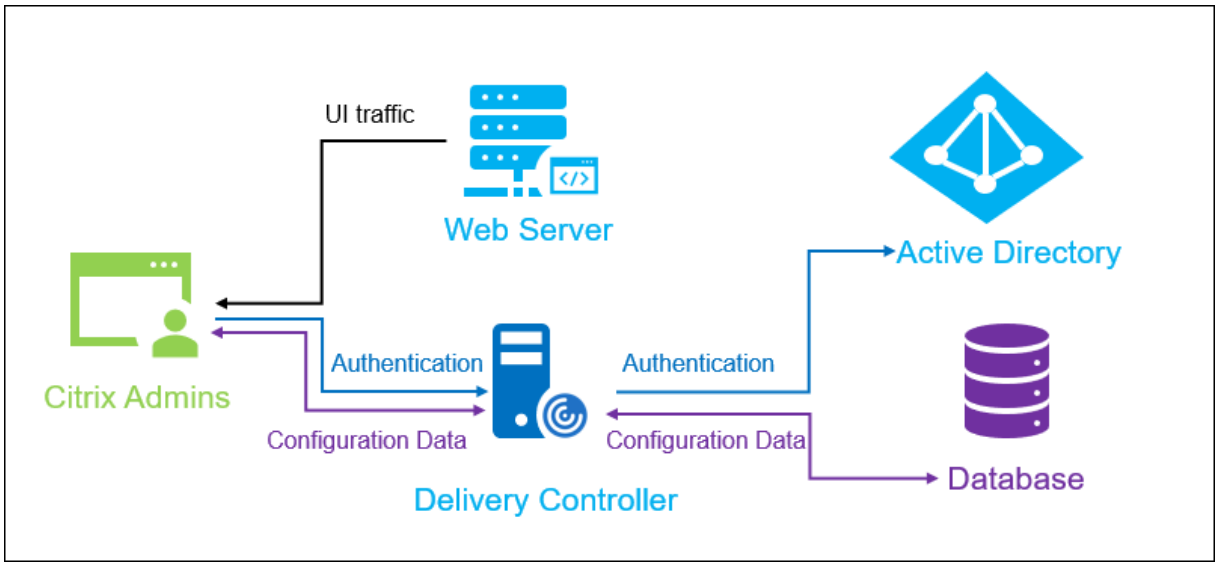
June 28, 2024

Introduction

Citrix Studio est une console de gestion Windows qui vous permet de configurer et de gérer votre déploiement Citrix Virtual Apps and Desktops. Web Studio est la nouvelle génération de Citrix Studio,

une console de gestion Web offrant la même fonctionnalité que Citrix Studio. D'apparence identique à l'interface Configuration complète de Citrix DaaS, Web Studio modernise votre expérience de gestion en proposant une expérience Web native.

Vous pouvez déployer Web Studio sur n'importe quel serveur Windows sur lequel Internet Information Service (IIS) est installé. Pour un déploiement rapide, nous vous recommandons d'installer Web Studio avec un Delivery Controller. Dans ce cas, Web Studio est installé en tant que site Web sur le Delivery Controller. Nous vous recommandons de suivre cette configuration pour simplifier votre architecture et réduire vos frais de gestion. Le schéma suivant montre l'architecture de Web Studio :



Voici un flux de travail général pour que Web Studio soit opérationnel :

1. Installer Web Studio
2. Configurer un site
3. Ajouter des Delivery Controller à Web Studio à des fins de gestion
4. Se connecter à Web Studio.

Pour configurer un déploiement de Web Studio avec équilibrage de charge, consultez cet article.

Nouvelles fonctionnalités disponibles dans Web Studio

Consultez l'article Nouveautés.

Configuration système requise

Systèmes d'exploitation pris en charge :

- Windows Server 2022
- Windows Server 2019, éditions Standard et Datacenter, avec option Server Core
- Windows Server 2016, éditions Standard et Datacenter, avec option Server Core
- Windows 11
- Windows 10

Navigateurs pris en charge :

- Internet Explorer 11
  - Le mode de compatibilité n'est pas pris en charge pour Internet Explorer. Utilisez les paramètres par défaut pour accéder à Web Studio.
  - Lorsque vous installez Internet Explorer, acceptez la valeur par défaut pour utiliser les paramètres de sécurité et de compatibilité recommandés. Si vous avez déjà installé le navigateur et que vous avez choisi de ne pas utiliser les paramètres recommandés, accédez à **Outils > Options Internet > Avancé > Réinitialiser** et suivez les instructions.
- Microsoft Edge
- Firefox ESR (version de prise en charge étendue)
- Chrome

La résolution d'écran optimale recommandée pour afficher Web Studio est 1440 x 1024.

Logiciel requis

Cette version de Web Studio est compatible avec les déploiements de Citrix Virtual Apps and Desktops 2212 et versions ultérieures.

Pour les déploiements antérieurs à 2212, effectuez d'abord une mise à niveau vers 2212, puis installez Web Studio.

Limitations connues

Si vous utilisez Web Studio et Citrix Studio de manière interchangeable, tenez compte de la limitation suivante : un modèle créé dans Web Studio n'est pas affiché dans Citrix Studio, et vice versa. En effet, Web Studio utilise une base de données différente de Citrix Studio pour stocker les modèles. Pour contourner ce problème, créez une stratégie à partir d'un modèle dans Web Studio, puis créez un modèle à partir de cette stratégie dans Citrix Studio, et vice versa.

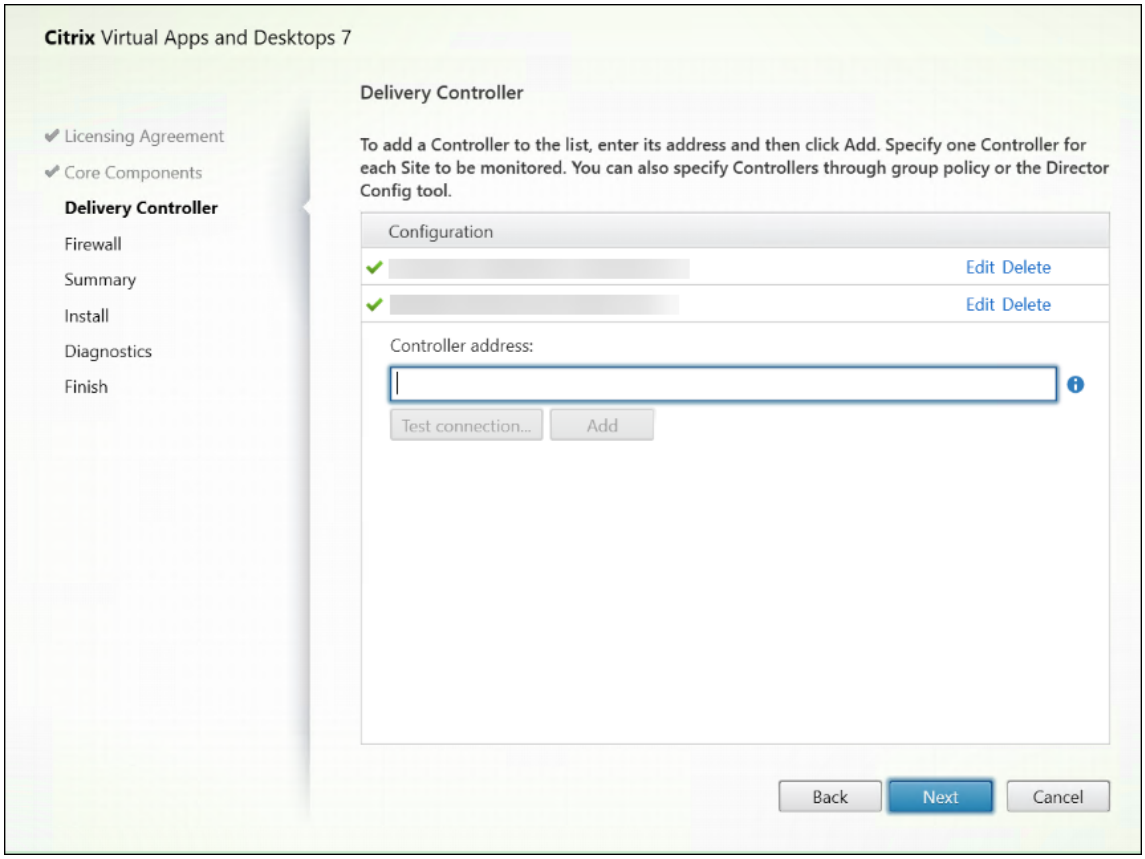
- Pour garantir la réussite de l'installation de Web Studio, ne modifiez pas le nom du site par défaut (**Site Web par défaut**) dans le gestionnaire des services Internet (IIS). Toute modification apportée au nom du site par défaut entraîne des échecs d'installation.

Installer Web Studio

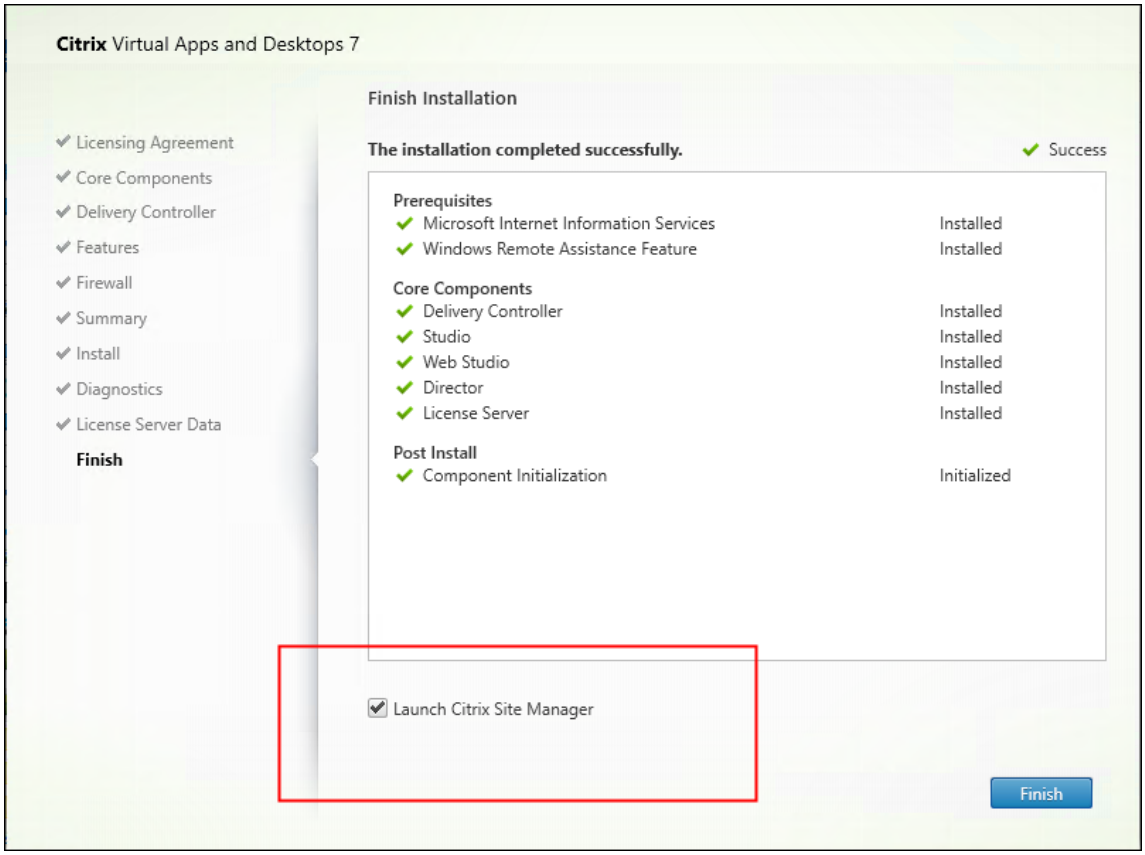
Les informations suivantes complètent les instructions de la section Installer les composants principaux. Pour installer Web Studio, procédez comme suit :

- Installez Web Studio à l'aide du programme d'installation ISO complet du produit pour Citrix Virtual Apps and Desktops. Le programme d'installation ISO vérifie les prérequis, installe les composants manquants, configure le site Web de Web Studio (sur le Delivery Controller s'il est inclus dans l'installation de Delivery Controller) et effectue la configuration de base.
- Si Web Studio n'a pas été inclus lors de l'installation, utilisez le programme d'installation pour ajouter Web Studio.
- Lors de l'installation de Web Studio, vous êtes invité à saisir l'adresse d'un Delivery Controller.

  > **Remarque :**
  >
  > - Vous pouvez ajouter plusieurs Delivery Controller. Web Studio tente de s'y connecter dans un ordre aléatoire. Si le Delivery Controller auquel Web Studio tente de se connecter est inaccessible, Web Studio revient automatiquement aux autres Delivery Controller.
  > - Si Director a été sélectionné dans **Composants principaux** et installé, les Delivery Controller que vous ajoutez ici sont utilisés à la fois pour Web Studio et Director.
  > - Si le certificat de confiance public externe n'est pas configuré et que vous ne souhaitez pas le demander à une autorité de certification d'entreprise, il vous suffit de configurer le nom de domaine complet de votre Delivery Controller.
  > - Si vous possédez le certificat de confiance public externe et que vous pouvez configurer le DNS public pour votre Delivery Controller, vous pouvez saisir le nom DNS comme adresse du Delivery Controller.
  > - Si vous pouvez demander le certificat auprès de l'autorité de certification de votre entreprise et spécifier votre DNS personnel, vous pouvez ajouter votre DNS personnel en tant qu'adresse du Delivery Controller.



- Pour sécuriser les communications entre le navigateur et le serveur Web et entre le navigateur et le Delivery Controller, le cryptage TLS doit être activé sur le site Web IIS hébergeant Web Studio et sur le Delivery Controller. Si aucun certificat TLS n'est configuré pour le Delivery Controller, le programme d'installation crée un certificat auto-signé, avec le nom de domaine complet du Delivery Controller et localhost comme certificat de nom DNS. Si un certificat TLS est configuré, le programme d'installation n'apporte aucune modification. Pour plus d'informations sur le cryptage TLS, voir Sécuriser un déploiement de Web Studio (facultatif).
- Sur la page **Fin**, la case à cocher **Lancer gestionnaire de site** est sélectionnée par défaut afin que Citrix Site Manager s'ouvre automatiquement. Pour le lancer ultérieurement, ouvrez le menu Démarrer de votre bureau et sélectionnez **Citrix > Citrix Site Manager**. Avant de lancer Web Studio, vous devez utiliser Citrix Site Manager pour créer un site ou rejoindre un site existant. Pour plus d'informations, consultez Configurer un site.



> **Remarque :**
>
> Vous pouvez également utiliser la ligne de commande pour installer Web Studio. Exemple : `.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local"/configure_firewall /quiet`. Pour de plus amples informations, consultez la section Installer à l'aide de la ligne de commande.

Configurer un site

Pour configurer votre déploiement Citrix Virtual Apps and Desktops (également appelé site), utilisez l'outil Citrix Site Manager. L'outil est installé automatiquement avec un Delivery Controller.

Pour configurer un site, procédez comme suit :

1. Sur un Delivery Controller, ouvrez le menu Démarrer du bureau, puis sélectionnez **Citrix > Citrix Site Manager**.
2. Dans Citrix Site Manager, sélectionnez **Créer un site**. L'assistant de configuration du site s'affiche.
3. Créez un site et configurez ses paramètres comme suit :
    - Sur la page **Introduction**, tapez le nom du site.

- La page **Bases de données** contient des sélections permettant de configurer les bases de données Site, Surveillance et Journalisation de la configuration. Pour plus d'informations, reportez-vous à l'étape 3. Base de données.
- Sur la page **Licences**, spécifiez l'adresse du serveur de licences, puis indiquez la licence à utiliser (installer). Pour plus d'informations, reportez-vous à l'étape 4. Gestion des licences.

4. Sur la page **Résumé**, vérifiez tous les paramètres et cliquez sur **Envoyer**.

   L'adresse IP de ce Controller est automatiquement ajoutée au site.

   > **Remarque :**
   >
   > L'utilisateur qui crée un site en devient l'administrateur complet. Pour plus d'informations, consultez Administration déléguée.

Si vous installez un nouveau Controller après avoir créé un site, vous devez ajouter le Controller au site. Les étapes détaillées sont les suivantes :

1. Exécutez Citrix Site Manager sur ce nouveau Controller.
2. Sélectionnez **Rejoindre un site existant**.
3. Entrez l'adresse d'un Controller déjà ajouté au site.
4. Cliquez sur **Envoyer**.

Ajouter des Delivery Controller à Web Studio à des fins de gestion

Utilisez l'outil de configuration Studio pour ajouter les Delivery Controller à Web Studio à des fins de gestion. Cet outil est disponible dans le dossier d'installation de Web Studio.

Par défaut, l'outil est installé dans le dossier suivant.

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Supposons que vous souhaitiez configurer les deux Delivery Controller suivants pour le site que vous souhaitez gérer avec Web Studio : `ddc1.studio.local` et `ddc2.studio.local`. Exécutez les commandes PowerShell suivantes :

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

> **Remarque :**
>
> - L'outil nécessite des autorisations d'administrateur pour l'ordinateur.
> - Les modifications de configuration du Delivery Controller peuvent ne pas prendre effet immédiatement en raison des paramètres de cache du serveur IIS. Pour un effet immédiat, accédez au serveur Web Studio, ouvrez le gestionnaire des services Internet (IIS), accédez

> à Page de démarrage > Sites > Site Web par défaut, puis sélectionnez **Redémarrer** dans le volet Gérer le site Web.
> - Pour afficher tous les paramètres pris en charge, exécutez `StudioConfig.exe --help`.

Configurer Web Studio en tant que proxy pour les Delivery Controller (facultatif)

Par défaut, lorsque vous gérez votre déploiement à l'aide de la console Web Studio, vous vous connectez au serveur Web Studio et aux Delivery Controller via le navigateur Web. Nous vous proposons la possibilité de configurer le serveur Web Studio en tant que proxy pour les Delivery Controller. Par conséquent, vous vous connectez uniquement au serveur Web Studio lorsque vous gérez votre déploiement.

Cette section vous explique comment configurer un serveur Web Studio en tant que proxy pour les Delivery Controller. Nous partons du principe que Web Studio et les Delivery Controller sont installés sur des serveurs différents.

Avant de commencer, vérifiez que tous les composants principaux nécessaires sont installés dans votre déploiement. Pour plus d'informations, voir Installer les composants principaux.

Pour activer le mode proxy pour Web Studio, procédez comme suit :

1. Sur le serveur Web Studio, exécutez Windows PowerShell en tant qu'administrateur.
2. Exécutez la commande suivante où vous remplacez `fqdn_of_webstudio_machine` par le nom de domaine complet de votre serveur Web Studio.

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe"--enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

   > **Remarque :**
   >
   > Si vous disposez d'un déploiement Web Studio avec équilibrage de charge, remplacez `fqdn_of_webstudio_machine` par le nom de domaine complet du serveur d'équilibrage de charge (également appelé serveur virtuel). Pour plus d'informations, consultez Configurer un déploiement de Web Studio avec équilibrage de charge.

Pour désactiver le mode proxy pour Web Studio, exécutez cette commande PowerShell :

```
`& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy`
```

> **Remarque :**
>
> À titre de bonne pratique, nous vous recommandons de sécuriser votre déploiement de Web Studio à l'aide d'un certificat délivré par une autorité de certification d'entreprise ou d'un certificat

> de confiance public externe. Pour plus d'informations, consultez Sécuriser un déploiement de Web Studio.

Se connecter à Web Studio

Le site Web Studio se trouve à l'adresse `https://<address of the server hosting Web Studio>/Citrix/Studio`.

Pour vous connecter à Web Studio, ouvrez le menu Démarrer de votre bureau et sélectionnez **Citrix > Citrix Web Studio**. Les administrateurs autorisés à utiliser Web Studio doivent être des utilisateurs du domaine Active Directory. Lorsque vous vous connectez à Web Studio, considérez les scénarios suivants :

- Si vous n'avez pas encore spécifié de Delivery Controller pour le site. Vous êtes invité à spécifier un Delivery Controller afin de disposer d'un accès temporaire à Web Studio.
- Si les Delivery Controller spécifiés sont actuellement inaccessibles, vous ne pouvez pas vous connecter à Web Studio. Testez vos connexions pour vous assurer que ces Delivery Controller sont accessibles. Vous pouvez également spécifier un autre Delivery Controller afin de bénéficier d'un accès temporaire à Web Studio.

Étapes suivantes

1. Installer des VDA
2. Utilisez Web Studio pour fournir des applications et des bureaux virtuels à vos utilisateurs avec :
   a) Création d'un catalogue de machines
   b) Création d'un groupe de mise à disposition
   c) Création d'un groupe d'applications (facultatif)

Installer des VDA

June 27, 2024

> **Important :**
>
> - Si vous effectuez une mise à niveau et que votre version actuelle est dotée du logiciel Personal vDisk ou AppDisks, reportez-vous à la section Suppression de PvD, AppDisks et d'hôtes non pris en charge.

> - Les fichiers binaires distribués par Citrix sont désormais signés. Les fichiers binaires signés indiquent qu'ils sont validés soit par des certificats générés par Citrix, soit par des certificats tiers authentiques.

Il existe deux types de VDA pour machines Windows : VDA pour OS multi-session et VDA pour OS mono-session (pour de plus amples informations sur les VDA pour machines Linux, consultez la documentation Virtual Delivery Agent Linux).

Avant de commencer une installation, passez en revue la section Préparer l'installation et terminez toutes les tâches de préparation.

Avant l'installation de VDA, installez les composants principaux. Vous pouvez également créer le site avant d'installer les VDA.

Cet article décrit la séquence de l'assistant d'installation lors de l'installation d'un VDA. Des lignes de commande équivalentes sont fournies. Consultez la section Installer à l'aide de la ligne de commande pour plus de détails.

Étape 1. Télécharger le logiciel du produit et démarrer l'assistant

Si vous utilisez le programme d'installation du produit entier :

1. Si vous n'avez pas encore téléchargé l'ISO du produit :
   - Utilisez vos informations d'identification de compte Citrix pour accéder à la page de téléchargement de Citrix Virtual Apps and Desktops. Téléchargez le fichier ISO du produit.
   - Décompressez le fichier. Éventuellement, gravez un DVD du fichier ISO.
2. Utilisez un compte d'administrateur local sur l'image ou la machine sur laquelle vous installez le VDA. Insérez le DVD dans le lecteur ou montez le fichier ISO. Si le programme d'installation ne se lance pas automatiquement, double-cliquez sur l'application **AutoSelect** sur le lecteur monté.

   L'assistant d'installation démarre.

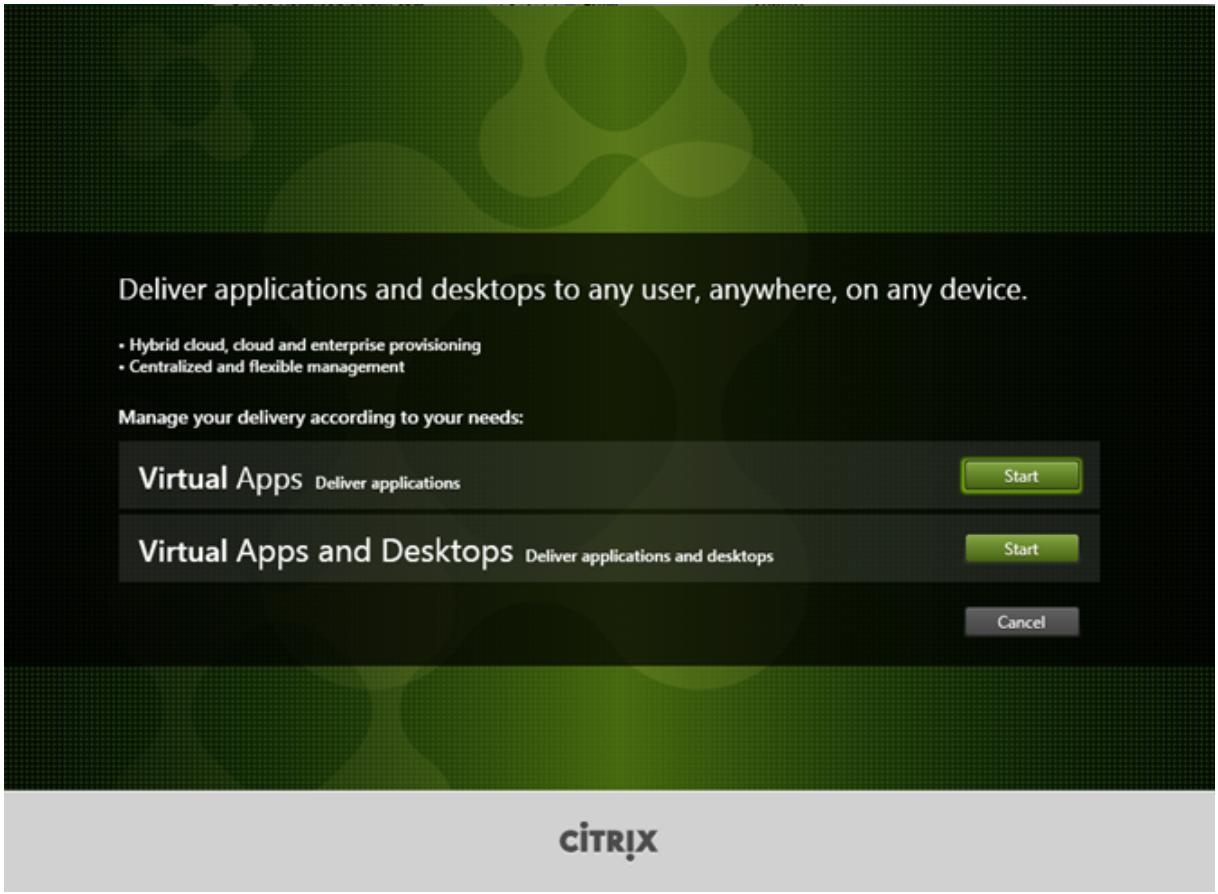
Si vous utilisez un pack autonome :

1. Utilisez vos informations d'identification de compte Citrix pour accéder à la page de téléchargement de Citrix Virtual Apps and Desktops. Téléchargez le pack approprié :
   - `VDAServerSetup_2308.exe` : VDA avec OS multi-session *version*
   - `VDAWorkstationSetup_2308.exe` : VDA avec OS mono-session *version*
   - `VDAWorkstationCoreSetup_2308.exe`: VDA avec Services de base OS mono-session *version*

2. Cliquez avec le bouton droit sur le pack et choisissez **Exécuter en tant qu'administrateur**.

   L'assistant d'installation démarre.

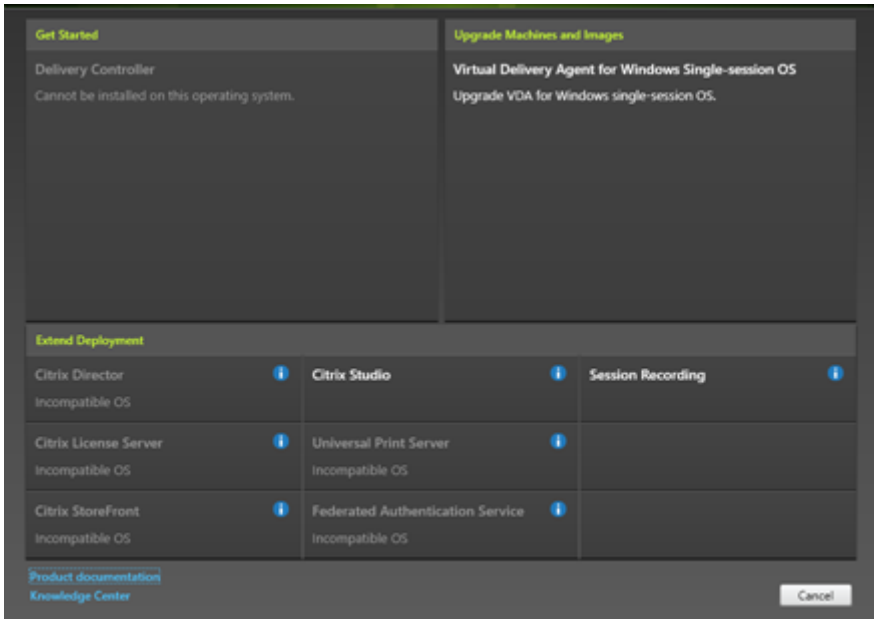
Étape 2. Choisir le produit à installer



Cliquez sur **Démarrer** à côté du produit à installer : Citrix Virtual Apps ou Citrix Virtual Desktops. (si la machine dispose déjà d'un composant Citrix Virtual Apps ou Citrix Virtual Desktops, cette page ne s'affiche pas).

Option de ligne de commande : /xenapp pour installer Citrix Virtual Apps. Citrix Virtual Desktops est installé si cette option est omise

Étape 3. Sélectionner le VDA

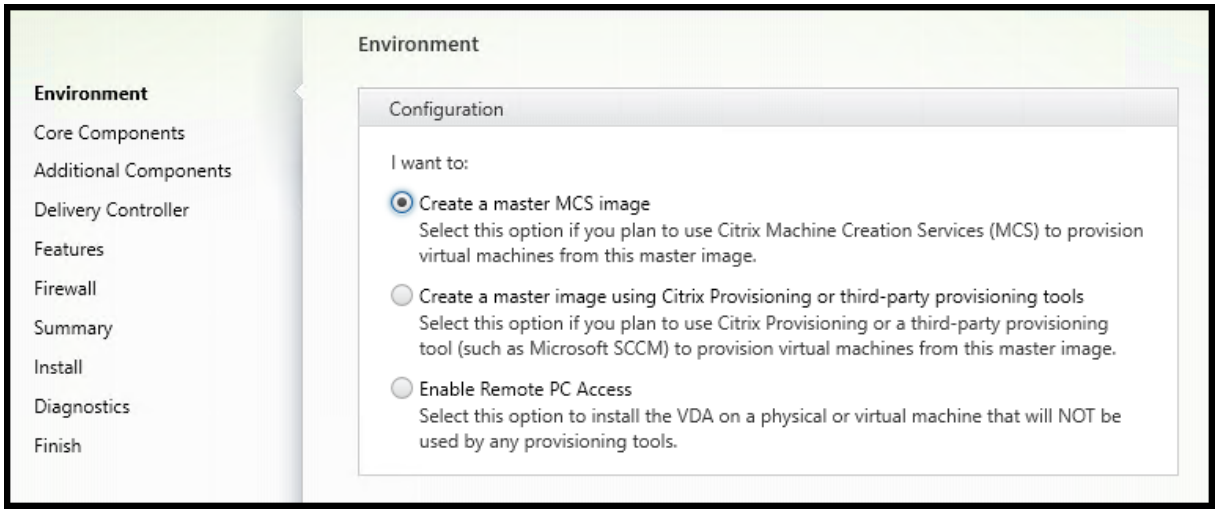


Sélectionnez l'entrée **Virtual Delivery Agent**. Le programme d'installation sait s'il s'exécute sur un OS mono-session ou multi-session, il présente donc uniquement le type de VDA approprié.

Par exemple, lorsque vous exécutez le programme d'installation sur une machine Windows Server 2019, l'option VDA pour OS multi-session est disponible. L'option VDA pour OS mono-session n'est pas disponible.

Si vous tentez d'installer (ou de mettre à niveau) un VDA Windows sur un système d'exploitation non pris en charge par cette version de Citrix Virtual Apps and Desktops, un message vous renvoie vers des informations sur les options.

Étape 4. Spécifier comment le VDA sera utilisé



Sur la page **Environnement**, indiquez comment vous prévoyez d'utiliser le VDA, en indiquant si vous utiliserez ou non cette machine en tant qu'image pour provisionner des machines.

L'option que vous choisissez affecte les outils de Citrix Provisioning qui sont installés automatiquement (le cas échéant), ainsi que les valeurs par défaut de la page Composants supplémentaires du programme d'installation du VDA.

Plusieurs MSI (Provisioning et autres) sont installés automatiquement lorsque vous installez un VDA. La seule façon d'empêcher leur installation est d'utiliser l'option `/exclude` dans une installation par ligne de commande.

Sélectionnez l'une des options suivantes :

- **Créer une image MCS principale :** sélectionnez cette option pour installer un VDA sur une image de machine virtuelle, si vous prévoyez d'utiliser Machine Creation Services pour provisionner les machines virtuelles. Cette option installe Machine Identity Service. Option par défaut.

  Option de ligne de commande : `/mastermcsimage` ou `/masterimage`

> **Important :**
>
> Le support d'installation ou l'image ISO doit être monté localement. Le montage d'une image ISO sur un lecteur réseau aux fins de l'installation d'un logiciel n'est pas pris en charge.

- **Créer une image principale à l'aide de Citrix _Provisioning ou d'outils de provisioning tiers :** sélectionnez cette option pour installer un VDA sur une image de machine virtuelle, si vous envisagez d'utiliser Citrix Provisioning ou des outils tiers (tels que Microsoft System Center Configuration Manager) pour mettre à disposition des machine virtuelle.

  Option de ligne de commande : `/masterpvsimage`

- (Apparaît uniquement sur les machines avec OS multi-session) **Activer connexions réparties à un serveur :** sélectionnez cette option pour installer un VDA sur une machine physique ou virtuelle qui ne sera pas utilisée comme image pour provisionner d'autres machines.

  Option de ligne de commande : `/remotepc`

- (Apparaît uniquement sur les machines avec OS mono-session) **Activer Remote PC Access** : sélectionnez cette option pour installer un VDA sur une machine physique à utiliser avec Remote PC Access.

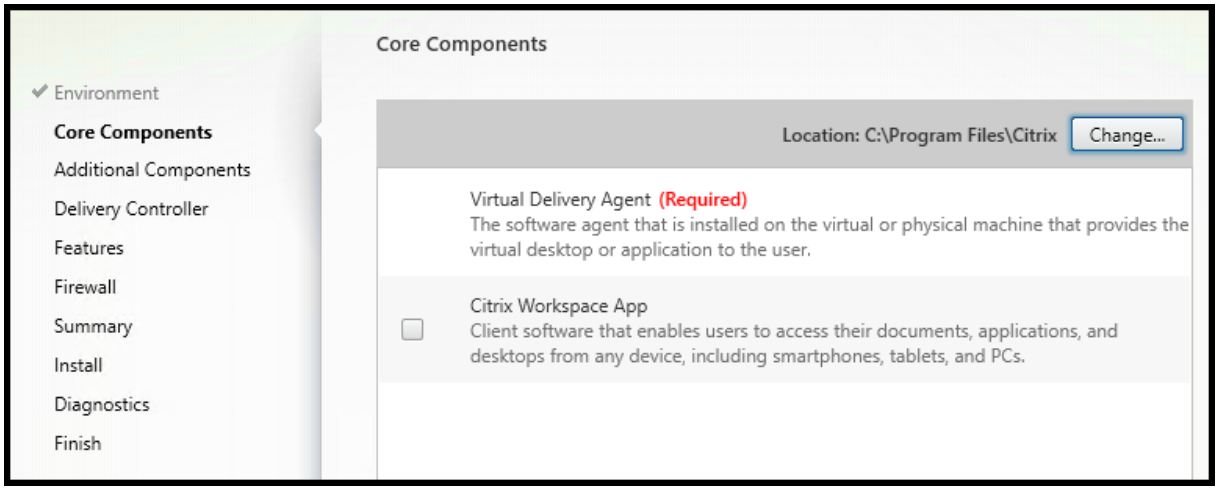
  Option de ligne de commande : `/remotepc`

Cliquez sur **Suivant**.

Cette page ne s'affiche pas :

- si vous mettez à niveau un VDA
- Si vous utilisez le programme d'installation `VDAWorkstationCoreSetup_2308.exe`, `VDAServerSetup_2308.exe` ou `VDAWorkstationSetup_2308.exe`

Étape 5. Sélectionner les composants à installer et l'emplacement d'installation



Sur la page **Composants principaux** :

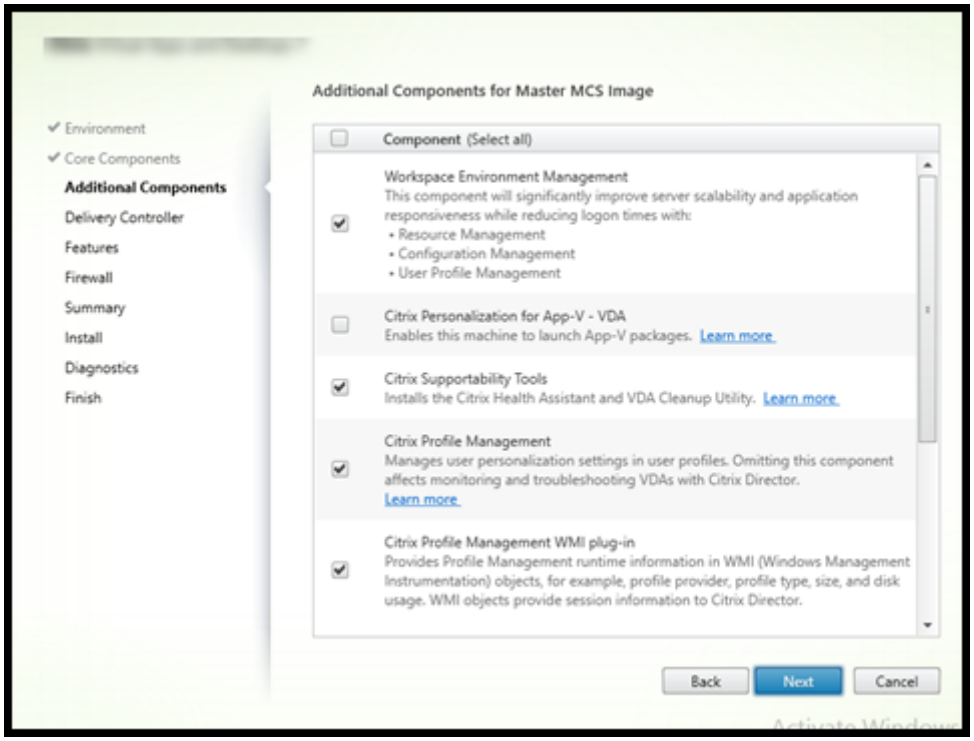
- **Emplacement :** par défaut, les composants sont installés dans `C:\Program Files\Citrix`. Ce paramètre par défaut convient à la plupart des déploiements. Si vous spécifiez un autre emplacement, ce dernier doit disposer d'autorisations `execute` pour le service réseau.
- **Composants :** par défaut, l'application Citrix Workspace pour Windows n'est pas installée avec le VDA. Si vous utilisez le programme d'installation `VDAWorkstationCoreSetup.exe`, l'application Citrix Workspace pour Windows n'est jamais installée, donc cette case à cocher n'est pas affichée.

Cliquez sur **Suivant**.

Options de ligne de commande : `/installdir`, `/components vda,plugin` pour installer le VDA et l'application Citrix Workspace pour Windows.

> **Remarque :**
>
> Vous pouvez choisir d'installer, de mettre à niveau ou de désinstaller l'application Citrix Workspace lors de l'installation, de la mise à niveau ou de la désinstallation d'un VDA dans les scénarios suivants :
>
> - Lors de l'installation d'un VDA, vous pouvez choisir d'installer l'application Citrix Workspace. Par défaut, l'application Citrix Workspace n'est pas installée lors de l'installation du VDA.
> - Lors d'une mise à niveau du VDA, si l'application Citrix Workspace n'est pas déjà installée dans le VDA, vous pouvez choisir d'installer l'application Citrix Workspace.
> - Lors d'une mise à niveau du VDA, si la version de l'application Citrix Workspace peut être mise à niveau, l'option de mise à niveau de l'application Citrix Workspace s'affiche.
> - Lors de la désinstallation d'un VDA, vous pouvez choisir de ne pas désinstaller l'application Citrix Workspace. Par défaut, l'application Citrix Workspace est désinstallée lors de la désinstallation du VDA.

Étape 6. Installer des composants supplémentaires



La page **Composants supplémentaires** contient des cases à cocher permettant d'activer ou de désactiver l'installation de fonctions et technologies supplémentaires avec le VDA. Dans une installation par ligne de commande, vous pouvez utiliser l'option `/exclude` ou `/includeadditional` pour omettre ou inclure expressément un ou plusieurs composants disponibles.

Le tableau suivant indique le paramètre par défaut des éléments sur cette page. Le paramètre par défaut dépend de l'option que vous avez sélectionnée sur la page **Environnement**.

Page Composants supplémentaires	Page Environnement : « Image principale avec MCS » ou « Image principale avec Citrix Provisioning » sélectionné	Page Environnement : « Activer connexions réparties à un serveur » (pour OS multi-session) ou « Remote PC Access » (pour OS mono-session) sélectionné
Citrix Personalization pour AppV - VDA	Non sélectionné	Non sélectionné
Couche de personnalisation de l'utilisateur	Non sélectionné	Non affiché car non valide pour ce cas d'utilisation.
Citrix Profile Management	Sélectionné	Non sélectionné
Plug-in WMI de Citrix Profile Management	Sélectionné	Non sélectionné
Agent de mise à niveau de Citrix VDA	Non sélectionné	Non sélectionné
Citrix Backup and Restore	Non sélectionné	Non sélectionné
Pilote E/S de MCS Citrix	Non sélectionné	Non sélectionné
Citrix Rendezvous V2	Non sélectionné	Non sélectionné

Cette page ne s'affiche pas si :

- Vous utilisez le programme d'installation `VDAWorkstationCoreSetup.exe`. Par ailleurs, les options de ligne de commande des composants supplémentaires ne sont pas valides avec ce programme d'installation.
- Vous mettez à niveau un VDA et tous les composants supplémentaires sont déjà installés. Si certains des composants supplémentaires sont déjà installés, la page répertorie uniquement ceux qui ne sont pas installés.

Cochez ou désélectionnez les cases suivantes. (Les composants peuvent apparaître dans un ordre différent dans le programme d'installation.)

- **Citrix Personalization pour App-V :** installez ce composant si vous prévoyez d'utiliser des applications à partir de packages Microsoft App-V. Pour plus d'informations, consultez la section

Déployer et fournir des applications App-V.

Option de ligne de commande : `/includeadditional "Citrix Personalization for App-V – VDA"` pour permettre l'installation du composant, `/exclude "Citrix Personalization for App-V – VDA"` pour empêcher l'installation du composant.

- **Couche de personnalisation de l'utilisateur Citrix :** installe le MSI pour la couche de personnalisation de l'utilisateur. Pour plus d'informations, voir Couche de personnalisation de l'utilisateur.

  Ce composant apparaît uniquement lors de l'installation d'un VDA sur une machine Windows 10 mono-session.

  Option de ligne de commande : `/includeadditional "User Personalization Layer"` pour permettre l'installation du composant, `/exclude "User Personalization Layer"` pour empêcher l'installation du composant.

- **Citrix Profile Management :** ce composant permet de gérer les paramètres de personnalisation utilisateur dans les profils utilisateur. Pour de plus amples informations, consultez la section Profile Management.

  L'exclusion de Citrix Profile Management à partir de l'installation de ces paramètres affecte la surveillance et la résolution des problèmes des VDA avec Citrix Director. Sur les pages **Détails de l'utilisateur** et **Point de terminaison**, les panneaux **Personnalisation** et **Durée de l'ouverture de session** échouent. Sur les pages **Tableau de bord** et **Tendances**, le panneau **Durée moyenne d'ouverture de session** affiche les données uniquement pour les machines sur lesquelles Profile Management est installé.

  Même si vous n'utilisez pas une solution de gestion de profils utilisateur tierce, Citrix vous recommande d'installer et d'exécuter Citrix Profile Management Service. L'activation de Citrix Profile Management Service n'est pas nécessaire.

  Option de ligne de commande : `/includeadditional "Citrix Profile Management "` pour permettre l'installation du composant, `/exclude "Citrix Profile Management "` pour empêcher l'installation du composant.

- **Plug-in WMI de Citrix Profile Management :** ce plug-in fournit des informations d'exécution sur Profile Management dans les objets WMI (Windows Management Instrumentation), par exemple le fournisseur de profils, le type de profil, la taille et l'utilisation du disque. Les objets WMI fournissent des informations sur les sessions à Director.

  Option de ligne de commande : `/includeadditional "Citrix Profile Management WMI Plug-in"` pour permettre l'installation du composant, `/exclude "Citrix Profile Management WMI Plug-in"` pour empêcher l'installation du composant.

- **Agent de mise à niveau de VDA :** applicable uniquement aux déploiements Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Permet au VDA de participer à la fonctionnal-

ité de mise à niveau de VDA. Vous pouvez utiliser cette fonctionnalité pour mettre à niveau les VDA d'un catalogue à partir de la console de gestion, immédiatement ou à une heure planifiée. Si cet agent n'est pas installé, vous pouvez mettre à niveau un VDA en exécutant le programme d'installation du VDA sur la machine.

Options de ligne de commande : `/includeadditional "Citrix VDA Upgrade Agent"` pour permettre l'installation du composant, `/exclude "Citrix VDA Upgrade Agent"` pour empêcher l'installation du composant.

- **Cache en écriture des E/S de MCS pour optimiser le stockage :** installe le pilote d'E/S de MCS Citrix. Pour plus d'informations, consultez les sections Stockage partagé par les hyperviseurs et Configurer un cache pour les données temporaires.

  Options de ligne de commande : `/includeadditional "Citrix MCS IODriver"` pour permettre l'installation du composant, `/exclude "Citrix MCS IODriver"` pour empêcher l'installation du composant.

- **Configuration du proxy :** installez ce composant si vous prévoyez d'utiliser le protocole Rendezvous avec le Gateway Service, VDA Upgrade Service, etc., dans votre environnement et si vous disposez d'un proxy non transparent sur votre réseau pour les connexions sortantes, indiquez le proxy ici. Seuls les proxys HTTP sont pris en charge.

  Si vous installez ce composant, spécifiez l'adresse du proxy ou le chemin d'accès au fichier PAC sur la page **Configuration du proxy Rendezvous** . Pour plus d'informations sur les fonctionnalités, consultez Protocole Rendezvous.

  Option de ligne de commande : `/includeadditional "Citrix Rendezvous V2"` pour permettre l'installation du composant, `/exclude "Citrix Rendezvous V2"` pour empêcher l'installation du composant.

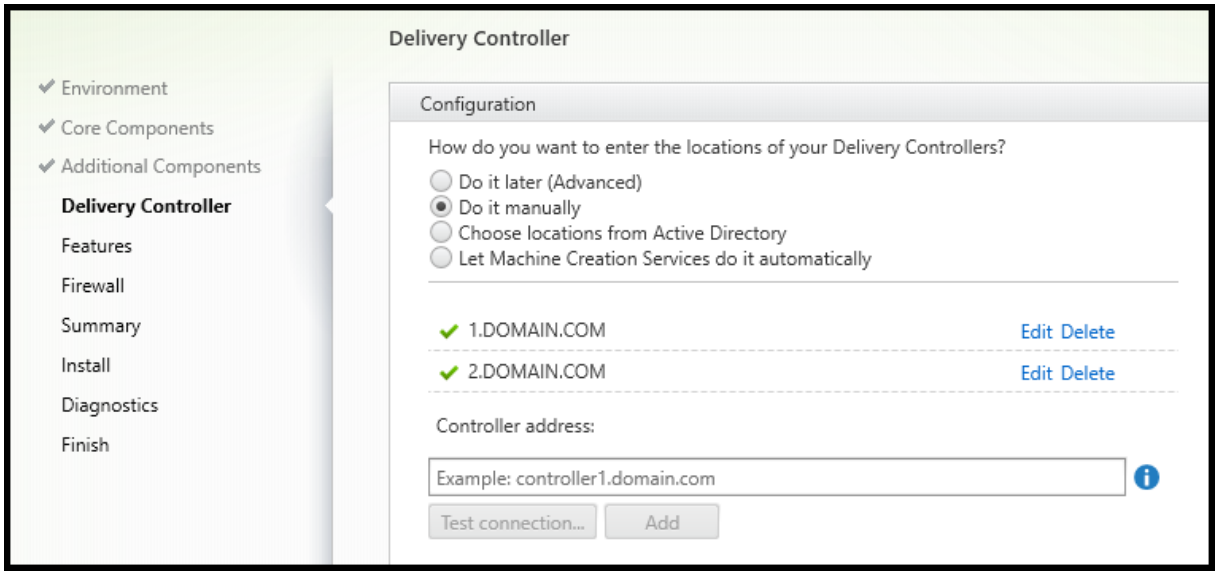
- **Citrix Backup and Restore :** si l'installation ou la mise à niveau d'un VDA échoue, ce composant peut renvoyer la machine à une sauvegarde effectuée avant l'installation ou la mise à niveau.

  Assurez-vous que les conditions préalables Microsoft sont remplies, comme indiqué dans la section Préparer l'installation.

  Option de ligne de commande : `/includeadditional "Citrix Backup and Restore"` pour permettre l'installation du composant, `/exclude "Citrix Backup and Restore"` pour empêcher l'installation du composant.

  > **Remarque :**
  >
  > Si l'optimisation du stockage MCS est activée, la sauvegarde ou la restauration pour le système d'exploitation Windows Server ou de bureau peut échouer. Pour résoudre ce problème, désactivez l'option d'optimisation du stockage MCS dans le méta-installateur.

Étape 7. Adresses Delivery Controller



Sur la page **Delivery Controller**, choisissez la manière dont vous souhaitez entrer les adresses des Controller installés. Citrix vous recommande de spécifier les adresses pendant que vous installez le VDA (**Effectuer manuellement**). Le VDA ne peut pas s'enregistrer auprès d'un Controller sans ces informations. Si un VDA ne peut pas s'enregistrer, les utilisateurs ne peuvent pas accéder aux applications et aux bureaux sur ce VDA.

- **Effectuer manuellement :** (valeur par défaut) entrez le nom de domaine complet d'un Controller installé, puis cliquez sur **Ajouter**. Si vous avez installé des Controller supplémentaires, ajoutez leurs adresses.
- **Le faire plus tard (avancé) :** si vous choisissez cette option, l'assistant vous demande de confirmer avant de continuer. Pour spécifier des adresses ultérieurement, vous pouvez soit exécuter de nouveau le programme d'installation ultérieurement soit utiliser la stratégie de groupe Citrix. L'assistant vous le rappelle également sur la page **Résumé**.
- **Choisir les emplacements d'Active Directory :** valide uniquement lorsque la machine est associée à un domaine et que l'utilisateur est un utilisateur de domaine.
- **Utiliser le jeton WebSocket (Technical Preview) :** crée un VDA WebSocket. Le WebSocketToken est destiné au jeton requis.
- **Laisser Machine Creation Services effectuer ceci automatiquement :** valide uniquement si vous utilisez MCS pour provisionner des machines.

Cliquez sur **Suivant**. Si vous avez sélectionné l'option **Le faire plus tard (avancé)**, vous êtes invité à confirmer que vous devrez spécifier des adresses de Controller ultérieurement.

Autres considérations :

- L'adresse ne peut pas contenir de caractères non alphanumériques.

- Si vous spécifiez les adresses lors de l'installation du VDA et dans la stratégie de groupe, les paramètres de la stratégie remplacent les paramètres fournis au cours de l'installation.
- L'enregistrement du VDA requiert également que les ports de pare-feu utilisés pour les communications avec le Controller soient ouverts. Ce paramètre est activé par défaut sur la page **Pare-feu** de l'assistant.
- Une fois que vous avez spécifié l'emplacement des Controller (au cours de l'installation du VDA ou ultérieurement), vous pouvez utiliser la fonctionnalité de mise à jour automatique pour mettre les VDA à jour lorsque des Controller sont ajoutés ou supprimés. Pour de plus amples informations sur la façon dont les VDA découvrent et s'enregistrent auprès de Controller, consultez Enregistrement de VDA.

Option de ligne de commande : `/controllers`

Étape 8. Configuration du proxy

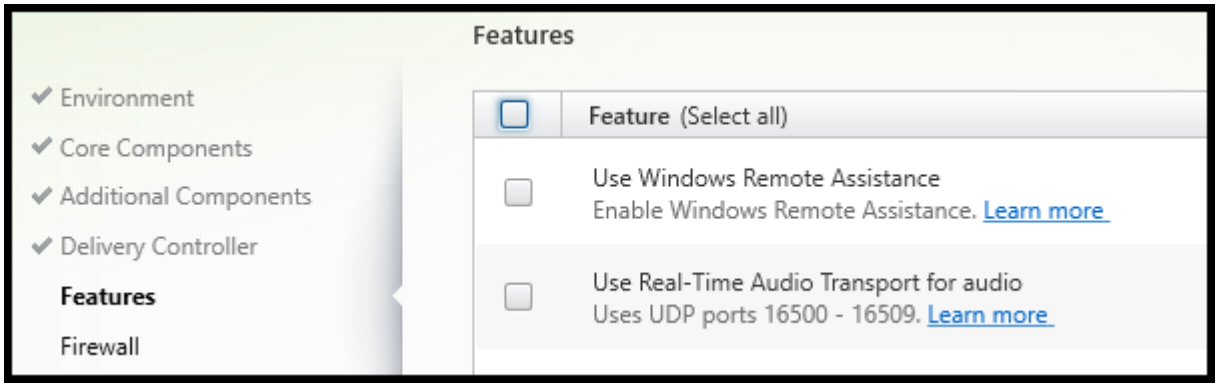
La page **Configuration du proxy** s'affiche uniquement si vous avez coché la case **Configuration du proxy** sur la page **Composants supplémentaires**.

1. Indiquez si vous allez spécifier la source proxy par adresse proxy ou chemin d'accès au fichier PAC.
2. Spécifiez l'adresse proxy ou le chemin d'accès au fichier PAC.
    - Format d'adresse du proxy : `http://<url-or-ip>:<port>`
    - Format du fichier PAC : `http://<url-or-ip>:<port>/<path>/<filename>.pac`

Le pare-feu du port proxy doit être ouvert pour que le test de connexion réussisse. Si aucune connexion ne peut être établie avec le proxy, vous pouvez choisir de poursuivre l'installation du VDA.

Option de ligne de commande : `/proxyconfig`

Étape 9 –Activer ou désactiver des fonctionnalités



Sur la page **Fonctionnalités**, cochez les cases pour activer ou désactiver les fonctionnalités que vous souhaitez utiliser.

- **Utiliser Windows Remote Assistance :** lorsque cette option est activée, l'Assistance à distance Windows est utilisée avec la fonctionnalité d'observation utilisateur de Director. L'Assistance à distance Windows ouvre les ports dynamiques dans le pare-feu. (Valeur par défaut = désactivé)

  Option de ligne de commande : `/enable_remote_assistance`

- **Utiliser le transport audio en temps réel pour l'audio :** activez cette fonctionnalité si la fonctionnalité VoIP est largement utilisée dans votre réseau. Cette fonctionnalité réduit la latence et améliore la résilience audio sur les réseaux avec perte. Elle permet aux données audio d'être transmises à l'aide du protocole de transport RTP via UDP. (Valeur par défaut = désactivé)

  Option de ligne de commande : `/enable_real_time_transport`

- **Utiliser le partage d'écran :** lorsque cette option est activée, les ports utilisés par le partage d'écran sont ouverts dans le pare-feu Windows. (Valeur par défaut = désactivé)

  Option de ligne de commande : `/enable_ss_ports`

- **Ce VDA est-il installé sur une VM dans le cloud :** ce paramètre aide Citrix à identifier correctement les emplacements de ressources des déploiements de VDA locaux et de service (Citrix Cloud) à des fins de télémétrie. Cette fonctionnalité n'a aucun impact sur l'utilisation du côté client. Activez ce paramètre si votre déploiement utilise le service Citrix DaaS (par défaut = désactivé)

  Option de ligne de commande : `/xendesktopcloud`

Cliquez sur **Suivant**.

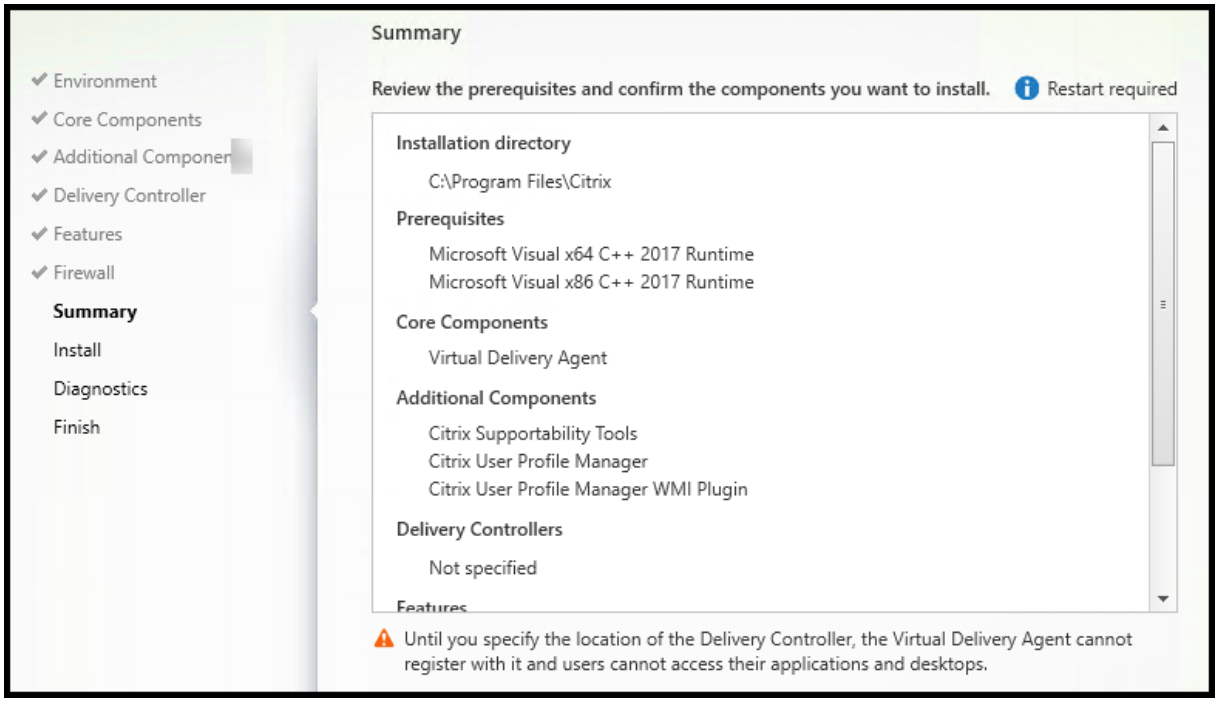
Étape 10. Ports du pare-feu

Sur la page **Pare-feu**, par défaut, les ports sont ouverts automatiquement si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Ce paramètre par défaut convient à la plupart des déploiements. Pour obtenir des informations sur le port, consultez la section Ports réseau.

Cliquez sur **Suivant**.

Option de ligne de commande : `/enable_hdx_ports`

Étape 11. Vérifier les composants requis et confirmer l'installation

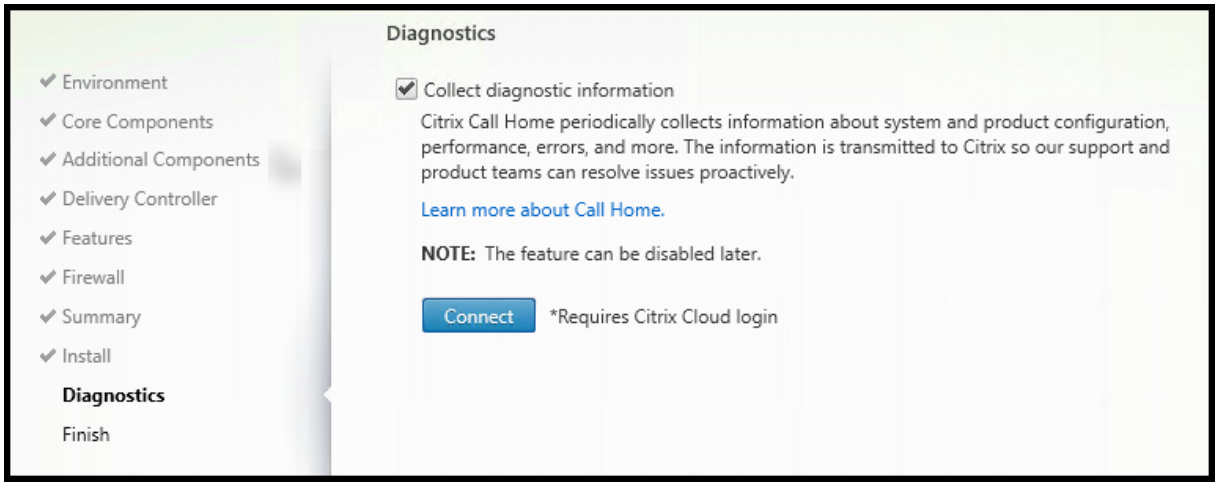


La page **Résumé** répertorie les éléments qui seront installés. Utilisez le bouton **Précédent** pour revenir sur les pages précédentes de l'assistant et modifier les réglages.

Lorsque vous êtes prêt, cliquez sur **Installer**.

Si des composants requis ne sont pas déjà installés ou activés, la machine peut redémarrer plusieurs fois. Consultez la section Préparer l'installation.

Étape 12. Diagnostics



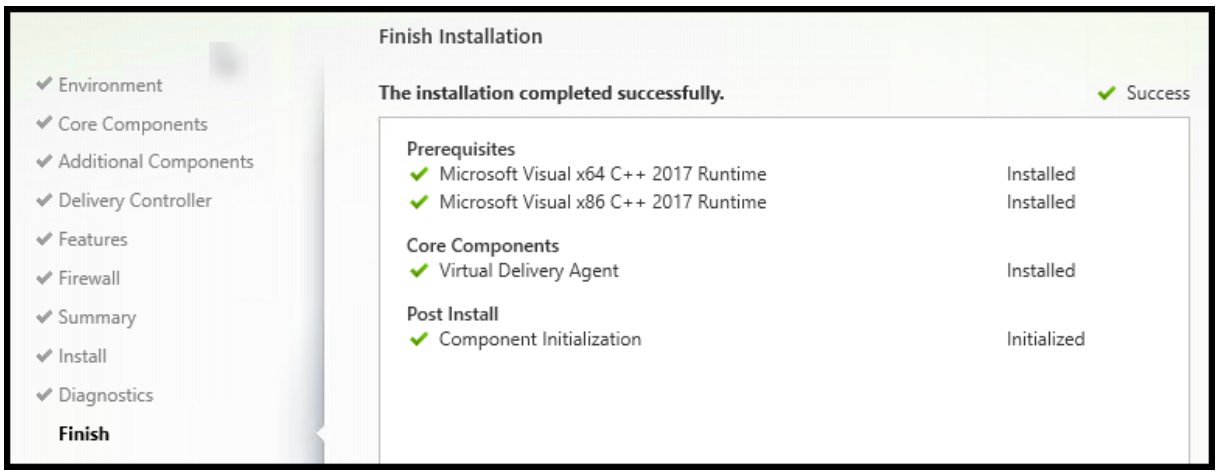
Sur la page **Diagnostics**, indiquez si vous souhaitez participer au programme Citrix Call Home. Si vous choisissez de participer (valeur par défaut), cliquez sur **Connecter**. Lorsque vous y êtes invité, saisissez vos informations d'identification de compte Citrix.

Une fois que vos informations d'identification sont validées (ou si vous choisissez de ne pas participer au programme), cliquez sur **Suivant**.

Lorsque vous utilisez le programme d'installation complet du produit, si vous cliquez sur **Se connecter** sur la page **Diagnostics** sans sélectionner d'abord **Collecter des informations de diagnostic**, après avoir fermé la boîte de dialogue **Se connecter à Citrix Insight Services**, le bouton **Suivant** est désactivé. Vous ne pouvez pas passer à la page suivante. Pour réactiver le bouton **Suivant**, sélectionnez et désélectionnez immédiatement **Collecter des informations de diagnostic**.

Pour plus d'informations, consultez Call Home.

Étape 13. Terminer cette installation



La page **Terminer** contient des coches vertes pour tous les éléments pré-requis et composants installés et initialisés avec succès.

Cliquez sur **Terminer**. Par défaut, la machine redémarre automatiquement. Bien que vous puissiez désactiver le redémarrage automatique, le VDA ne peut pas être utilisé jusqu'à ce que la machine redémarre.

Étapes suivantes

Répétez la procédure ci-dessus pour installer des VDA sur d'autres machines ou images, si nécessaire.

Après avoir installé tous les VDA, démarrez Studio. Si vous n'avez pas encore créé de site, Studio vous guide dans cette tâche. Lorsque vous avez terminé, Studio vous guide dans la création d'un catalogue

de machines, puis d'un groupe de mise à disposition. Consultez :

- Créer un site
- Créer des catalogues de machines
- Créer des groupes de mise à disposition

Citrix Optimizer

Citrix Optimizer est un outil pour Windows qui aide les administrateurs Citrix à optimiser les VDA en supprimant et en optimisant divers composants.

Après avoir installé un VDA et terminé le redémarrage final, téléchargez et installez Citrix Optimizer. Voir CTX224676. L'article CTX contient le package de téléchargement, ainsi que des instructions sur l'installation et l'utilisation de Citrix Optimizer.

Personnaliser un VDA

Pour personnaliser un VDA installé, procédez comme suit :

1. À partir de la fonctionnalité Windows de suppression ou modification des programmes, sélectionnez **Citrix Virtual Delivery Agent** ou **Citrix Remote PC Access/VDI Core Services VDA**. Cliquez ensuite avec le bouton droit sur **Modifier**.
2. Sélectionnez **Personnaliser les paramètres Virtual Delivery Agent**. Lorsque le programme d'installation démarre, vous pouvez modifier :
   - les adresses de Controller
   - le numéro du port TCP/IP à enregistrer auprès du Controller (valeur par défaut = 80)
   - si les ports de pare-feu Windows doivent s'ouvrir automatiquement

Dépannage

- Pour en savoir plus sur la façon dont Citrix présente le résultat de l'installation des composants, consultez Codes de retour de l'installation Citrix.
- Dans l'écran Studio d'un groupe de mise à disposition, l'entrée **Version de VDA installée** dans le panneau **Détails** peut ne pas être la version installée sur les machines. Les programmes et fonctionnalités Windows de la machine affichent la version actuelle du VDA.
- Une fois qu'un VDA est installé, il ne peut pas fournir d'applications ou de bureau aux utilisateurs tant qu'il n'est pas enregistré auprès d'un Delivery Controller.

  Pour en savoir plus sur les méthodes d'enregistrement du VDA et la résolution des problèmes d'enregistrement, consultez la section Enregistrement de VDA.

Limitation connue

Lorsque vous utilisez l'application Citrix Workspace pour Windows version 1912 ou antérieure, la session est interrompue au bout d'un moment. Ce problème est résolu dans les nouvelles versions LTSR et CR de l'application Citrix Workspace.
Pour plus d'informations sur les versions prises en charge, consultez Application Citrix Workspace pour Windows/Citrix Receiver pour Windows Long Term Service Releases.

Configurer Windows Defender Access Control dans le cadre de l'installation de VDA

June 27, 2024

Les clients configurent les paramètres de Windows Defender Access Control (WDAC) pour interdire le chargement de fichiers binaires non signés. Les fichiers binaires non signés distribués via les programmes d'installation de VDA sont donc interdits, ce qui limite l'installation du VDA.

Citrix signe désormais tous les fichiers binaires générés par Citrix à l'aide d'un certificat de signature de code Citrix. Citrix signe également les fichiers binaires tiers qui sont distribués avec notre produit à l'aide d'un certificat qui authentifie ces fichiers binaires tiers en tant que fichiers binaires fiables.

> **Important :**
>
> La mise à niveau d'un ancien VDA avec des fichiers binaires tiers non signés vers une version plus récente du VDA avec des fichiers binaires signés peut ne pas toujours placer les fichiers binaires signés sur la machine mise à niveau.
> Cela est dû à un mécanisme du système d'exploitation selon lequel la mise à niveau du système ne remplace pas les fichiers binaires par la même version.
> Bien que les fichiers binaires tiers aient été signés, leurs versions, contrôlées par des tiers, ne peuvent pas être mises à jour par Citrix, de sorte que ces fichiers binaires ne sont pas mis à jour.
> Pour éviter cette limitation, procédez comme suit :
>
> 1. Incluez les fichiers binaires dans une liste verte. Il n'est donc plus nécessaire de signer les fichiers binaires.
> 2. Désinstallez l'ancien VDA et installez le nouveau VDA. Cela ressemble à une nouvelle installation de VDA et les versions signées seront installées.

Créer une nouvelle stratégie de base à l'aide de l'assistant

WDAC vous permet d'ajouter des fichiers binaires fiables à exécuter sur votre système. Après l'installation de WDAC, l'**Assistant de stratégie Windows Defender Application Control** s'ouvre automatiquement.

Pour ajouter les fichiers binaires, une nouvelle stratégie WDAC de base doit être créée. Les directives recommandées par Citrix pour la création d'une stratégie de base sont fournies dans cette section.

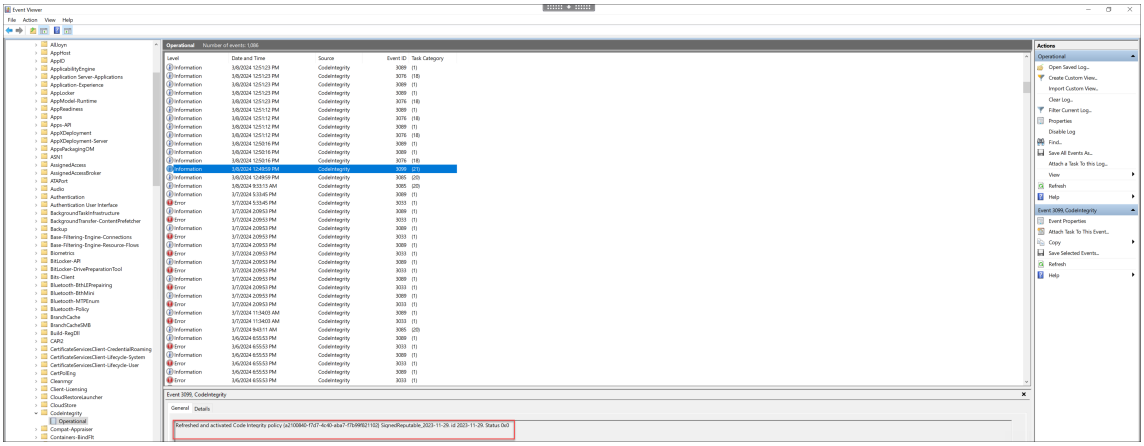
- Sélectionnez le mode **Signed and Reputable Mode** comme modèle de base, car il autorise les composants d'exploitation Windows, les applications installées depuis le Microsoft Store, tous les logiciels signés par Microsoft et les pilotes tiers compatibles avec le matériel Windows.
- Activez l'option **Enable Audit Mode**, car elle vous permet de tester les nouvelles stratégies Windows Defender Application Control avant de les appliquer.
- Pour **Files Rules**, ajoutez une règle personnaliséeCustom Rule afin de spécifier le niveau auquel les applications sont identifiées et fiables, et fournissez un fichier de référence. En sélectionnant « Publisher » comme type de règle, vous pouvez sélectionner un fichier de référence signé par l'un des certificats Citrix.
- Une fois les règles ajoutées, accédez au dossier dans lequel les fichiers `.XML` et `.CIP` sont enregistrés. Le fichier `.XML` contient toutes les règles définies dans la stratégie. Il peut être configuré pour modifier, ajouter ou supprimer des règles.
- Avant de déployer les stratégies WDAC, le fichier `.XML` doit être converti dans sa forme binaire. Le fichier WDAC convertit le fichier `.XML` en fichier `.CIP`.
- Copiez et collez le fichier `.CIP` dans C:\WINDOWS\System32\CodeIntegrity\CiPolicies\Active et redémarrez l'ordinateur. La stratégie générée sera appliquée en mode audit.
- Pour un processus étape par étape permettant de créer une stratégie de base, consultez la page Création d'une stratégie de base avec l'Assistant.

Lorsque cette stratégie est appliquée, WDAC n'émet aucun avertissement concernant les fichiers Citrix signés par l'autorité d'éditeur ou de certification spécifiée.

De même, nous pouvons créer une règle au niveau de l'éditeur pour les fichiers qui ont été signés par le tiers.

Vérifier la stratégie appliquée

1. Après le redémarrage de la machine, ouvrez **l'observateur d'événements** et accédez à **Journaux des applications et des services > Microsoft > Windows > CodeIntegrity > Operational**.
2. Assurez-vous que la stratégie appliquée est activée.



3. Recherchez les journaux qui n'ont pas respecté la stratégie et vérifiez les propriétés de ce fichier. Tout d'abord, confirmez qu'il a été signé. Si ce n'est pas le cas et que cette machine a fait l'objet d'une mise à niveau du VDA, il s'agit probablement du cas décrit dans la limitation ci-dessus. S'il est signé, ce fichier est potentiellement signé avec l'autre certificat, comme décrit précédemment.

Exemple de fichier généré par Citrix et signé avec un certificat Citrix : `C:\Windows\System32\drivers\picadm.sys`.
Exemple de fichier binaire tiers signé avec le certificat tiers Citrix : `C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`.

Installer des VDA à l'aide de scripts

June 27, 2024

> **Remarque :**
>
> Citrix n'est pas responsable des problèmes causés par des scripts qui ont été modifiés pour répondre aux exigences des environnements de production des clients. Pour tout problème lié à l'installation de Citrix, ouvrez un dossier de support technique et ajoutez-y les journaux d'installation correspondants à l'aide du portail de support Citrix.

Cet article s'applique à l'installation de VDA sur des machines avec systèmes d'exploitation Windows. Pour de plus amples informations sur les VDA pour systèmes d'exploitation Linux, consultez la documentation Virtual Delivery Agent Linux.

Le support d'installation contient des exemples de scripts qui permettent d'installer, mettre à niveau ou supprimer les VDA pour des machines dans Active Directory. Vous pouvez également utiliser les scripts pour gérer les images principales utilisées par Machine Creation Services et Citrix Provisioning (anciennement Provisioning Services).

Accès requis :

- Les scripts doivent disposer d'un accès en lecture Tout le monde sur le partage réseau sur lequel figure la commande d'installation. La commande d'installation est `XenDesktopVdaSetup.exe` à partir de l'image ISO du produit complet ou bien `VDAWorkstationSetup.exe` ou `VDAServerSetup.exe` dans un programme d'installation autonome.
- Les informations de journalisation sont stockées sur chaque machine locale. Pour consigner les résultats de manière centralisée à des fins de vérification et d'analyse, les scripts doivent disposer d'un accès en lecture et écriture Tout le monde sur le partage réseau approprié.

Pour vérifier les résultats de l'exécution d'un script, examinez le partage du journal central. Les journaux consignés incluent le journal du script, le journal du programme d'installation et les journaux d'installation MSI. Chaque tentative d'installation ou de suppression est enregistrée dans un dossier horodaté. Le titre du dossier indique le résultat de l'opération avec le préfixe PASS ou FAIL. Vous pouvez utiliser les outils de recherche d'annuaire standard pour trouver une installation ayant échoué ou une suppression dans le journal central. Cela vous évite d'effectuer une recherche locale sur les machines cibles.

Avant de commencer l'installation, lisez et complétez les tâches décrites dans la section Préparer l'installation.

Installer ou mettre à niveau des VDA à l'aide du script

1. Obtenez le script exemple **InstallVDA.bat** à partir de \Support\AdDeploy\ sur le support d'installation. Citrix vous recommande d'effectuer une sauvegarde du script d'origine avant de le personnaliser.
2. Modifiez le script :
    - Spécifiez la version du VDA à installer : `SET DESIREDVERSION`. La valeur complète est disponible sur le support d'installation dans le fichier ProductVersion.txt. Toutefois, une correspondance complète n'est pas nécessaire.
    - Spécifiez l'emplacement du partage réseau où le programme d'installation va être appelé. Pointez sur la racine de la structure (point le plus élevé de l'arborescence). La version appropriée du programme d'installation (32 bits ou 64 bits) est automatiquement appelée lorsque le script s'exécute. Par exemple : `SET DEPLOYSHARE=\\fileserver1\share1`.
    - Si vous le souhaitez, vous pouvez spécifier un emplacement de partage réseau pour le stockage des journaux centralisés. Par exemple : `SET LOGSHARE=\\fileserver1\log1`).
    - Spécifiez les options de configuration VDA comme décrit dans la section Installer à l'aide de la ligne de commande. Les options `/quiet` et `/noreboot` sont incluses par défaut dans le script et sont requises : `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT`.

3. À l'aide de scripts de démarrage de stratégie de groupe, attribuez le script à l'unité d'organisation contenant vos machines. Cette unité d'organisation doit uniquement contenir les machines sur lesquelles vous souhaitez installer le VDA. Lorsque les machines dans l'unité d'organisation sont redémarrées, le script s'exécute sur toutes ces machines. Un VDA est installé sur chaque machine qui dispose d'un système d'exploitation pris en charge.

Supprimer des VDA à l'aide du script

1. Obtenez le script exemple UninstallVDA.bat à partir de \Support\AdDeploy\ sur le support d'installation. Citrix vous recommande d'effectuer une sauvegarde du script d'origine avant de le personnaliser.
2. Modifiez le script.
   - Spécifiez la version du VDA à supprimer : `SET CHECK\\_VDA\\_VERSION`. La valeur complète est disponible sur le support d'installation dans le fichier ProductVersion.txt (par exemple, 7.0.0.3018). Toutefois, une correspondance complète n'est pas nécessaire.
   - Si vous le souhaitez, vous pouvez spécifier un emplacement de partage réseau pour le stockage des journaux centralisés.
3. À l'aide de scripts de démarrage de stratégie de groupe, attribuez le script à l'unité d'organisation contenant vos machines. Cette unité d'organisation doit uniquement contenir les machines sur lesquelles vous souhaitez supprimer le VDA. Lorsque les machines dans l'unité d'organisation sont redémarrées, le script s'exécute sur toutes ces machines et supprime un VDA de chaque machine. Le VDA est supprimé de chaque machine.

Dépannage

- Le script génère des fichiers journaux internes qui décrivent la progression de l'exécution du script. Le script copie un journal `Kickoff_VDA_Startup_Script` sur le partage de journal central quelques secondes après le démarrage du déploiement sur la machine. Vous pouvez vérifier que le processus fonctionne. Si ce journal n'est pas copié dans le partage de journaux central comme prévu, corrigez le problème en inspectant la machine locale. Le script place deux fichiers journaux de débogage dans le dossier `%temp%` sur chaque machine :
  - `Kickoff_VDA_Startup_Script_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.log`

  Vérifiez ces journaux pour vous assurer que le script :
  - S'exécute comme prévu.
  - Détecte correctement le système d'exploitation cible.

  - Est correctement configuré pour pointer vers la racine `ROOT` du partage `DEPLOYSHARE` (contient le fichier appelé `AutoSelect.exe`).
  - Est capable de s'authentifier auprès des partages `DEPLOYSHARE` et `LOG`.

- Pour plus d'informations sur la façon dont Citrix présente le résultat de l'installation des composants, veuillez consulter la section Codes de retour de l'installation de Citrix.
- Dans l'écran Studio d'un groupe de mise à disposition, l'entrée **Version de VDA installée** dans le panneau **Détails** peut ne pas être la version installée sur les machines. Les programmes et fonctionnalités de la machine affichent la version actuelle du VDA.
- Une fois qu'un VDA est installé, il ne peut pas fournir d'applications ou de bureau aux utilisateurs tant qu'il n'est pas enregistré auprès d'un Delivery Controller.

  Pour en savoir plus sur les méthodes d'enregistrement du VDA et la résolution des problèmes d'enregistrement, consultez la section Enregistrement de VDA.

Installer des VDA à l'aide de SCCM

June 28, 2024

> **Remarque :**
>
> Citrix n'est pas responsable des problèmes liés au déploiement d'un Virtual Delivery Agent (VDA) à l'aide d'outils de distribution de logiciels tels que Microsoft System Center Configuration Manager (SCCM) qui ont été adaptés pour répondre aux exigences des environnements de production des clients. Pour tout problème lié à l'installation de Citrix, ouvrez un dossier de support technique et ajoutez-y les journaux d'installation correspondants à l'aide du portail de support Citrix.

Vue d'ensemble

Pour déployer correctement un Virtual Delivery Agent (VDA) à l'aide de Microsoft System Center Configuration Manager (SCCM) ou d'outils de distribution de logiciels similaires, Citrix recommande d'utiliser le programme d'installation du VDA en plusieurs étapes.

Citrix ne recommande pas d'utiliser l'utilitaire de nettoyage de VDA dans le cadre d'une installation ou d'une mise à niveau de VDA. Utilisez l'utilitaire de nettoyage de VDA uniquement dans le cas où le programme d'installation du VDA a échoué précédemment.

Redémarrages

Le nombre requis de redémarrages lors de l'installation du VDA dépend de l'environnement. Par exemple :

- Un redémarrage peut être nécessaire pour les mises à jour en attente ou les redémarrages à partir d'installations logicielles antérieures.
- Les fichiers précédemment verrouillés par d'autres processus peuvent nécessiter des mises à jour, ce qui entraîne un redémarrage supplémentaire.
- Certains composants facultatifs du programme d'installation du VDA (tels que le Citrix Profile Management ou Citrix Files) peuvent nécessiter un redémarrage.

Le séquenceur de tâches SCCM gère tous les redémarrages nécessaires.

Définir la séquence de tâches

Après avoir identifié tous les prérequis et procédé au redémarrage, utilisez le séquenceur de tâches SCCM pour effectuer les opérations suivantes :

- Le VDA peut être installé à partir d'une copie accessible du support d'installation ou de l'un des programmes d'installation autonomes de VDA :
  - `VDAWorkstationSetup_XXXX.exe`
  - `VDAServerSetup_XXXX.exe`
  - `VDAWorkstationCoreSetup_XXXX.exe`

  Pour plus d'informations sur les programmes d'installation de VDA, consultez la section Programmes d'installation.
- Lors de la mise à niveau d'un VDA, la machine sur laquelle il est installé doit être en mode de maintenance, sans session.
- Lorsqu'une installation de VDA est exécutée pour la première fois sur une machine, le programme d'installation de VDA utilisé est copié sur cette machine.
  - Lorsque vous utilisez un programme d'installation de VDA autre que `VDAWorkstationCoreSetup_.exe`, le programme d'installation de VDA est copié dans `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`.
  - Lors de l'utilisation de `VDAWorkstationCoreSetup_XXXX.exe`, le programme d'installation de VDA est copié dans `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe`.

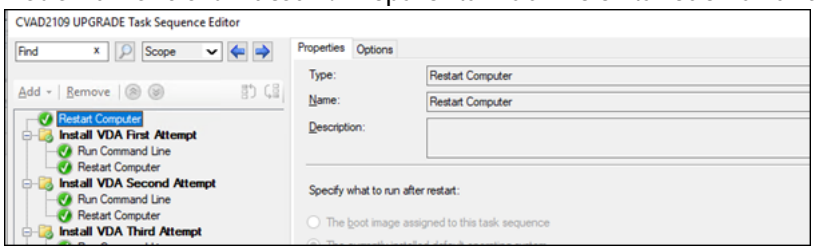
‘

- L'emplacement du répertoire du programme d'installation de VDA est également stocké dans le Registre : "HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall" "MetaInstallerInstallLocation".
- Ajoutez les options de ligne de commande /NOREBOOT, /NORESUME et /QUIET à vos options de ligne de commande.
  - /QUIET : ne pas afficher l'interface utilisateur pendant l'installation, afin que SCCM ait le contrôle du processus d'installation.
  - /NOREBOOT : ne pas redémarrer automatiquement le programme d'installation de VDA. Les déclencheurs SCCM redémarrent en cas de besoin.
  - /NORESUME : en général, lorsqu'un redémarrage est nécessaire pendant l'installation, le programme d'installation de VDA définit une clé de registre runonce (\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce). Lorsque la machine redémarre, Windows utilise la clé pour lancer le programme d'installation de VDA. Cela représente un problème pour SCCM, car SCCM ne peut pas surveiller l'installation et capturer le code de sortie.

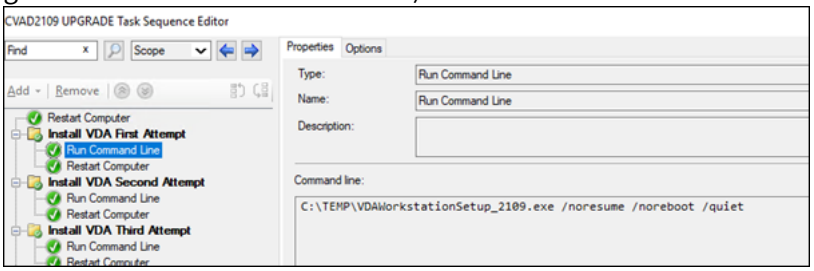
Exemple de séquence d'installation utilisant SCCM

L'exemple suivant illustre la séquence d'installation.

1. **Redémarrer l'ordinateur :** Préparez la machine en la redémarrant.

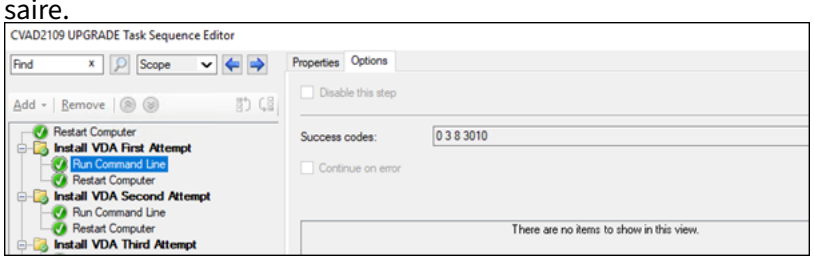


2. **Première tentative d'installation du VDA :**démarrez l'installation du VDA.
   a) Ajoutez les options /quiet, /noreboot et /noresume à vos options de ligne de commande.
   b) Exécutez le programme d'installation de VDA de votre choix (image locale ou l'un des programmes d'installation minimaux).

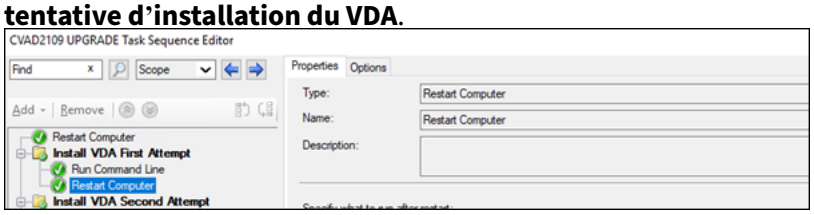


   c) SCCM doit saisir le code de retour.

- Si le code de retour est 0 ou 8, l'installation est terminée et un redémarrage est nécessaire.

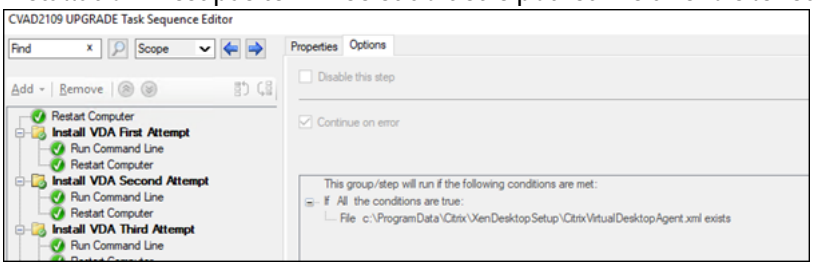


- Si le code de retour est 3, redémarrez la machine, puis passez le contrôle à **Deuxième tentative d'installation du VDA**.



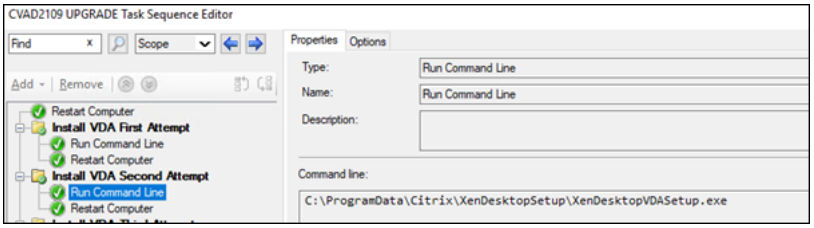
3. **Deuxième tentative d'installation du VDA :** Poursuivez l'installation du VDA.

   a) Après la **Première tentative d'installation du VDA**, si le fichier `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` existe, l'installation n'est pas terminée et doit être poursuivie une fois le redémarrage terminé.



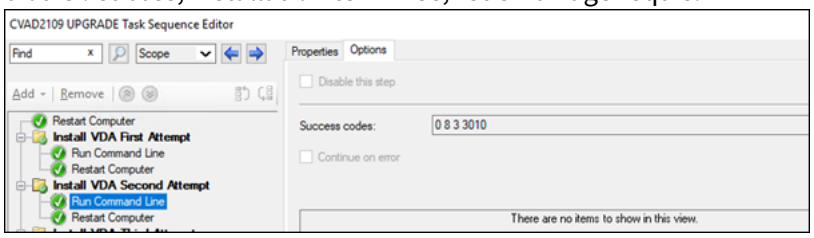
   b) La **Deuxième tentative d'installation du VDA** se répète jusqu'à ce que le fichier `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` n'existe plus ou qu'un code de retour différent de 0 ou 8 soit renvoyé. Traitez tout autre code de retour comme une erreur. DEUXIÈME TENTATIVE D'INSTALLATION DU VDA devrait signaler une erreur et s'arrêter.

   c) Reprenez l'installation du VDA en exécutant le programme d'installation du VDA approprié (`XenDesktopVdaSetup.exe` dans la plupart des cas, ou `XenDesktopRemotePCSetup.exe` si `VDAWorkstationCoreSetup_XXXX.exe` a été utilisé) à partir du répertoire de fichier `%programdata%\Citrix\XenDesktopSetup\` sans aucun paramètre de ligne de commande. (Le programme d'installation du VDA utilise les paramètres qu'il a enregistrés lors de la première exécution du programme d'installation.)



d) Surveiller le code de retour du programme d'installation de VDA.

- 0 ou 8 : succès, installation terminée, redémarrage requis.



- 3 : l'installation n'est pas terminée. Redémarrez la machine et répétez DEUXIÈME TENTATIVE D'INSTALLATION DU VDA jusqu'à ce que le fichier `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` n'existe plus ou que la valeur 0 ou 8 soit renvoyée. Traitez tout autre code de retour comme une erreur. DEUXIÈME TENTATIVE D'INSTALLATION DU VDA devrait signaler une erreur et se terminer.

Pour plus d'informations sur les codes de retour, consultez la section Codes de retour d'installation Citrix.

Exemples de commande d'installation de VDA

Les options d'installation disponibles varient en fonction du programme d'installation utilisé. Consultez les articles suivants pour plus de détails sur les options de ligne de commande.

- Installer des VDA
- Installer à l'aide de la ligne de commande

Commandes d'installation pour Remote PC Access

- La commande suivante utilise le programme d'installation de VDA mono-session principal (`VDAWorkstationCoreSetup.exe`) :

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "control.domain.com" /enable_hdx_ports /noresume /noreboot
  ```

- La commande suivante utilise le programme d'installation de VDA mono-session complet (`VDAWorkstationSetup.exe`) :


```
VDAWorkstationSetup.exe /quiet /remotepc /physicalmachine /
controllers “control.domain.com” /enable_hdx_ports /noresume /
noreboot
```

Commande d’installation pour VDI dédié

- La commande suivante utilise le programme d’installation de VDA mono-session complet (`VDAWorkstationSetup.exe`) :

  ```
  VDAWorkstationSetup.exe /quiet /components vda /controllers “
  control.domain.com” /enable_hdx_ports /enable_remote_assistance /
  noresume /noreboot
  ```

Créer un site

June 27, 2024

> **Remarque :**
>
> Lors de la création du site, après avoir ajouté une licence pour activer la licence de droits hybrides, les hôtes de cloud public (tels que Microsoft Azure, Google Cloud Platform et Amazon Web Services) n’apparaissent pas dans la liste des types de connexion tant que la création du site n’est pas terminée.

Un site est le nom que vous donnez à un déploiement Citrix Virtual Apps and Desktops. Il comprend les Delivery Controller et autres composants principaux, les VDA, les connexions aux hôtes, les catalogues de machines et les groupes de mise à disposition. Vous créez le site après avoir installé les composants et avant la création du premier catalogue de machines et groupe de mise à disposition.

Si votre Controller est installé sur Server Core, utilisez les applets de commande PowerShell dans le SDK Citrix Virtual Apps and Desktops pour créer un site.

Lorsque vous créez un site, vous êtes automatiquement inscrit au Programme d’amélioration de l’expérience utilisateur Citrix (CEIP). CEIP recueille des informations d’utilisation et des statistiques anonymes, puis les envoie à Citrix. Le premier package de données est envoyé à Citrix approximativement sept jours après la création du site. Vous pouvez modifier votre inscription à tout moment après la création du site. Sélectionnez **Paramètres** dans le volet gauche de Web Studio, puis recherchez le paramètre **Programme d’amélioration de l’expérience cliente Citrix** . Pour plus de détails, consultez http://more.citrix.com/XD-CEIP.

L’utilisateur qui crée un site en devient l’administrateur complet. Pour plus d’informations, consultez Administration déléguée.

Consultez cet article avant de créer le site pour savoir ce qui vous attend.

Étape 1. Ouvrir l'assistant de création de site pour Citrix Site Manager

Pour configurer votre déploiement Citrix Virtual Apps and Desktops (également appelé site), utilisez l'outil Citrix Site Manager. L'outil est installé automatiquement lorsque vous installez un Delivery Controller.

Pour exécuter cet outil, ouvrez le menu Démarrer du bureau sur un Delivery Controller et sélectionnez **Citrix > Citrix Site Manager**. Reportez-vous à la section Installer Web Studio.

Étape 2. Site name

Sur la page **Introduction**, tapez le nom du site.

Étape 3. Base de données

La page **Bases de données** contient des sélections permettant de configurer les bases de données Site, Surveillance et Journalisation de la configuration. Pour de plus amples informations sur les choix et les exigences de configuration de base de données, consultez la section Bases de données.

> **Remarque :**
>
> Si un écouteur SQL Server Always On est configuré pour le chiffrement TLS, vous pouvez être invité à entrer des informations d'identification avec des autorisations de création de base de données. Les tentatives de création de la base de données échouent même si vous entrez des informations d'identification d'administrateur valides. Vérifiez que le certificat SQL Server inclut le nom DNS du processus d'écoute dans les SAN (Subject Alternative Names). Pour plus d'informations, consultez https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates.

Si vous choisissez d'installer le logiciel SQL Server Express en tant que base de données du site (paramètre par défaut), un redémarrage se produit après l'installation du logiciel. Ce redémarrage ne se produit pas si vous choisissez de ne pas installer le logiciel SQL Server Express en tant que base de données du site.

Si vous n'utilisez pas la valeur par défaut SQL Server Express, assurez-vous que le logiciel SQL Server est installé sur les machines avant de créer un site. La section Configuration système requise répertorie les versions prises en charge.

Si vous souhaitez ajouter plusieurs Delivery Controller au site, et que vous avez déjà installé le logiciel du Controller sur d'autres serveurs, vous pouvez ajouter ces Controller au site à partir de cette page.

Si vous souhaitez aussi générer des scripts qui configurent les bases de données, ajoutez les Controller avant de générer les scripts.

Étape 4. Gestion des licences

Sur la page **Licences**, spécifiez l'adresse du serveur de licences, puis indiquez la licence à utiliser (installer).

- Indiquez l'adresse du serveur de licences au format `name:[port]`. Le *nom* doit être un nom de domaine complet, NetBIOS ou une adresse IP. Un nom de domaine complet est recommandé. Si vous omettez le numéro de port, la valeur par défaut est 27000. Cliquez sur **Connect**. Vous ne pouvez pas passer à la page suivante tant qu'une connexion n'a pas été établie avec le serveur de licences.
- Lorsqu'une connexion est établie, l'option **Utiliser une licence existante** est sélectionnée par défaut. L'affichage répertorie les produits compatibles avec lesquels ce produit peut être configuré, en fonction des licences actuellement installées.
  - Si vous souhaitez configurer ce produit comme l'un des produits répertoriés (par exemple, Citrix Virtual Apps Premium ou Citrix Virtual Desktops Premium), sélectionnez cette entrée à l'aide de l'une de ces licences.
  - Si vous avez déjà alloué et téléchargé une licence (à l'aide de l'outil Citrix Manage Licenses) à utiliser avec ce produit, mais que vous n'avez pas encore installé la licence :
    - Cliquez sur **Rechercher un fichier de licences**.
    - Dans l'explorateur de fichiers, recherchez et sélectionnez la licence que vous avez téléchargée. Les produits associés apparaissent désormais sur la page **Licences** de l'assistant de création de site. Sélectionnez l'entrée que vous souhaitez utiliser.
  - Si le produit souhaité n'est pas affiché, ou si vous n'avez pas de licences allouées et téléchargées, vous pouvez allouer, télécharger et installer une licence. Pour ce faire, le serveur de licences doit disposer d'un accès Internet. Vous devez disposer d'un code d'accès aux licences pour le produit que vous souhaitez. Citrix vous envoie ce code par e-mail.
    - Cliquez sur **Allouer et télécharger**.
    - Dans la boîte de dialogue **Allouer des licences**, entrez le code d'accès aux licences envoyé par Citrix. Cliquez sur **Allouer des licences**.
    - Les produits associés à la nouvelle licence apparaissent sur la page **Licences** de l'assistant de création de site. Sélectionnez l'entrée que vous souhaitez utiliser.

  Vous pouvez également sélectionner **Utiliser l'évaluation gratuite de 30 jours** et installer les licences ultérieurement. Consultez la documentation relative au système de licences pour plus d'informations.

Étape 5. Résumé

La page **Résumé** répertorie les informations que vous avez spécifiées. Utilisez le bouton **Précédent** si vous souhaitez modifier quoi que ce soit. Lorsque vous avez terminé, cliquez sur **Terminer**.

Informations supplémentaires

Connexion hôte, réseau et stockage

Si vous utilisez des machines virtuelles sur un hyperviseur ou autre service pour fournir des bureaux et des applications, vous pouvez éventuellement créer la première connexion à cet hôte. Vous pouvez également spécifier des ressources réseau et de stockage pour cette connexion. Après avoir créé le site, vous pouvez modifier cette connexion et les ressources et créer davantage de connexions. Pour de plus amples informations, veuillez consulter la section Connexions et ressources.

- Pour plus d'informations sur la page **Connexion**, voir Connexions et ressources.
  - Si vous n'utilisez pas de VM sur un hyperviseur ou un autre service (ou si vous utilisez Web Studio pour gérer les bureaux sur des PC lames dédiés), sélectionnez le type de connexion **Aucun**.
  - Si vous configurez un site Remote PC Access et prévoyez d'utiliser la fonctionnalité Wake on LAN, sélectionnez le type **Microsoft System Center Virtual Machine Manager** ou **Wake on LAN de Remote PC**. Pour plus d'informations, consultez Wake on LAN.

  Outre le type de connexion, spécifiez également si vous allez utiliser les outils Citrix (tels que Machine Creation Services) ou d'autres outils pour créer des VM.
- Pour plus d'informations sur les pages **Stockage** et **Réseau**, voir Stockage hôte, Gestion du stockage et Sélection du stockage.
- Si vous avez une licence de droits hybrides et que vous avez ajouté des connexions hôtes de cloud public (par exemple, AWS), ces connexions sont répertoriées ici. Pour afficher ces connexions hôtes de cloud public, actualisez Web Studio quelques minutes après les avoir ajoutées.

Remote PC Access

Pour de plus amples informations sur les déploiements Remote PC Access, consultez la section Remote PC Access.

Si vous utilisez la fonctionnalité Wake on LAN, suivez les étapes de configuration sur la console Microsoft System Center Configuration Manager avant de créer le site. Pour plus de détails, consultez la section Configuration Manager et Remote PC Access Wake on LAN.

Créer et gérer des connexions et des ressources

June 27, 2024

> **Important :**
>
> Depuis Citrix Virtual Apps and Desktops 7 2006, si votre déploiement actuel utilise l'une des technologies suivantes, vous pouvez mettre à niveau votre déploiement vers la version actuelle uniquement après avoir supprimé les éléments en fin de vie qui utilisent ces technologies.
>
> - Personal vDisk (PvD)
> - AppDisks
> - Types d'hôtes de cloud public : Citrix CloudPlatform, Microsoft Azure Classic
>
> Pour de plus amples informations, consultez la section Suppression de PvD, AppDisks et d'hôtes non pris en charge.
>
> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Si vous souhaitez utiliser des connexions hôtes de cloud public pour votre déploiement, vous avez besoin d'une licence de droits hybrides pour effectuer votre nouvelle installation ou mettre à niveau vers la version actuelle.

Lorsque le programme d'installation détecte une ou plusieurs technologies ou connexions hôtes non prises en charge sans licence de droits hybrides, la mise à niveau est suspendue ou s'arrête et un message explicatif s'affiche. Les journaux du programme d'installation contiennent des détails. Pour plus d'informations, veuillez consulter la section Mettre un déploiement à niveau.

Effet de la licence Hybrid Rights sur la connexion hôte

Il existe trois scénarios dans lesquels la connexion hôte aux hôtes de cloud public est affectée par la licence de droits hybrides :

- Pour créer une connexion hôte aux hôtes de cloud public, vous devez disposer d'une licence de droits hybrides.
- Si vous avez une licence de droits hybrides mais que la licence a expiré, les connexions existantes aux hôtes de cloud public sont marquées comme non autorisées et passent en mode de

maintenance. Lorsque les connexions hôtes existantes sont en mode de maintenance, vous ne pouvez pas effectuer les opérations suivantes :

  - Ajouter ou modifier des connexions hôtes
  - Créer un catalogue et mettre à jour une image
  - Effectuer des actions d'alimentation

- Lorsque des connexions hôtes non autorisées deviennent autorisées, les connexions d'hébergement existantes sont réactivées.

Introduction

Vous pouvez éventuellement créer votre première connexion pour héberger des ressources lorsque vous créez un site. Plus tard, vous pouvez modifier cette connexion et en créer de nouvelles. La configuration d'une connexion implique de sélectionner le type de connexion parmi les hyperviseurs pris en charge, ainsi que le stockage et le réseau sélectionnés parmi les ressources de cette connexion.

Les administrateurs en lecture seule peuvent afficher les détails de la connexion et des ressources. Vous devez être un administrateur complet pour effectuer les tâches de connexion et de gestion des ressources. Pour de plus amples informations, veuillez consulter la section Administration déléguée.

Où trouver des informations sur les types de connexion

Vous pouvez utiliser les plates-formes de virtualisation prises en charge pour héberger et gérer des machines dans votre environnement Citrix Virtual Apps ou Citrix Virtual Desktops. L'article Configuration système requise répertorie les types pris en charge.

Pour de plus amples informations, consultez les sources d'informations suivantes :

- **XenServer (anciennement Citrix Hypervisor) :**
  - Environnements de virtualisation XenServer.
  - documentation XenServer.
- **Nutanix Acropolis :**
  - Environnements de virtualisation Nutanix.
  - Documentation Nutanix.
- **VMware :**
  - Environnements de virtualisation VMware.
  - Documentation du produit VMware.

- **Microsoft Hyper-V :**
  - Article Environnements de virtualisation Microsoft System Center Virtual Machine Manager.
  - Documentation Microsoft.
- **Connexions hôtes au cloud public (AWS, Google Cloud, Microsoft Azure, solutions cloud et partenaires Nutanix, et solutions cloud et partenaires VMware) :** pour plus d'informations sur les hôtes de cloud public, voir Configurer le type de ressource.

> **Remarque :**
>
> Les sources d'informations vous dirigent vers la documentation Citrix DaaS. Si vous connaissez les hôtes de cloud public du produit Citrix DaaS, veuillez noter que la version sur site présente plusieurs différences. Dans Citrix Virtual Apps and Desktops sur site, l'interface de gestion est appelée Web Studio. Les mises à jour sont déployées sur le service environ toutes les quatre semaines. Par conséquent, vous pourrez constater que certaines fonctionnalités disponibles avec le service ne sont pas disponibles avec la version sur site.

Stockage hôte

Un produit de stockage est pris en charge lorsqu'il est géré par un hyperviseur pris en charge. Le support Citrix aide les fournisseurs de produits de stockage à résoudre les problèmes, et à documenter ces problèmes dans le centre de connaissances, si nécessaire.

Lors du provisioning de machines, les données sont classées par type :

- Données du système d'exploitation, ce qui comprend les images principales.
- Données temporaires. Ces données comprennent toutes les données non persistantes écrites sur les machines provisionnées avec MCS, les fichiers de pages Windows, les données du profil utilisateur et les données qui sont synchronisées avec ShareFile. Ces données sont supprimées chaque fois qu'une machine redémarre.

La mise à disposition d'espaces de stockage distincts pour chaque type de données peut réduire la charge et améliorer les performances sur chaque périphérique de stockage, ce qui permet d'utiliser les ressources disponibles de l'hôte de manière optimale. Cela permet également d'utiliser un stockage approprié pour les différents types de données : la persistance et la résilience sont des facteurs plus importants pour certaines données que pour d'autres.

Le stockage peut être partagé (centralisé, séparé de l'hôte, utilisé par tous les hôtes) ou local sur un hyperviseur. Par exemple, un stockage partagé central peut être un ou plusieurs volumes de stockage en cluster Windows Server 2012 (avec ou sans stockage attaché), ou l'appliance d'un fournisseur de stockage. Le stockage central peut également fournir ses propres optimisations telles que des

chemins de contrôle de stockage de l'hyperviseur et un accès direct au travers de plug-ins de partenaires.

Le stockage des données temporaires localement évite d'avoir à traverser le réseau pour accéder à un espace de partagé. Cela permet également de réduire la charge sur le périphérique de stockage partagé. Le stockage partagé peut être plus coûteux, par conséquent le stockage des données localement peut réduire les dépenses. Ces avantages doivent être pondérés par rapport à la disponibilité d'un stockage suffisant sur les serveurs hyperviseur.

Lorsque vous créez une connexion, vous devez choisir l'une des deux méthodes de gestion du stockage : stockage partagé par les hyperviseurs, ou stockage local sur l'hyperviseur.

Lorsque vous utilisez le stockage local sur un ou plusieurs hôtes XenServer pour le stockage des données temporaires, assurez-vous que chaque emplacement de stockage du pool a un nom unique. (Pour modifier un nom dans XenCenter, cliquez avec le bouton droit sur le stockage et modifiez le nom de la propriété.)

Stockage partagé par les hyperviseurs

La méthode de stockage partagé par les hyperviseurs stocke centralement les données qui doivent être archivées à long terme, ce qui offre une gestion et une sauvegarde centralisées. Ce stockage contient les disques du système d'exploitation.

Lorsque vous sélectionnez cette méthode, vous pouvez choisir d'utiliser le stockage local (sur les serveurs dans le même pool d'hyperviseurs) pour les données temporaires. Cette méthode ne nécessite pas de persistance ni autant de résilience que les données du stockage partagé, appelé *cache de données temporaires*. Le disque local permet de réduire le trafic vers le stockage du système d'exploitation principal. Ce disque est effacé après chaque redémarrage de machine. Le disque est accessible via un cache mémoire en écriture continue. Si vous utilisez le stockage local pour les données temporaires, le VDA provisionné est associé à un hyperviseur hôte spécifique. Si cet hôte échoue, la machine virtuelle ne peut pas démarrer.

Exception : Microsoft System Center Virtual Machine Manager n'autorise pas les disques de mise en cache des données temporaires sur le stockage local si vous utilisez des volumes de stockage en cluster (CSV).

Créez une connexion pour stocker des données temporaires localement, puis activez et configurez des valeurs autres que les valeurs par défaut pour la taille de disque et de mémoire pour chaque machine virtuelle. Les valeurs par défaut sont adaptées au type de connexion, et sont suffisantes pour la plupart des cas. Pour de plus amples informations, consultez la section Créer des catalogues de machines.

L'hyperviseur peut également fournir des technologies d'optimisation par le biais d'une mise en cache de lecture locale des images de disque. Par exemple, XenServer propose IntelliCache, qui réduit

le trafic réseau vers le stockage central.

Stockage local sur l'hyperviseur

La méthode de stockage local sur l'hyperviseur stocke les données localement sur l'hyperviseur. Avec cette méthode, les images principales et d'autres données du système d'exploitation sont transférées vers les hyperviseurs du site. Ce processus se produit pour la création initiale de la machine et les futures mises à jour de l'image. Il se traduit par un trafic important sur le réseau de gestion. Les transferts d'images sont également chronophages, et les images deviennent disponibles auprès de chaque hôte à un moment différent.

Créer une connexion et des ressources

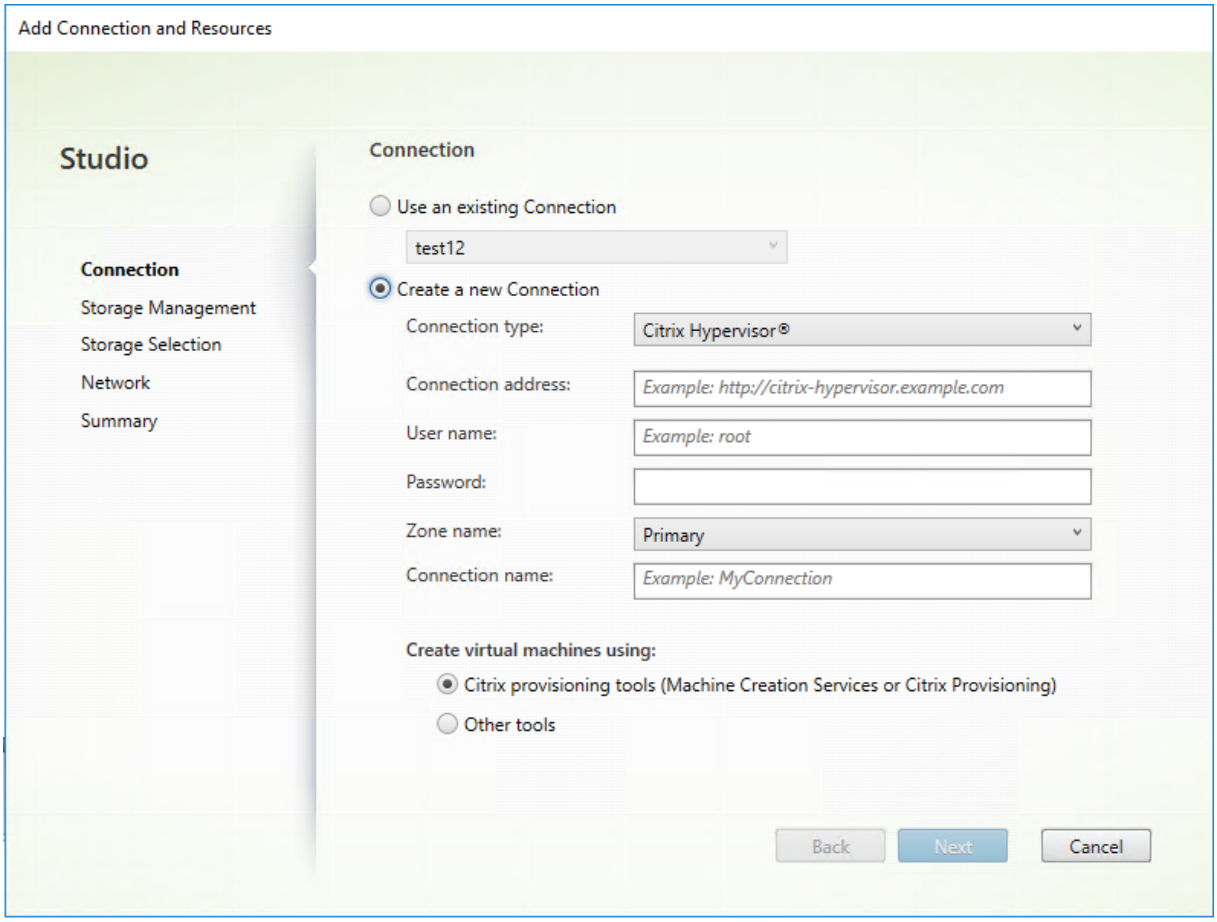
Vous pouvez éventuellement créer la première connexion lorsque vous créez le site. L'assistant de création de site contient les pages liées à la connexion décrites dans les sections suivantes.

Si vous créez une connexion après la création du site, commencez à l'étape 1.

> **Important :**
>
> Les ressources hôte (stockage et réseau) doivent être disponibles avant de créer une connexion.

1. Connectez-vous à Web Studio.
2. Sélectionnez **Hébergement** dans le volet de gauche.
3. Sélectionnez **Ajouter une connexion et des ressources** dans le volet Actions.
4. L'assistant vous guide à travers les pages suivantes (le contenu des pages dépend du type de connexion sélectionné). Après avoir complété chaque page, cliquez sur **Suivant** jusqu'à la page **Résumé**.

Connexion



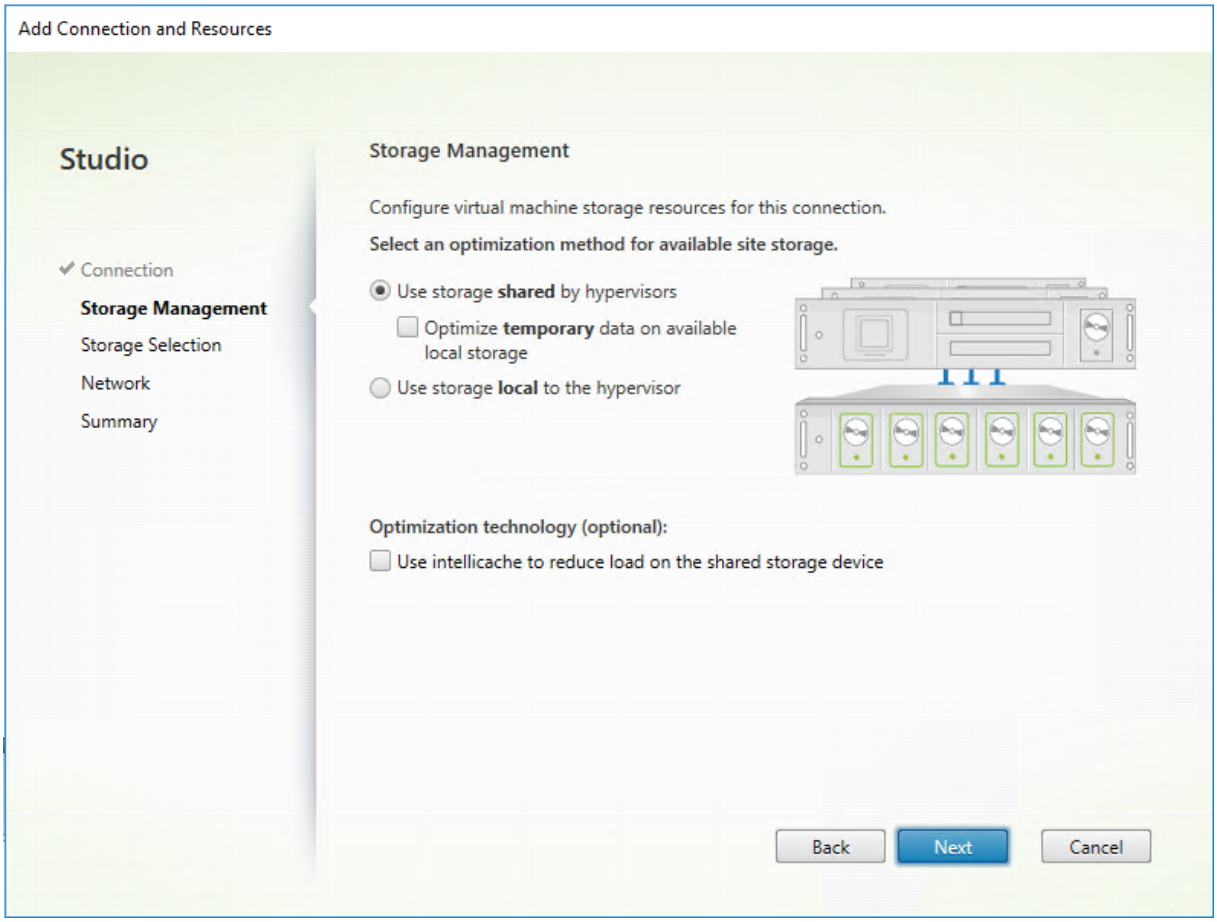
Sur la page **Connexion** :

- Pour créer une connexion, sélectionnez **Créer une nouvelle connexion**. Pour créer une connexion basée sur la même configuration d'hôte qu'une connexion existante, sélectionnez **Utiliser une connexion existante**, puis choisissez la connexion appropriée
- Sélectionnez l'hyperviseur que vous utilisez dans le champ **Type de connexion**. Les connexions hôtes de cloud public sont répertoriées dans la liste déroulante uniquement si vous utilisez la licence de droits hybrides. Vous pouvez également utiliser la commande PowerShell `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true pour obtenir les informations suivantes :
  - Liste de tous les plug-ins d'hyperviseur pris en charge par Citrix, y compris les plug-ins tiers
  - Disponibilité du plug-in d'hyperviseur. Si l'état de disponibilité est **false**, cela peut être dû au fait que le plug-in de l'hyperviseur n'est pas installé correctement ou que vous ne disposez pas des droits liés à la licence de droits hybrides.
- Les champs relatifs à l'adresse de connexion et aux informations d'identification diffèrent en

fonction du type de connexion sélectionné. Entrez les informations requises.

- Entrez un nom pour la connexion. Ce nom apparaît dans Web Studio.
- Choisissez l'outil que vous utilisez pour créer des machines virtuelles : les outils Web Studio (Machine Creation Services ou Citrix Provisioning) ou d'autres outils.

Gestion du stockage



Pour de plus amples informations sur les types et méthodes de gestion du stockage, consultez la section Stockage hôte.

Si vous configurez une connexion à un hôte Hyper-V ou VMware, sélectionnez un nom de cluster. D'autres types de connexion ne nécessitent pas de nom de cluster.

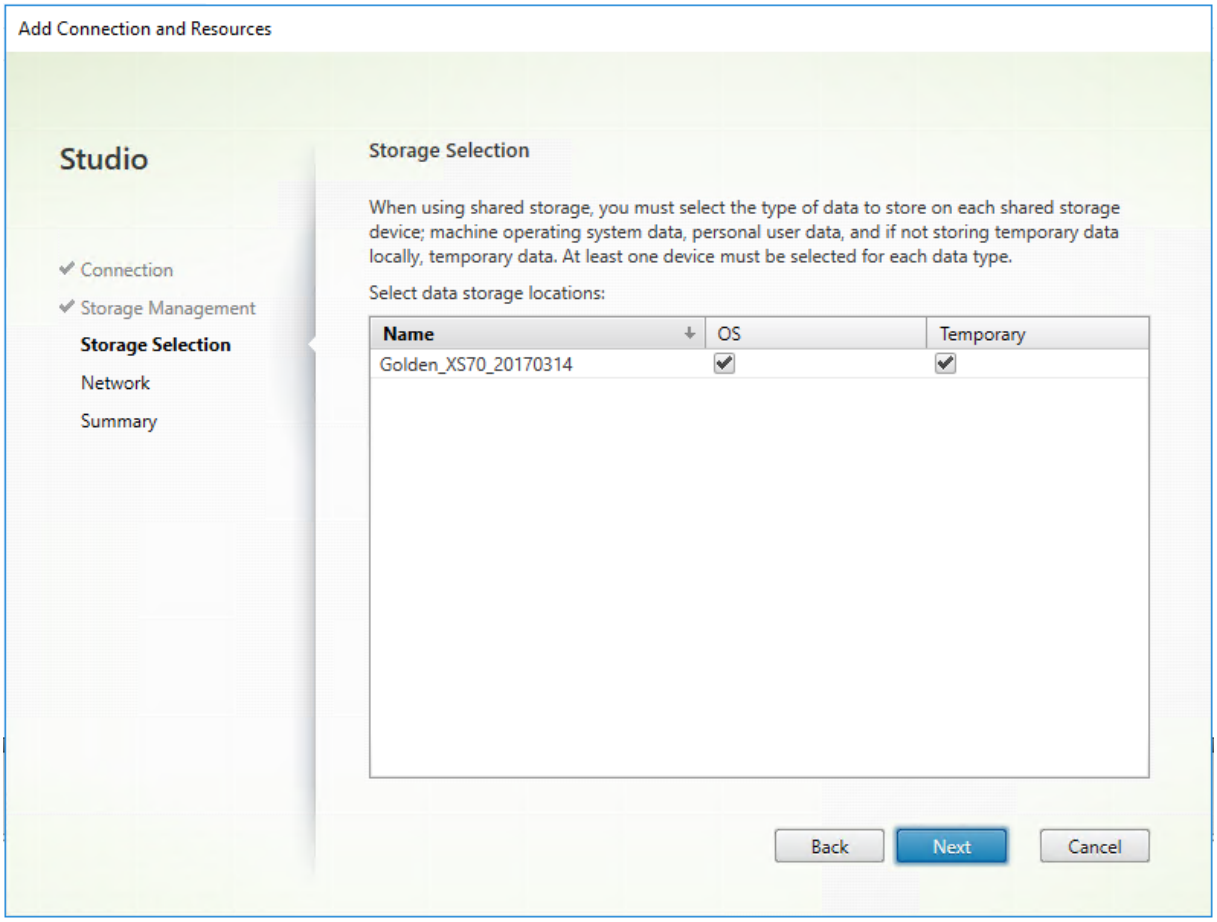
Sélectionnez une méthode de gestion du stockage : stockage partagé par les hyperviseurs ou stockage local sur l'hyperviseur.

- Si vous choisissez le stockage partagé par les hyperviseurs, indiquez si vous souhaitez conserver les données temporaires sur l'espace de stockage local disponible. (Vous pouvez spécifier des tailles de stockage temporaire autres que les valeurs par défaut dans les catalogues de machines qui utilisent cette connexion.) **Exception :** lors de l'utilisation de volumes de stockage

en cluster (CSV), Microsoft System Center Virtual Machine Manager n'autorise pas les disques de mise en cache des données temporaires sur le stockage local. La configuration de la gestion du stockage dans Web Studio échoue.

Si vous utilisez un espace de stockage partagé sur un pool XenServer, indiquez si vous souhaitez utiliser IntelliCache pour réduire la charge sur le périphérique de stockage partagé. Consultez la section Utiliser les connexions IntelliCache pour XenServer.

Sélection du stockage



Pour de plus amples informations sur la sélection du stockage, consultez la section Stockage hôte.

Sélectionnez au moins un périphérique de stockage hôte pour chaque type de données disponible. La méthode de gestion du stockage que vous avez sélectionnée sur la page précédente affecte les types de données disponibles sur cette page. Sélectionnez au moins un périphérique de stockage pour chaque type de données pris en charge avant de pouvoir passer à la page suivante de l'assistant.

La partie inférieure de la page **Sélection du stockage** contient d'autres options de configuration si vous avez choisi le stockage partagé par les hyperviseurs et activé **Optimiser les données tempo-**

raires sur le stockage local disponible sur la page précédente. Vous pouvez sélectionner les périphériques de stockage locaux à utiliser pour les données temporaires.

Le nombre de périphériques de stockage actuellement sélectionnés est affiché (dans le diagramme précédent, « 1 périphérique de stockage sélectionné »). Lorsque vous placez le curseur sur cette entrée, les noms des périphériques sélectionnés s'affichent.

1. Cliquez sur **Sélectionner** pour modifier les périphériques de stockage à utiliser.
2. Dans la boîte de dialogue **Sélectionner un stockage**, activez ou désactivez les cases de périphérique de stockage, puis cliquez sur **OK**.

Réseau

Sur la page **Réseau**, entrez un nom pour les ressources. Ce nom apparaît dans Web Studio pour identifier la combinaison stockage et réseau associée à la connexion.

Sélectionnez un ou plusieurs réseaux que les machines virtuelles utilisent.

Résumé

Sur la page **Résumé**, passez en revue vos sélections. Lorsque vous avez terminé, cliquez sur **Terminer**.

Rappel : le stockage des données temporaires localement permet de configurer des valeurs autres que les valeurs par défaut pour le stockage des données temporaires lorsque vous créez le catalogue de machines contenant les machines utilisant cette connexion. Voir Créer des catalogues de machines.

Modifier les paramètres de connexion

N'utilisez pas cette procédure pour renommer une connexion ou pour créer une connexion. Ces connexions sont des opérations différentes. Modifiez l'adresse uniquement si la machine hôte actuelle possède une nouvelle adresse. La saisie d'une adresse d'une autre machine rompt les catalogues de machines de la connexion.

Vous ne pouvez pas modifier les paramètres **GPU** d'une connexion, car les catalogues de machines qui accèdent à cette ressource doivent utiliser une image principale appropriée spécifique au GPU. Créez une connexion.

1. Connectez-vous à Web Studio.
2. Sélectionnez **Hébergement** dans le volet de gauche.
3. Sélectionnez la connexion, puis sélectionnez **Modifier la connexion** dans le volet Actions.

4. Vous trouverez les paramètres disponibles lorsque vous modifiez une connexion.
5. Lorsque vous avez terminé, cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

Page **Propriétés de la connexion** :

- Pour modifier l'adresse et les informations d'identification de connexion, sélectionnez **Modifier les paramètres…** et entrez de nouvelles informations.
- Pour spécifier les serveurs haute disponibilité pour une connexion XenServer, sélectionnez **Modifier les serveurs…** et sélectionnez les serveurs. Citrix vous recommande de sélectionner tous les serveurs du pool pour permettre la communication avec XenServer au cas où le pool principal échoue.

  > **Remarque :**
  >
  > Si vous utilisez le protocole HTTPS et souhaitez configurer des serveurs à haute disponibilité, n'installez pas de certificat générique pour tous les serveurs d'un pool. Un certificat individuel est requis pour chaque serveur.

Page **Avancé** :

- Pour un type de connexion Microsoft System Center Configuration Manager (ConfMgr) Wake on LAN, qui est utilisé avec Remote PC Access, entrez les informations **ConfMgr Wake Proxy**, des paquets magiques et des transmissions de paquets.
- Les paramètres de seuil de limitation vous permettent de spécifier un nombre maximal d'actions d'alimentation autorisées sur une connexion. Ces paramètres peuvent aider lorsque les paramètres de gestion de l'alimentation autorisent trop ou trop peu de machines à démarrer en même temps. Chaque type de connexion dispose de valeurs par défaut qui sont appropriées à la plupart des cas et ne doivent pas être modifiées.
- Le paramètre **Actions simultanées (tous types)** définit deux valeurs : le nombre maximal absolu pouvant se produire simultanément sur cette connexion, et un pourcentage maximal de toutes les machines utilisant cette connexion. Vous devez spécifier à la fois des valeurs absolues et des valeurs de pourcentage. La limite réelle appliquée est la valeur la plus basse.

  Par exemple, dans un déploiement de 34 machines, si **Actions simultanées (tous types)** sont définies sur une valeur absolue de 10 et une valeur de pourcentage de 10, la limite réelle appliquée est de 3 (10 pour cent de 34 arrondis au nombre entier le plus proche, qui est inférieure à la valeur absolue de 10 machines).
- Le **nombre maximal de nouvelles actions par minute** est un nombre absolu. Il n'existe pas de valeur de pourcentage.

- Entrez les informations dans le champ **Options de connexion** uniquement selon les directives d'un représentant de l'assistance Citrix ou les instructions explicites de la documentation.

Page **Locataires partagés** :

cette page vous permet d'ajouter des locataires et des abonnements qui partagent Azure Compute Gallery avec l'abonnement de la connexion. Par conséquent, lors de la création ou de la mise à jour de catalogues, vous pouvez sélectionner des images partagées provenant de ces locataires et de ces abonnements.

- Renseignez les champs **ID d'application** et **Secret d'application** pour l'application associée à cette connexion. Avec ces informations, vous pouvez vous authentifier auprès d'Azure. Nous vous recommandons de changer régulièrement les clés pour des raisons de sécurité.
- Spécifiez les locataires partagés et les abonnements. Vous pouvez ajouter jusqu'à huit locataires partagés. Pour chaque locataire, vous pouvez ajouter jusqu'à huit abonnements.
- Cliquez sur **Enregistrer** et **Appliquer** lorsque vous avez terminé.

Entrez les informations dans le champ **Options de connexion** uniquement selon les directives d'un représentant de l'assistance Citrix.

Modifier les réseaux

Vous pouvez changer de réseau pour une connexion. Procédez comme suit :

1. Cliquez sur **Hébergement**.
2. Sélectionnez les ressources cibles sous la connexion, puis sélectionnez **Modifier le réseau** dans la barre d'actions.
3. Sélectionnez un ou plusieurs réseaux à utiliser par les machines virtuelles.
4. Cliquez sur **Enregistrer** pour enregistrer vos modifications et quitter.

Activer ou désactiver le mode maintenance pour une connexion

Le fait d'activer le mode de maintenance pour une connexion empêche toute nouvelle action d'alimentation d'affecter les machines stockées sur cette connexion. Les utilisateurs ne peuvent pas se connecter à une machine lorsqu'elle est en mode de maintenance. Si les utilisateurs sont déjà connectés, le mode maintenance prend effet lorsqu'ils ferment leur session.

1. Connectez-vous à Web Studio.
2. Sélectionnez **Hébergement** dans le volet de gauche.
3. Sélectionnez la connexion. Pour activer le mode de maintenance, sélectionnez **Activer le mode de maintenance** dans la barre d'actions. Pour désactiver le mode de maintenance, sélectionnez **Désactiver le mode de maintenance**.

Vous pouvez également activer ou désactiver le mode de maintenance pour des machines individuelles. De plus, vous pouvez activer ou désactiver le mode de maintenance sur les machines dans les catalogues de machines ou les groupes de mise à disposition.

Supprimer une connexion

La suppression d'une connexion peut entraîner la suppression de nombreuses machines et la perte de données. Assurez-vous que les données utilisateur sur les machines affectées sont sauvegardées ou ne sont plus nécessaires.

Avant de supprimer une connexion, assurez-vous que :

- Tous les utilisateurs ont fermé leur session sur les machines stockées sur la connexion.
- Aucune session utilisateur déconnectée n'est en cours d'exécution.
- Le mode de maintenance est activé pour les machines regroupées et dédiées.
- Toutes les machines des catalogues de machines utilisées par la connexion sont hors tension.

Un catalogue de machines devient inutilisable lorsque vous supprimez une connexion référencée par ce catalogue. Si cette connexion est référencée par un catalogue, vous avez la possibilité de supprimer le catalogue. Avant de supprimer un catalogue, assurez-vous qu'il n'est pas utilisé par d'autres connexions.

1. Connectez-vous à Web Studio.
2. Sélectionnez **Hébergement** dans le volet de gauche.
3. Sélectionnez la connexion, puis sélectionnez **Supprimer la connexion** dans la barre d'actions.
4. Si cette connexion possède des machines stockées sur celle-ci, vous êtes invité à indiquer si elles doivent être supprimées. Si elles doivent être supprimées, spécifiez la procédure à suivre pour les comptes d'ordinateurs Active Directory associés.

Renommer ou tester une connexion

1. Connectez-vous à Web Studio.
2. Sélectionnez **Hébergement** dans le volet de gauche.
3. Sélectionnez la connexion puis sélectionnez **Renommer la connexion** ou **Tester la connexion** dans la barre d'actions.

Afficher les détails des machines sur une connexion

1. Connectez-vous à Web Studio.
2. Sélectionnez **Hébergement** dans le volet de gauche.
3. Sélectionnez la connexion, puis sélectionnez **Afficher les machines** dans la barre d'actions.

Le volet supérieur dresse la liste des machines accessibles via la connexion. Sélectionnez une machine pour afficher les détails correspondants dans le volet inférieur. Les détails de session sont également fournis pour les sessions ouvertes.

Utilisez la fonctionnalité de recherche pour trouver des machines rapidement. Soit sélectionnez une recherche enregistrée dans la liste en haut de la fenêtre, soit créez une recherche. Vous pouvez effectuer la recherche en tapant le nom de la machine ou une partie de celui-ci, ou créer une expression que vous utiliserez ensuite dans une recherche avancée. Pour créer une expression, cliquez sur le bouton de **développement**, puis sélectionnez dans les listes de propriétés et d'opérateurs.

Gérer les machines sur une connexion

1. Connectez-vous à Web Studio.
2. Sélectionnez **Hébergement** dans le volet de gauche.
3. Sélectionnez une connexion, puis sélectionnez **Afficher les machines** dans le volet **Actions**.
4. Sélectionnez l'une des options suivantes dans la barre d'actions. Certaines actions ne sont pas disponibles, en fonction de l'état de la machine et le type d'hôte de la connexion.

Action	Description
Démarrer	Démarre la machine si celle-ci est hors tension ou suspendue.
Suspendre	Met en pause la machine sans la fermer et actualise la liste de machines.
Arrêter	Requiert la fermeture du système d'exploitation.
Forcer l'arrêt	Place la machine hors tension de manière forcée et actualise la liste des machines.
Redémarrer	Requiert la fermeture du système d'exploitation de la machine, puis redémarrage de la machine. Si le système d'exploitation ne peut pas répondre, le bureau reste dans son état actuel.
Activer le mode de maintenance	Arrête temporairement les connexions à une machine. Les utilisateurs ne peuvent pas se connecter à une machine dans cet état. Si les utilisateurs sont connectés, le mode maintenance prend effet lorsqu'ils ferment leur session. (Vous pouvez aussi activer ou désactiver le mode de maintenance sur toutes les machines accessibles via une connexion, comme décrit ci-dessus.)

Action	Description
Supprimer d'un groupe de mise à disposition	La suppression d'une machine d'un groupe de mise à disposition ne la supprime pas dans le catalogue de machines que le groupe de mise à disposition utilise. Vous ne pouvez supprimer une machine que si aucun utilisateur n'y est connecté. Activez le mode de maintenance pour empêcher temporairement les utilisateurs de se connecter lors de la suppression de la machine.
Supprimer	Lorsque vous supprimez une machine, les utilisateurs n'y ont plus accès et la machine disparaît du catalogue de machines. Avant de supprimer une machine, assurez-vous que toutes les données utilisateur sont sauvegardées ou ne sont plus nécessaires. Vous ne pouvez supprimer une machine que si aucun utilisateur n'y est connecté. Activez le mode de maintenance pour empêcher temporairement les utilisateurs de se connecter lors de la suppression de la machine.

Pour les actions qui impliquent la fermeture de la machine, si la machine ne se ferme pas dans les 10 minutes, elle est mise hors tension. Si Windows tente d'installer des mises à jour durant la fermeture, il y a un risque que la machine soit mise hors tension avant la fin des mises à jour.

Modifier un espace de stockage

Vous pouvez afficher l'état des serveurs utilisés pour stocker les données du système d'exploitation et les données temporaires des machines virtuelles qui utilisent une connexion. Vous pouvez également spécifier les serveurs que vous souhaitez utiliser pour le stockage de chaque type de données.

1. Connectez-vous à Web Studio.
2. Sélectionnez **Hébergement** dans le volet de gauche.
3. Sélectionnez la connexion, puis sélectionnez **Modifier le stockage** dans la barre d'actions.
4. Dans le panneau de gauche, sélectionnez le type de données : système d'exploitation ou temporaires.
5. Cochez ou décochez les cases à cocher d'un ou plusieurs périphériques de stockage pour le type de données sélectionné.

6. Cliquez sur **OK**.

Chaque périphérique de stockage dans la liste inclut son nom et l'état du stockage. Les valeurs d'état du stockage valides sont les suivantes :

- **En cours d'utilisation :** le stockage est utilisé pour la création de machines.
- **Remplacé** : le stockage est utilisé uniquement pour des machines existantes. Aucune nouvelle machine n'est ajoutée à ce stockage.
- **Non utilisé** : le stockage n'est pas utilisé pour la création de machines.

Si vous désactivez la case à cocher d'un périphérique qui est actuellement **en cours d'utilisation**, son état passera à **Remplacé**. Les machines existantes continueront à utiliser ce périphérique de stockage (et peuvent écrire des données dessus), par conséquent, il est possible que cet emplacement atteigne sa pleine capacité même après qu'il cesse d'être utilisé pour la création de machines.

Supprimer, renommer ou test des ressources

1. Connectez-vous à Web Studio.
2. Sélectionnez **Hébergement** dans le volet de gauche.
3. Sélectionnez la ressource puis sélectionnez l'entrée appropriée dans la barre d'actions : **Supprimer les ressources**, **Renommer les ressources** ou **Tester les ressources**.

Détecter les ressources Azure orphelines

Les ressources orphelines sont des ressources inutilisées présentes dans le système et elles peuvent entraîner des dépenses inutiles.

Cette fonctionnalité vous permet de détecter les ressources Azure orphelines dans les hôtes de votre site Citrix Virtual Apps and Desktops.

Suivez les étapes sur Web Studio :

1. Dans **Gérer**, sélectionnez **Hébergement** dans le volet de gauche.
2. Sélectionnez une connexion, puis sélectionnez **Détecter les ressources orphelines** dans la barre d'actions. La boîte de dialogue **Détecter les ressources orphelines** affiche le rapport sur les ressources orphelines.
3. Pour consulter le rapport sur les ressources orphelines, sélectionnez **Afficher le rapport**.

Vous pouvez également détecter les ressources Azure orphelines à l'aide de PowerShell. Pour plus d'informations, reportez-vous à la section Récupérer une liste de ressources orphelines.

Pour comprendre pourquoi ces ressources sont orphelines et pour savoir comment procéder, consultez Gérer efficacement les ressources Azure orphelines avec Citrix.

Horloges de connexion

Vous pouvez utiliser des paramètres de stratégie permettant de configurer trois horloges de connexion :

- **Minuteur de connexion maximal :** détermine la durée maximale d'une connexion non interrompue entre une machine utilisateur et un bureau virtuel. Utilisez les paramètres de stratégies **Horloge de connexion de session** et **Intervalle d'horloge de connexion de session**.
- **Minuteur de connexion inactif :** détermine la durée pendant laquelle une connexion non interrompue d'une machine utilisateur à un bureau virtuel est maintenue si aucune entrée utilisateur n'est effectuée. Utilisez les paramètres de stratégie **Horloge inactive de session** et **Intervalle d'horloge inactive de session**.
- **Horloge de déconnexion :** détermine la durée pendant laquelle un bureau virtuel déconnecté et verrouillé peut rester verrouillé avant que la session ne se ferme. Utilisez les paramètres de stratégie **Horloge de session déconnectée** et **Intervalle d'horloge de session déconnectée**.

Lorsque vous mettez à jour l'un de ces paramètres, vous devez vous assurer qu'ils sont cohérents sur votre déploiement.

Consultez la documentation sur les paramètres de stratégie pour plus d'informations.

Récupérer une liste de ressources orphelines

Vous pouvez obtenir une liste des ressources orphelines créées par MCS mais qui ne sont plus suivies par MCS. Cela s'applique actuellement aux environnements Azure. Pour obtenir la liste, vous pouvez utiliser les commandes PowerShell. Vous pouvez filtrer à l'aide de connexions.

> **Remarque :**
>
> - La commande PowerShell est rejetée si un provisioning ou une mise à jour d'image est en cours.
> - Une ressource gérée par le client balisée avec toutes les balises Citrix est détectée comme ressource orpheline. Toutefois, si vous ajoutez une autre balise CitrixDetectIgnore dont la valeur est true pour cette ressource, la ressource est ignorée lors de la détection de ressources orphelines.

Limitations

- Seul un utilisateur administrateur ayant un rôle intégré d'administrateur complet ou d'administrateur de cloud peut exécuter la commande PowerShell et obtenir la liste des ressources orphelines.

- Pour éviter une reconnaissance incorrecte des ressources orphelines, ne mettez pas les machines virtuelles sous tension pendant le filtrage des ressources orphelines.
- Environ 2 000 enregistrements sont affichés comme étant orphelins en cas de charge de travail potentiellement importante.

Pour afficher la liste des ressources orphelines, procédez comme suit :

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez les commandes suivantes :

   a) Obtenez l'UID de connexion. L'UID de connexion est la valeur de l'attribut HypervisorConnectionUid.

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.PluginId -like 'Azure*'  }
    "
   <!--NeedCopy-->
   ```

   b) Consultez la liste des ressources orphelines.

   ```
   get-provorphanedresource -HypervisorConnectionUid <connection
       uid>
   <!--NeedCopy-->
   ```

Pour afficher la liste des ressources orphelines à partir d'un ID d'abonnement, procédez comme suit :

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez les commandes suivantes :

   a) Trouvez l'UID de connexion à l'aide de l'ID d'abonnement. L'UID de connexion est la valeur de l'attribut HypervisorConnectionUid.

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.CustomProperties -match '<subscriptionId>'  }

   <!--NeedCopy-->
   ```

   b) Consultez la liste des ressources orphelines :

   ```
   get-provorphanedresource -HypervisorConnectionUid <connection
       uid>
   <!--NeedCopy-->
   ```

> **Remarque :**
>
> Vérifiez attentivement les ressources avant de les supprimer.

Autres ressources

Pour plus d'informations sur la connexion à des types d'hôtes spécifiques, consultez :

- Connexion à AWS
- Connexion à XenServer
- Connexion à des environnements Google Cloud
- Connexion à Microsoft Azure
- Connexion à Microsoft System Center Virtual Machine Manager
- Connexion à Nutanix
- Connexion aux solutions partenaires et cloud Nutanix
- Connexion à VMware
- Connexion aux solutions partenaires et cloud VMware

Si vous êtes dans le processus de déploiement initial, créez un catalogue de machines.

Connexion à AWS

June 27, 2024

La section Créer et gérer des connexions et des ressources décrit les assistants qui créent une connexion. Les informations suivantes couvrent les détails spécifiques aux environnements de cloud AWS.

> **Remarque :**
>
> Avant de créer une connexion à AWS, vous devez d'abord terminer la configuration de votre compte AWS en tant qu'emplacement de ressources. Voir Environnements de cloud AWS.

Créer une connexion

Lorsque vous créez une connexion à partir de Web Studio :

- Vous devez fournir les valeurs de la clé API et de la clé secrète. Vous pouvez exporter le fichier de clé contenant ces valeurs à partir d'AWS, puis les importer. Vous devez également fournir la région, la zone de disponibilité, le nom du VPC, les adresses de sous-réseau, le nom du domaine, les noms de groupe de sécurité et les informations d'identification.
- Le fichier d'informations d'identification pour le compte AWS de racine, (récupéré à partir de la console AWS) n'est pas au même format que les fichiers d'informations d'identification téléchargés pour les utilisateurs standard AWS. Par conséquent, la gestion de Citrix Virtual Apps and Desktops ne peut pas utiliser le fichier pour remplir les champs de clé API et de clé secrète. Vérifiez que vous utilisez les fichiers d'informations d'identification AWS (IAM).

> **Remarque :**
>
> Après avoir créé une connexion, les tentatives de mise à jour de la clé API et de la clé secrète peuvent échouer. Pour résoudre le problème, vérifiez les restrictions de votre serveur proxy ou de votre pare-feu et vérifiez que l'adresse suivante est contactable : `https://*.amazonaws.com`.

Valeurs par défaut des connexions hôtes

Lorsque vous créez des connexions hôtes dans des environnements cloud AWS, les valeurs par défaut suivantes sont affichées :

Option	Absolu	Pourcentage
Actions simultanées (tous types)	125	100
Nouvelles actions maximales par minute	125	

MCS prend en charge 100 opérations de provisioning simultanées maximum par défaut.

URL du point de terminaison de service

URL du point de terminaison de service de zone standard

Lorsque vous utilisez MCS, une nouvelle connexion AWS est ajoutée avec une clé API et un secret API. Avec ces informations, ainsi que le compte authentifié, MCS interroge AWS pour connaître les zones prises en charge à l'aide de l'appel d'API EC2 DescribeRegions AWS. La requête est effectuée à l'aide d'une URL de point de terminaison de service EC2 générique `https://ec2.amazonaws.com/`. Utilisez MCS pour sélectionner la zone de connexion dans la liste des zones prises en charge. L'URL de point de terminaison de service AWS préférée est automatiquement sélectionnée pour la zone. Toutefois, après avoir créé l'URL du point de terminaison de service, vous ne pouvez plus définir ou modifier l'URL.

Définir les autorisations IAM

Utilisez les informations de cette section pour définir les autorisations IAM pour Citrix Virtual Apps and Desktops sur AWS. Le service IAM d'Amazon autorise les comptes ayant plusieurs utilisateurs, qui peuvent être organisés en groupes. Ces utilisateurs peuvent disposer d'autorisations différentes pour contrôler leur capacité à effectuer des opérations associées au compte. Pour plus d'informations sur les autorisations IAM, consultez Référence de stratégie JSON IAM.

Pour appliquer la stratégie d'autorisations IAM à un nouveau groupe d'utilisateurs :

1. Connectez-vous à AWS Management Console et sélectionnez le **service IAM** dans la liste déroulante.
2. Sélectionnez **Créer un groupe d'utilisateurs**.
3. Tapez un nom pour le nouveau groupe d'utilisateurs et sélectionnez **Continuer**.
4. Sur la page **Autorisations**, choisissez **Stratégie personnalisée**. Sélectionnez **Sélectionner**.
5. Tapez un nom pour la stratégie **Autorisations**.
6. Dans la section **Document de stratégie**, entrez les autorisations appropriées.

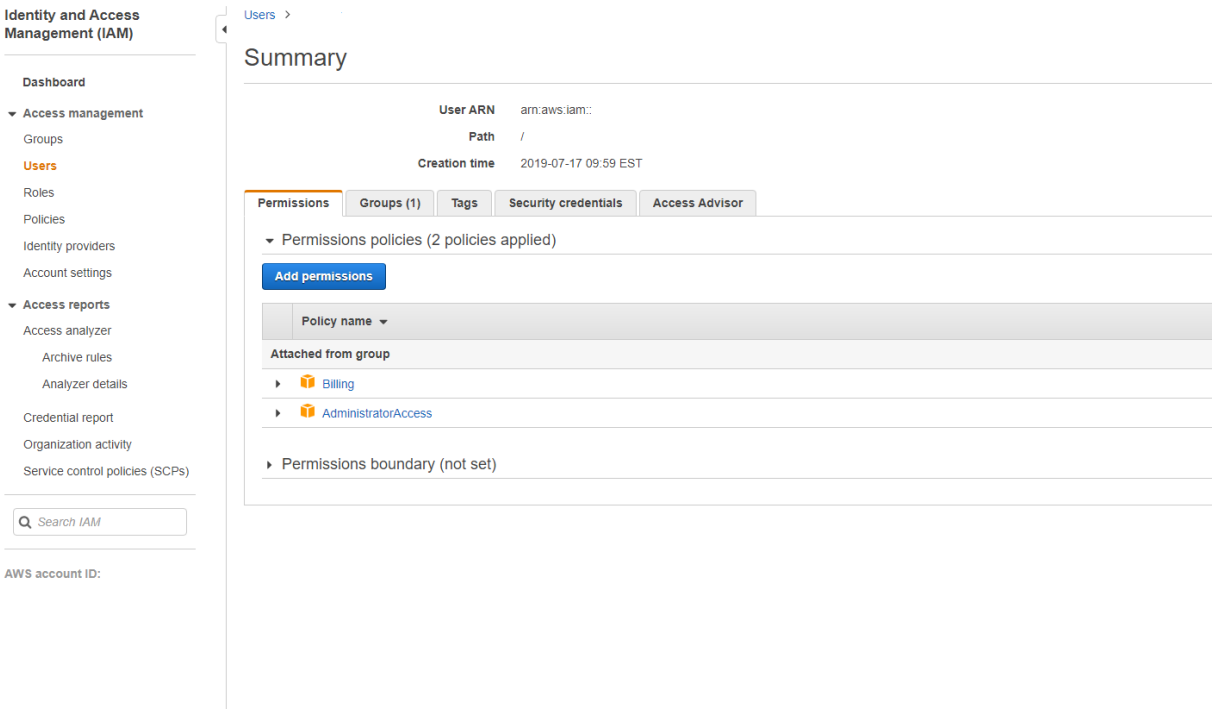
Après avoir saisi les informations de stratégie, sélectionnez **Continuer** pour compléter le groupe d'utilisateurs. Les utilisateurs du groupe sont autorisés à effectuer uniquement les actions requises pour Citrix Virtual Apps and Desktops.

> **Important :**
>
> Utilisez le texte de stratégie fourni dans l'exemple plus tôt pour répertorier les actions que Citrix Virtual Apps and Desktops utilise pour effectuer des actions au sein d'un compte AWS sans les restreindre à des ressources spécifiques. Citrix vous recommande d'utiliser cet exemple à des fins de test. Pour les environnements de production, vous pouvez choisir d'ajouter d'autres restrictions sur les ressources.

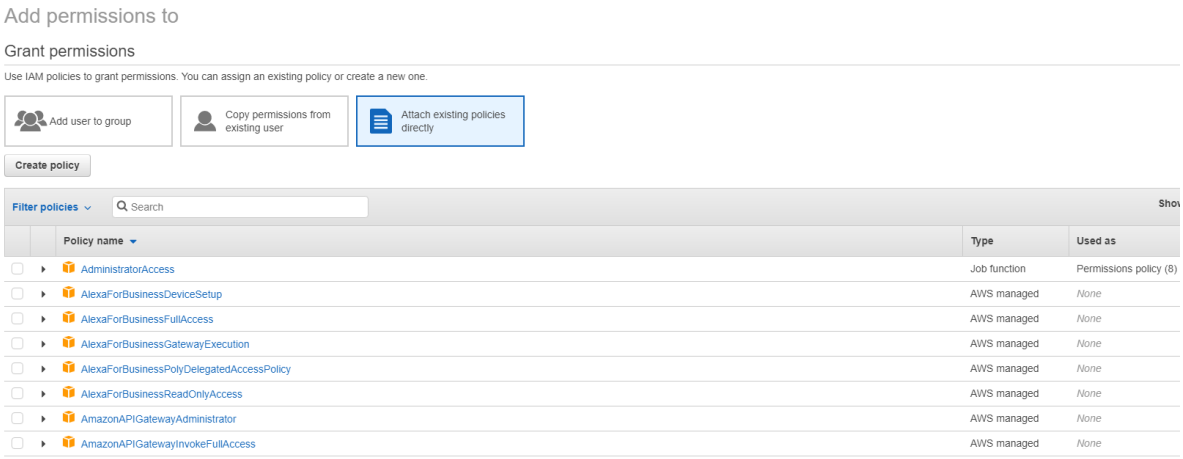
Définir les autorisations IAM

Définissez les autorisations dans la section **IAM** d'AWS Management Console :

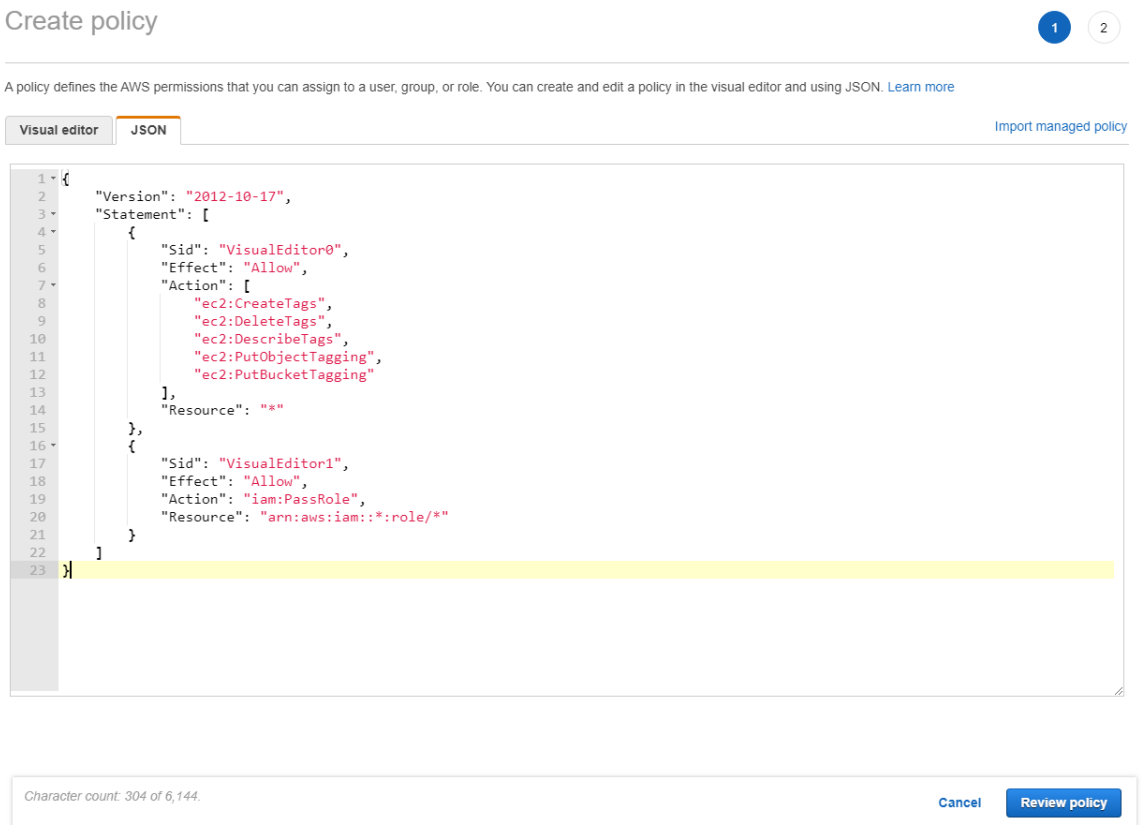
1. Dans le panneau **Summary**, sélectionnez l'onglet **Permissions**.
2. Sélectionnez **Add permissions**.



Dans l'écran **Add Permissions to**, accordez des autorisations :



Utilisez l'exemple suivant dans l'onglet **JSON** :



> **Conseil :**
>
> L'exemple JSON mentionné peut ne pas inclure toutes les autorisations pour votre environnement. Consultez Comment faire pour définir les autorisations de gestion des identités et des accès en exécutant Citrix Virtual Apps and Desktops sur AWS pour plus d'informations.

Autorisations AWS requises

Cette section contient la liste complète des autorisations AWS.

> **Remarque :**
>
> L'autorisation *iam:PassRole* n'est requise que pour **role_based_auth**.

Création d'une connexion hôte

Une nouvelle connexion hôte est ajoutée à l'aide des informations d'AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
```



```
6
7               "Action": [
8                   "ec2:DescribeAvailabilityZones",
9                   "ec2:DescribeImages",
10                  "ec2:DescribeInstances",
11                  "ec2:DescribeInstanceTypes",
12                  "ec2:DescribeSecurityGroups",
13                  "ec2:DescribeSubnets",
14                  "ec2:DescribeVpcs"
15              ],
16              "Effect": "Allow",
17              "Resource": "*"
18          }
19
20      ]
21  }
22
23  <!--NeedCopy-->
```

Gestion de l'alimentation des machines virtuelles

Les instances de machine sont sous tension ou hors tension.

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Action": [
8                  "ec2:AttachVolume",
9                  "ec2:CreateVolume",
10                 "ec2:DeleteVolume",
11                 "ec2:DescribeInstances",
12                 "ec2:DescribeVolumes",
13                 "ec2:DetachVolume",
14                 "ec2:StartInstances",
15                 "ec2:StopInstances"
16             ],
17             "Effect": "Allow",
18             "Resource": "*"
19         }
20
21     ]
22 }
23
24 <!--NeedCopy-->
```


Création, mise à jour ou suppression de machines virtuelles

Un catalogue de machines est créé, mis à jour ou supprimé avec des machines virtuelles provisionnées en tant qu'instances AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
 ,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
```



```
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
         }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

Remarque :

La section EC2 relative aux groupes de sécurité n'est nécessaire que si un groupe de sécurité d'isolement doit être créé pour la machine virtuelle de préparation lors de la création du catalogue. Une fois cette action effectuée, ces autorisations ne sont pas requises.

Chargement et téléchargement directs sur disque Le chargement direct sur disque élimine le besoin du travailleur de volume pour le provisioning de catalogue de machines et utilise à la place des API publiques fournies par AWS. Cette fonctionnalité réduit le coût associé aux comptes de stockage supplémentaires et la complexité de la gestion des opérations du travailleur de volume.

> **Remarque :**
>
> Le travailleur de volume n'est plus pris en charge.

Les autorisations suivantes doivent être ajoutées à la stratégie :

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

> **Important :**
>
> - Vous pouvez ajouter une machine virtuelle à des catalogues de machines existants sans aucune opération du travailleur de volume, telle que l'AMI et la machine virtuelle du travailleur de volume.
> - Si vous supprimez un catalogue existant qui utilise un travailleur de volume, tous les artefacts, y compris ceux liés au travailleur de volume, sont supprimés.

Cryptage EBS des volumes créés

EBS peut crypter automatiquement les volumes nouvellement créés si l'AMI est cryptée, ou EBS est configuré pour crypter tous les nouveaux volumes. Toutefois, pour implémenter cette fonctionnalité, les autorisations suivantes doivent être incluses dans la stratégie IAM.

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
```



```
                    "kms:DescribeKey",
                    "kms:GenerateDataKeyWithoutPlainText",
                    "kms:ReEncryptTo",
                    "kms:ReEncryptFrom"
                ],
                "Resource": "*"
            }

        ]
    }

<!--NeedCopy-->
```

Remarque :

Les autorisations peuvent être limitées à des clés spécifiques en incluant un bloc Ressource et Condition à la discrétion de l'utilisateur. Par exemple, **Autorisations KMS avec condition** :

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                   -456d-a12b-a123b4cd56ef"
            ],
            "Condition": {

                "Bool": {

                    "kms:GrantIsForAWSResource": true
                 }

             }

         }

    ]
}

<!--NeedCopy-->
```


La déclaration de stratégie de clé suivante est la stratégie de clé par défaut complète pour les clés KMS qui est requise pour permettre au compte d'utiliser des stratégies IAM afin de déléguer l'autorisation pour toutes les actions (kms: *) sur la clé KMS.

```
{

"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {

"AWS": "arn:aws:iam::111122223333:root"
 }
 ,
"Action": "kms:",
"Resource": ""
 }

<!--NeedCopy-->
```

Pour plus d'informations, consultez la documentation officielle d'AWS Key Management Service.

Authentification basée sur les rôles IAM

Les autorisations suivantes sont ajoutées pour prendre en charge l'authentification basée sur les rôles.

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
         }

    ]
 }

<!--NeedCopy-->
```

Stratégie d'autorisations IAM minimales

Le code JSON suivant peut être utilisé pour toutes les fonctionnalités actuellement prises en charge. Vous pouvez créer des connexions hôtes, créer, mettre à jour ou supprimer des machines virtuelles et gérer l'alimentation à l'aide de cette stratégie.

La stratégie peut être appliquée aux utilisateurs comme expliqué dans les sections Définition des autorisations IAM. Vous pouvez également utiliser l'authentification basée sur les rôles à l'aide de la clé de sécurité et de la clé secrète **role_based_auth**.

> **Important :**
>
> Pour utiliser **role_based_auth**, configurez d'abord le rôle IAM souhaité sur tous les Delivery Controller de notre site. À l'aide de Web Studio, ajoutez la connexion d'hébergement et fournissez l'élément role_based_auth pour la clé d'authentification et le secret. Une connexion d'hébergement avec ces paramètres utilise ensuite l'authentification basée sur les rôles.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
```



```
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
```



```
          }
  ,
         {

             "Effect": "Allow",
             "Action": [
                  "kms:CreateGrant",
                  "kms:Decrypt",
                  "kms:DescribeKey",
                  "kms:GenerateDataKeyWithoutPlainText",
                  "kms:GenerateDataKey",
                  "kms:ReEncryptTo",
                  "kms:ReEncryptFrom"
             ],
             "Resource": "*"
          }
  ,
         {

             "Effect": "Allow",
             "Action": "iam:PassRole",
             "Resource": "arn:aws:iam::*:role/*"
          }

     ]
  }

<!--NeedCopy-->
```

Remarque :

- La section EC2 relative aux groupes de sécurité n'est nécessaire que si un groupe de sécurité d'isolement doit être créé pour la machine virtuelle de préparation lors de la création du catalogue. Une fois cette action effectuée, ces autorisations ne sont pas requises.
- La section KMS n'est requise que lors de l'utilisation du cryptage de volume EBS.
- La section d'autorisation iam:PassRole n'est requise que pour **role_based_auth**.
- En fonction de vos besoins et de votre environnement, vous pouvez ajouter des autorisations spécifiques au niveau des ressources au lieu d'un accès complet. Consultez les documents AWS Demystifying EC2 Resource-Level Permissions et Gestion de l'accès pour les ressources AWS pour plus de détails.

Autres ressources

- Si vous êtes dans le processus de déploiement initial, consultez la section Créer des catalogues de machines.
- Pour obtenir des informations spécifiques à AWS, consultez la section Créer un catalogue AWS.

Informations supplémentaires

- Connexions et ressources
- Créer des catalogues de machines

Connexion à XenServer

June 27, 2024

La section Créer et gérer des connexions et des ressources décrit les assistants qui créent une connexion. Les informations suivantes couvrent les détails spécifiques aux environnements de virtualisation XenServer.

> **Remarque :**
>
> Avant de créer une connexion à XenServer, vous devez d'abord terminer la configuration de votre compte XenServer en tant qu'emplacement de ressources. Voir Environnements de virtualisation XenServer.

Créer une connexion à XenServer

Lorsque vous créez une connexion à XenServer (anciennement Citrix Hypervisor), vous devez fournir les informations d'identification d'un administrateur d'alimentation de machine virtuelle avancé ou d'un utilisateur de niveau plus élevé.

Citrix vous recommande d'utiliser HTTPS pour sécuriser les communications avec XenServer. Pour utiliser HTTPS, vous devez remplacer le certificat SSL par défaut installé sur XenServer ; consultez l'article CTX128656.

Si la haute disponibilité est activée sur le serveur XenServer, vous pouvez la configurer. Citrix vous recommande de sélectionner tous les serveurs du pool (dans Modifier les serveurs HA) pour permettre la communication avec le serveur XenServer en cas d'échec du pool principal.

Vous pouvez sélectionner un type et un groupe de processeur graphique, ou de pass-through, si XenServer prend en charge vGPU. La vue indique si la sélection possède des ressources GPU dédiées.

Lorsque vous utilisez le stockage local sur un ou plusieurs hôtes XenServer pour le stockage des données temporaires, assurez-vous que chaque emplacement de stockage du pool a un nom unique. (Pour modifier un nom dans XenCenter, cliquez avec le bouton droit sur le stockage et modifiez le nom de la propriété.)

Vous pouvez utiliser Machine Creation Services (MCS) et Citrix Provisioning (anciennement Provisioning Services) pour provisionner :

- Les ordinateurs BIOS d'ancienne génération pour les machines virtuelles avec OS de bureau ou de serveur prises en charge.
- Les ordinateurs UEFI pour les machines virtuelles avec OS de bureau ou de serveur prises en charge, y compris le démarrage sécurisé.

> **Remarque :**
>
> Des autorisations Pool Operator ou supérieures sont requises lors de la configuration de MCS.

Utiliser les connexions IntelliCache pour XenServer

À l'aide d'IntelliCache, les déploiements VDI hébergés sont plus rentables car ils vous permettent d'utiliser une combinaison de stockage partagé et de stockage local. Cela améliore les performances et réduit le trafic réseau. Le stockage local met en cache l'image principale depuis le stockage partagé ; cela réduit le nombre de lectures sur le stockage partagé. Pour les bureaux partagés, les écritures sur les disques de différenciation s'effectuent sur le stockage local sur l'hôte et non sur le stockage partagé.

- Le stockage partagé doit être de type NFS si vous utilisez IntelliCache.
- Citrix vous recommande d'utiliser un périphérique de stockage local à hautes performances pour assurer un transfert de données optimal.

Pour utiliser IntelliCache, vous devez l'activer dans ce produit et XenServer.

- Lors de l'installation de XenServer, sélectionnez **Activer l'allocation dynamique (Stockage optimisé pour Virtual Desktops)**. Citrix ne prend pas en charge les regroupements mixtes de serveurs avec IntelliCache activé et de serveurs sans IntelliCache activé. Pour plus d'informations, veuillez consulter la documentation de XenServer.
- Dans Citrix Virtual Apps and Desktops, IntelliCache est désactivé par défaut. Vous pouvez modifier le paramètre uniquement lors de la création d'une connexion XenServer ; vous ne pouvez pas désactiver IntelliCache ultérieurement. Lorsque vous ajoutez une connexion XenServer :
  - Sélectionnez**Partagé**en tant que type de stockage.
  - Sélectionnez la case à cocher **Utiliser IntelliCache**.

Autorisations XenServer requises

Les autorisations XenServer sont basées sur un rôle (RBAC). La fonctionnalité de contrôle d'accès basé sur un rôle (RBAC) de XenServer vous permet d'attribuer des utilisateurs, des rôles et des autorisations pour contrôler qui a accès à votre XenServer et quelles actions ils peuvent effectuer. Le système

RBAC XenServer mappe un utilisateur (ou un groupe d'utilisateurs) à des rôles définis (un ensemble d'autorisations nommé). Les rôles sont associés à des autorisations XenServer leur permettant d'effectuer certaines opérations.

Pour plus d'informations, consultez la section Contrôle d'accès basé sur un rôle.

La hiérarchie des rôles par ordre croissant des autorisations est la suivante : Lecture seule → Opérateur de machine virtuelle → Administrateur de machine virtuelle → Administrateur d'alimentation de VM → Opérateur de pool → Administrateur du pool.

La section suivante récapitule le rôle minimum requis pour chaque tâche de provisioning.

Création d'une connexion hôte

Tâche	Rôle minimum requis
Ajouter une connexion hôte à l'aide des informations obtenues auprès de XenServer	Lecture seule
Afficher les utilisateurs et le rôle qui leur est attribué	Lecture seule

Gestion de l'alimentation des machines virtuelles

Tâche	Rôle minimum requis
Mettre sous tension ou hors tension les machines virtuelles	Opérateur de machine virtuelle

Création, mise à jour ou suppression de machines virtuelles

Tâche	Rôle minimum requis
Ajouter des machines virtuelles aux planifications d'instantanés existantes ou les supprimer	Administrateur d'alimentation de VM
Ajouter, modifier et supprimer des planifications d'instantanés	Opérateur de pool
Publier l'image principale	Opérateur de pool (nécessite le verrouillage des ports du commutateur)

Tâche	Rôle minimum requis
Créer un catalogue de machines	Opérateur de pool : nécessite le verrouillage des ports du commutateur
Ajouter ou supprimer des machines virtuelles (machines virtuelles non compatibles GPU)	Administrateur de machine virtuelle
Ajouter ou supprimer des machines virtuelles (machines virtuelles compatibles GPU)	Opérateur de pool
Ajouter, supprimer ou configurer des disques virtuels ou des périphériques CD	Administrateur de machine virtuelle
Gérer les balises	Opérateur de machine virtuelle

Pour plus d'informations sur les rôles et autorisations RBAC, consultez la section Rôles et autorisations RBAC.

Pour plus d'informations sur le verrouillage des ports de commutateur, consultez la section Utiliser le verrouillage des ports du commutateur.

Autres ressources

- Si vous êtes dans le processus de déploiement initial, consultez la section Créer des catalogues de machines.
- Pour obtenir des informations spécifiques à XenServer, consultez Créer un catalogue XenServer

Informations supplémentaires

- Connexions et ressources
- Créer des catalogues de machines

Connexion à des environnements Google Cloud

June 28, 2024

La section Créer et gérer des connexions et des ressources décrit les assistants qui créent une connexion. Les informations suivantes couvrent les détails spécifiques aux environnements Google Cloud.

> **Remarque :**
>
> Avant de créer une connexion aux environnements Google Cloud, vous devez d'abord terminer la configuration de votre compte Google Cloud en tant qu'emplacement de ressources. Voir Environnements Google Cloud.

Ajouter une connexion

Suivez les instructions sous Créer une connexion et des ressources. La procédure suivante vous guide tout au long de la configuration d'une connexion d'hébergement :

1. Dans **Gérer > Configuration**, sélectionnez **Hébergement** dans le panneau de gauche.
2. Sélectionnez **Ajouter une connexion et des ressources** dans le volet Actions.
3. Sur la page **Connexion**, sélectionnez **Créer une nouvelle connexion** et **Outils de provisioning Citrix**, puis sélectionnez **Suivant**.
   - **Type de connexion** : sélectionnez **Google Cloud** dans le menu.
   - **Nom de la connexion** : Tapez un nom pour la connexion.
4. Sur la page **Région**, sélectionnez un nom de projet dans le menu, sélectionnez une région contenant les ressources à utiliser, puis sélectionnez **Suivant**.
5. Sur la page **Réseau**, tapez un nom pour les ressources, sélectionnez un réseau virtuel dans le menu, sélectionnez un sous-ensemble, puis sélectionnez **Suivant**. Le nom des ressources facilite l'identification de la combinaison région/réseau. Les réseaux virtuels avec le suffixe *(Shared)* (Partagé) ajouté à leur nom représentent des VPC partagés. Si vous configurez un rôle IAM au niveau du sous-réseau pour un VPC partagé, seuls des sous-réseaux spécifiques du VPC partagé apparaissent dans la liste des sous-réseaux.

   > **Remarque :**
   >
   > - Le nom de la ressource peut contenir entre 1 et 64 caractères, et ne peut pas contenir uniquement des espaces ou les caractères `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

6. Sur la page **Résumé**, vérifiez les informations, puis sélectionnez **Terminer** pour quitter la fenêtre **Ajouter une connexion et des ressources**.

Une fois la connexion et les ressources créées, la connexion et les ressources que vous avez créées sont répertoriées. Pour configurer la connexion, sélectionnez la connexion, puis sélectionnez l'option appropriée dans la barre d'actions.

De même, vous pouvez supprimer, renommer ou tester les ressources créées sous la connexion. Pour ce faire, sélectionnez la ressource sous la connexion, puis l'option appropriée dans la barre d'actions.

URL du point de terminaison de service

Vous devez avoir accès aux URL suivantes :

- https://oauth2.googleapis.com
- https://cloudresourcemanager.googleapis.com
- https://compute.googleapis.com
- https://storage.googleapis.com
- https://cloudbuild.googleapis.com

Projets Google Cloud

Il existe essentiellement deux types de projets Google Cloud :

- Projet de provisioning : dans ce cas, le compte administrateur actuel est propriétaire des machines provisionnées du projet. Ce projet est également appelé projet local.
- Projet VPC partagé : projet dans lequel les machines créées dans le projet de provisioning utilisent le VPC du projet VPC partagé. Le compte administrateur utilisé pour le projet de provisioning dispose d'autorisations limitées dans ce projet, uniquement d'autorisations d'utilisation du VPC.

Créer un environnement sécurisé pour le trafic géré par GCP

Vous pouvez autoriser l'accès privé de Google à vos projets Google Cloud. Cette mise en œuvre améliore la sécurité lors de la gestion des données sensibles. Pour ce faire, vous pouvez effectuer l'une des opérations suivantes :

- Incluez les règles d'entrée suivantes de VPC Service Controls pour le compte de service Cloud Build. Si vous effectuez cette étape, ne suivez pas les étapes ci-dessous pour créer un environnement sécurisé pour le trafic géré par GCP.

```
Ingress Rule 1
From:
Identities:
<ProjectID>@cloudbuild.gserviceaccount.com
Source > All sources allowed
To:
Projects =
All projects
```



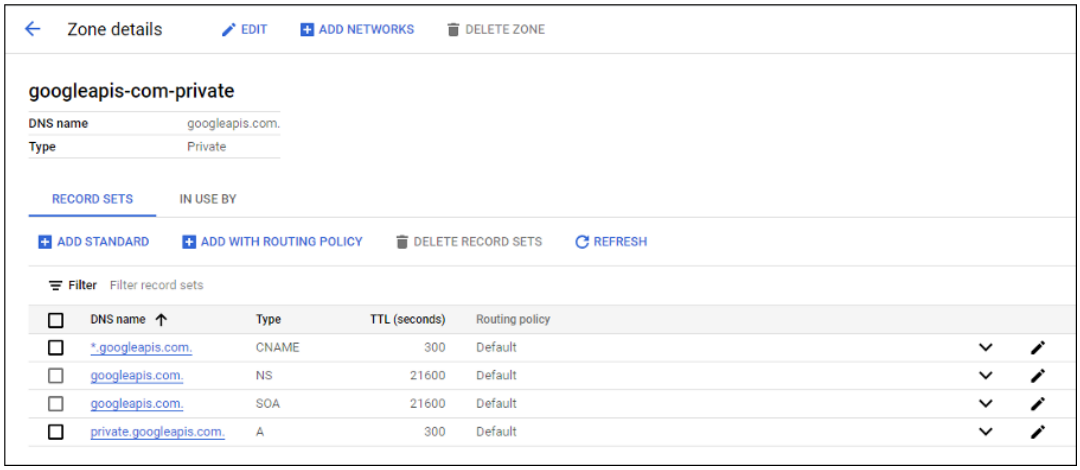
```
Services =
Service name: All services
<!--NeedCopy-->
```

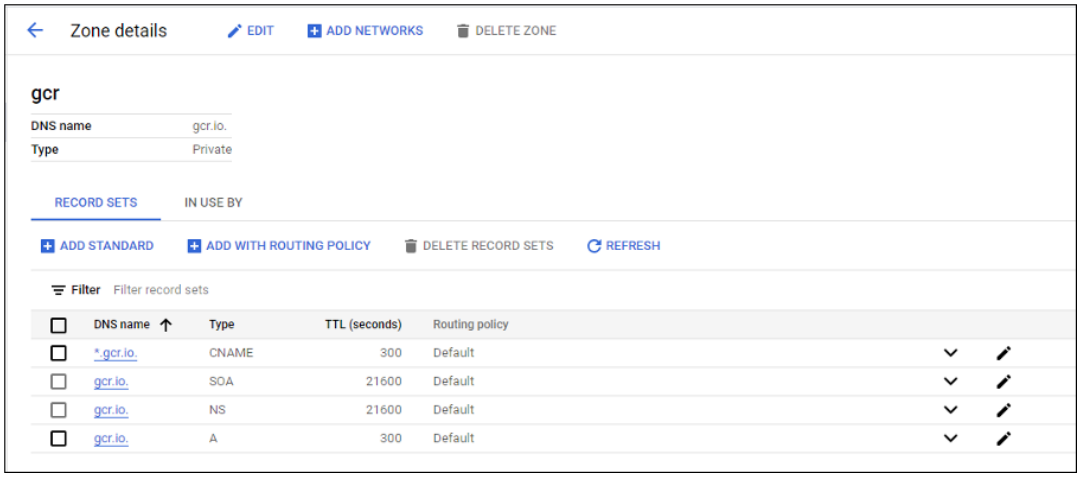
- Si vous utilisez un pool de travailleurs privés, ajoutez `UsePrivateWorkerPool` dans `CustomProperties`. Pour plus d'informations sur le pool de travailleurs privés, reportez-vous à la section Vue d'ensemble des pools privés.

Conditions requises pour créer un environnement sécurisé pour le trafic géré par GCP

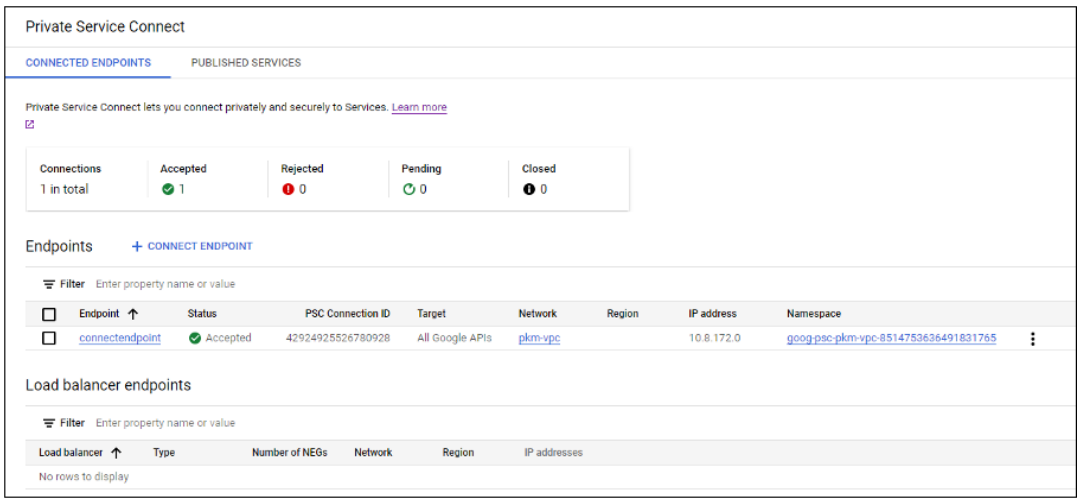
Les conditions requises pour créer un environnement sécurisé pour le trafic géré par GCP sont les suivantes :

- Assurez-vous que la connexion d'hébergement est en mode de maintenance lors de la mise à jour des propriétés personnalisées.
- Pour utiliser des pools de travailleurs privés, les modifications suivantes sont requises :
  - Pour un compte Citrix Cloud Service, ajoutez les rôles IAM suivants :
    - Compte de service Cloud Build
    - Administrateur d'instances Compute
    - Utilisateur du compte de service
    - Créateur de jetons de compte de service
    - Propriétaire du pool de travailleurs Cloud Build
  - Créez le compte Citrix Cloud Service dans le même projet que celui que vous utilisez pour créer une connexion d'hébergement.
  - Configurez les zones DNS pour **`private`**`.googleapis.com` et `gcr.io` comme décrit dans la section Configuration DNS.

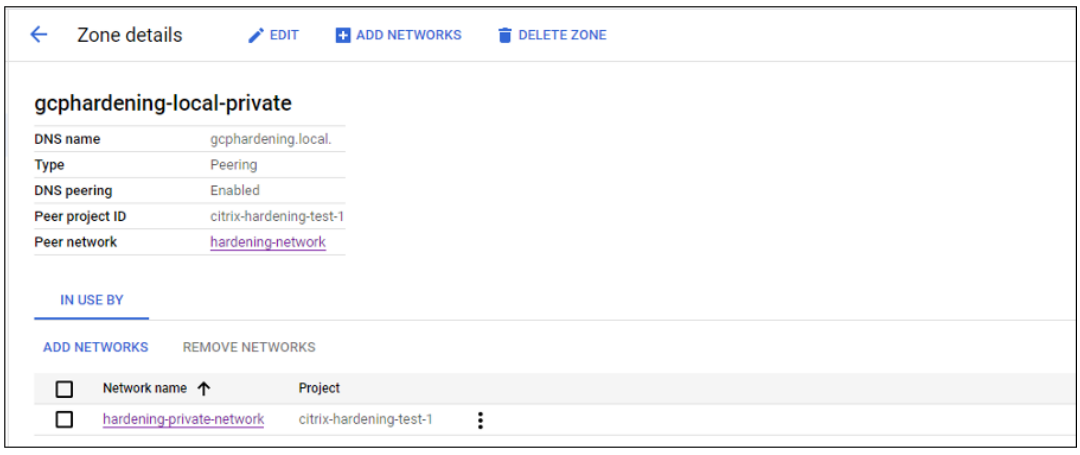




- Configurez la traduction d'adresses réseau (NAT) privée ou utilisez une connexion de service privée. Pour plus d'informations, consultez la section Accéder aux API Google via des points de terminaison.



- Si vous utilisez un VPC appairé, créez une zone Cloud DNS avec appairage au VPC appairé. Pour plus d'informations, consultez la section Créer une zone d'appairage.



- Dans les contrôles de service VPC, configurez des règles de sortie afin que les API et les

machines virtuelles puissent communiquer avec Internet. Les règles d'entrée sont facultatives. Par exemple :

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
<!--NeedCopy-->
```

Activer le pool de nœuds de calcul privé

Pour activer le pool de nœuds de calcul privé, définissez les propriétés personnalisées comme suit sur la connexion hôte :

1. Ouvrez une fenêtre PowerShell à partir de l'hôte Delivery Controller ou utilisez le SDK Remote PowerShell. Pour plus d'informations sur le Remote PowerShell SDK, reportez-vous à la section SDK et API.
2. Exécutez les commandes suivantes :
   a) `Add-PSSnapin citrix*`
   b) `cd XDHyp:\Connections\`
   c) `dir`
3. Copiez `CustomProperties` depuis la connexion vers un bloc-notes.
4. Ajoutez le paramètre de propriété `<Property xsi:type="StringProperty"Name="UsePrivateWorkerPool"Value="True"/>`. Par exemple :

```
```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance" xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation">
<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
   Value="True"/>
</CustomProperties>
<!--NeedCopy--> ```
```

5. Dans la fenêtre PowerShell, attribuez une variable aux propriétés personnalisées modifiées. Par exemple :
   `$customProperty = '&lt;CustomProperties...&lt;/CustomProperties&gt;'`.
6. Exécutez `$gcpServiceAccount = "&lt;ENTER YOUR SERVICE ACCOUNT EMAIL HERE&gt;"`.

 
```

7. Exécutez `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`.
8. Exécutez `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`.
9. Exécutez la commande suivante pour mettre à jour une connexion hôte existante :

```
Set-Item -PassThru -Path @('XDHyp:\Connections\<ENTER YOUR CONNECTION NAME HERE>') -SecurePassword $securePassword -UserName $gcpServiceAccount -CustomProperties $customProperty
<!--NeedCopy-->
```

Autorisations GCP requises

Cette section contient la liste complète des autorisations GCP. Utilisez l'ensemble complet d'autorisations indiqué dans la section pour que la fonctionnalité fonctionne correctement.

> **Remarque :**
>
> GCP apporte des modifications au comportement par défaut du service Cloud Build et à l'utilisation des comptes de service après le 29 avril 2024. Pour plus d'informations, consultez la page Modification d'un compte de service Cloud Build. Vos projets Google existants pour lesquels l'API Cloud Build a été activée avant le 29 avril 2024 ne sont pas concernés par cette modification. Toutefois, si vous souhaitez conserver le comportement existant du service Cloud Build après le 29 avril, vous pouvez créer ou appliquer la stratégie de l'organisation pour désactiver l'application des contraintes avant d'activer l'API. Si vous définissez la nouvelle stratégie d'organisation, vous pouvez toujours suivre les autorisations existantes dans cette section et les éléments marqués **Avant la modification du compte de service Cloud Build**. Si ce n'est pas le cas, suivez les autorisations existantes et les éléments marqués **Après la modification du compte de service Cloud Build**.

Création d'une connexion hôte

- Autorisations minimales requises pour le compte de service Citrix Cloud dans un projet de provisioning :

```
compute.instanceTemplates.list
compute.instances.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
```



```
<!--NeedCopy-->
```

Les rôles suivants définis par Google disposent des autorisations répertoriées ci-dessus :

- Administrateur informatique
- Utilisateur de Cloud Datastore

- Autorisations supplémentaires requises pour VPC partagé pour le compte de service Citrix Cloud dans un projet VPC partagé :

```
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.get
<!--NeedCopy-->
```

Les rôles suivants définis par Google disposent des autorisations répertoriées ci-dessus :

- Utilisateur de réseau Compute

Gestion de l'alimentation des machines virtuelles

Autorisations minimales requises pour le compte de service Citrix Cloud dans un projet de provisioning dans le cas où seulement des catalogues dont l'alimentation est gérée existent :

```
compute.instanceTemplates.list
compute.instances.list
compute.instances.get
compute.instances.reset
compute.instances.resume
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
compute.zoneOperations.get
<!--NeedCopy-->
```

Les rôles suivants définis par Google disposent des autorisations répertoriées ci-dessus :

- Administrateur informatique
- Utilisateur de Cloud Datastore

Création, mise à jour ou suppression de machines virtuelles

- Autorisations minimales requises pour le compte de service Citrix Cloud dans un projet de provisioning :

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
```



```
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
compute.networks.get
compute.resourcePolicies.use

<!--NeedCopy-->
```

Les rôles suivants définis par Google disposent des autorisations répertoriées ci-dessus :

- Administrateur informatique
- Administrateur de l'espace de stockage
- Éditeur Cloud Build
- Utilisateur du compte de service
- Utilisateur de Cloud Datastore

- Autorisations supplémentaires requises pour VPC partagé pour le compte de service Citrix Cloud dans un projet VPC partagé lors de la création d'une unité d'hébergement à l'aide de VPC et de sous-réseau depuis un projet VPC partagé :

```
compute.firewalls.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.get
```



```
compute.subnetworks.list
compute.subnetworks.use
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

Les rôles suivants définis par Google disposent des autorisations répertoriées ci-dessus :

- Utilisateur de réseau Compute
- Utilisateur de Cloud Datastore

- (Avant la modification du compte de service Cloud Build) : autorisations minimales requises pour le compte de service Cloud Build dans un projet Provisioning requis par le service Google Cloud Build lors du téléchargement du disque d'instructions de préparation vers MCS :
- (Après la modification du compte de service Cloud Build) : autorisations minimales requises pour le compte de service Cloud Compute dans un projet Provisioning requis par le service Google Cloud Build lors du téléchargement du disque d'instructions de préparation vers MCS :

```
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.images.get
compute.images.list
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.getSerialPortOutput
compute.instances.list
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
logging.logEntries.create
pubsub.topics.publish
resourcemanager.projects.get
source.repos.get
source.repos.list
```



```
storage.buckets.create
storage.buckets.get
storage.buckets.list
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

Les rôles suivants définis par Google disposent des autorisations répertoriées ci-dessus :

- Compte de service Cloud Build (après la modification du compte de service Cloud Build, il s'agit du compte de service Cloud Compute)
- Administrateur d'instances Compute
- Utilisateur du compte de service

- Autorisations minimales requises pour le compte de service Cloud Compute dans un projet de provisioning requis par le service Google Cloud Build lors du téléchargement du disque d'instructions de préparation vers MCS :

```
resourcemanager.projects.get
storage.objects.create
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

Les rôles suivants définis par Google disposent des autorisations répertoriées ci-dessus :

- Utilisateur de réseau Compute
- Utilisateur du compte de stockage
- Utilisateur de Cloud Datastore

- (Avant la modification du compte de service Cloud Build) : autorisations supplémentaires requises pour VPC partagé pour le compte de service Cloud Build dans un projet Provisioning requis par le service Google Cloud Build lors du téléchargement du disque d'instructions de préparation vers MCS :
- (Après la modification du compte de service Cloud Build) : autorisations supplémentaires requises pour VPC partagé pour le compte de service Cloud Build dans un projet Provisioning requis par le service Google Cloud Build lors du téléchargement du disque d'instructions de préparation vers MCS :

```
compute.firewalls.list
compute.networks.list
compute.subnetworks.list
compute.subnetworks.use
resourcemanager.projects.get
<!--NeedCopy-->
```


Les rôles suivants définis par Google disposent des autorisations répertoriées ci-dessus :

- Utilisateur de réseau Compute
- Utilisateur du compte de stockage
- Utilisateur de Cloud Datastore

- Autorisations supplémentaires requises pour Cloud Key Management Service (KMS) pour le compte de service Citrix Cloud dans un projet de provisioning :

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```

Les rôles suivants définis par Google disposent des autorisations répertoriées ci-dessus :

- Lecteur Compute KMS

Autorisations générales

Vous trouverez ci-dessous les autorisations du compte Citrix Cloud Service dans le projet Provisioning pour toutes les fonctionnalités prises en charge dans MCS. Ces autorisations offrent la meilleure compatibilité pour l'avenir :

```
resourcemanager.projects.get
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
```



```
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
compute.instances.updateSecurity
compute.instances.updateShieldedInstanceConfig
compute.instances.updateShieldedVmConfig
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
```



```
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
compute.disks.list
compute.instances.setServiceAccount
compute.networks.get
compute.networks.use
compute.networks.useExternalIp
iam.serviceAccounts.actAs
compute.resourcePolicies.use
<!--NeedCopy-->
```

Autres ressources

- Si vous êtes dans le processus de déploiement initial, consultez la section Créer des catalogues de machines.
- Pour obtenir des informations spécifiques à Google Cloud Platform (GCP), consultez la section Créer un catalogue Google Cloud Platform.

Informations supplémentaires

- Connexions et ressources
- Créer des catalogues de machines

Connexion à HPE Moonshot

June 27, 2024

La section Créer et gérer des connexions et des ressources décrit les assistants qui créent une connexion. Les informations suivantes couvrent les détails spécifiques à HPE Moonshot.

> **Remarque :**
>
> Avant de créer une connexion à HPE Moonshot, vous devez d'abord terminer la configuration de votre compte HPE. Voir Environnements de virtualisation HPE Moonshot.

Créer une connexion

Vous pouvez créer une connexion à HPE Moonshot à l'aide des outils suivants :

- Studio Web
- Commandes PowerShell

Créer une connexion à l'aide de Web Studio

1. Sur la page **Ajouter une connexion et des ressources**, sélectionnez **HPE Moonshot** comme type de connexion.
2. Entrez l'adresse de connexion de votre Moonshot iLO Chassis Manager. Vous pouvez utiliser une adresse IP, un nom d'hôte ou un nom de domaine complet pour l'adresse.
3. Entrez les informations d'identification administratives de votre châssis et un nom de connexion convivial.

La configuration de la connexion s'arrête dans l'une des situations suivantes :

- Citrix Virtual Apps and Desktops reçoit un certificat public signé par une autorité de certification contenant des erreurs : un message d'erreur s'affiche. Suivez les instructions qui s'affichent à l'écran pour résoudre le problème. Sinon, vous ne pourrez pas poursuivre la création de la connexion.
- Citrix Virtual Apps and Desktops reçoit un certificat privé signé par une autorité de certification. Une page d'avertissement apparaît. Comparez l'empreinte numérique reçue avec celle du serveur pour vérifier la validité du certificat. S'il est valide, sélectionnez **Certificat de confiance** et cliquez sur **OK** pour poursuivre la création de la connexion. Citrix Virtual Apps and Desktops fera ensuite confiance au certificat et stockera l'empreinte numérique pour une validation ultérieure.

Créer une connexion à l'aide de commandes PowerShell

Lorsque vous créez une connexion à l'aide de commandes PowerShell, fournissez les informations suivantes :

- IP : adresse IP du serveur HPE
- Nom d'utilisateur : nom d'utilisateur HPE
- Mot de passe : mot de passe HPE

Par exemple :

```
1 New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata @{
2  "Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false" }
```



```
3    -Path @("XDHyp:\Connections$connectionName") -Persist -PluginId "
        HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
        $UserName -sslthumbprint $SslThumbprint New-
        BrokerHypervisorConnection -HypHypervisorConnectionUid
        $HypervisorConnectionID
4  <!--NeedCopy-->
```

> **Remarque :**
>
> Le paramètre `sslthumbprint` est requis uniquement pour les certificats privés signés par une autorité de certification.

Validation du certificat et de l'empreinte numérique

Pour créer une connexion réussie à **HPE Moonshot**, le certificat ne doit pas contenir d'erreurs et l'empreinte numérique doit avoir une valeur correcte. Voici les cas d'utilisation liés à la validation du certificat et de l'empreinte numérique :

- Le certificat public signé par une autorité de certification contient des erreurs. La connexion n'est pas créée avec succès. Consultez les détails de l'erreur et résolvez le problème.
- Certificat public signé par une autorité de certification sans erreur. La connexion est créée avec succès et la valeur `SslThumbprints` est **Null**.
- Certificat privé signé par une autorité de certification sans erreur ni valeur `sslthumbprint`. La connexion est créée avec succès avec une valeur `SslThumbprints` correcte.
- Certificat privé signé par une autorité de certification avec une valeur d'empreinte numérique incorrecte. La connexion n'est pas créée avec succès.
- Certificat privé signé par une autorité de certification sans erreur. La connexion est créée avec succès. La valeur `SSlThumbprints` est **Null** lors de la création de la connexion. La valeur `SSlThumbprints` est mise à jour vers une valeur par le service du site.

Gérer les connexions

Cette section explique comment gérer les connexions :

- Résoudre les problèmes de certificat à l'aide de Web Studio
- Mettre à jour la valeur de l'empreinte numérique à l'aide de commandes PowerShell

Résoudre les problèmes liés aux certificats

Citrix Virtual Apps and Desktops bloque une connexion HPE Moonshot lorsque des problèmes de certificat surviennent, vous empêchant ainsi de fournir et de gérer les charges de travail sur les nœuds HPE

Moonshot associés. Une icône d'erreur apparaît à côté de la connexion dans la liste des **connexions hôtes**. Consultez le tableau suivant pour connaître les problèmes spécifiques et les solutions.

Problème	Solution
Une erreur de certificat se produit sur le certificat public signé par une autorité de certification	Cliquez sur la connexion et sélectionnez l'onglet **Dépannage**. Consultez les détails de l'erreur et résolvez le problème.
Le certificat reçu est privé, signé par une autorité de certification, ou a expiré.	Modifiez la connexion hôte pour mettre à jour l'empreinte numérique du certificat. Détails des étapes 1. Sélectionnez la connexion et cliquez sur **Modifier la connexion**. 1. Sur la page **Propriétés de la connexion**, cliquez sur **Modifier les paramètres**. 1. Entrez le mot de passe pour vous connecter au châssis HPE Moonshot, puis cliquez sur **Enregistrer**. 1. Sur la page **Avertissement** qui apparaît, comparez l'empreinte numérique reçue avec celle du serveur pour vérifier la validité du certificat. 1. Si elles sont identiques, sélectionnez **Approuver le certificat**, puis cliquez sur **OK**.

Mettre à jour la valeur de l'empreinte

Après avoir créé la connexion, vous pouvez mettre à jour la valeur de l'empreinte numérique d'une connexion à l'aide de la commande PowerShell `Set-Item`. Par exemple, exécutez les commandes suivantes :

1. Obtenez les détails d'une connexion. Par exemple :

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```

2. Mettez à jour la valeur de l'empreinte numérique. Par exemple :


```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
    Administrator -SslThumbprint
   xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
<!--NeedCopy-->
```

3. Vérifiez la valeur de l'empreinte numérique mise à jour. Par exemple :

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```

> **Remarque :**
>
> La mise à jour échoue si vous saisissez une valeur d'empreinte numérique incorrecte dans la commande `Set-Item`.

Autres ressources

- Si vous êtes dans le processus de déploiement initial, consultez la section Créer des catalogues de machines.
- Pour obtenir des informations spécifiques à HPE Moonshot, consultez Créer un catalogue de machines HPE Moonshot

Informations supplémentaires

- Connexions et ressources
- Créer des catalogues de machines

Connexion à Microsoft Azure

June 27, 2024

> **Remarque :**
>
> Depuis juillet 2023, Microsoft a renommé Azure Active Directory (Azure AD) Microsoft Entra ID. Dans ce document, toute occurrence de l'appellation Azure Active Directory, Azure AD ou de l'acronyme AAD fait désormais référence à Microsoft Entra ID.

La section Créer et gérer des connexions et des ressources décrit les assistants qui créent une connexion. Les informations suivantes couvrent les détails spécifiques aux environnements de cloud Azure Resource Manager.

> **Remarque :**
>
> Avant de créer une connexion à Microsoft Azure, vous devez terminer la configuration de votre compte Azure en tant qu'emplacement de ressources. Voir Environnements de cloud Microsoft Azure Resource Manager.

Créer des principaux de service et des connexions

Avant de créer des connexions, vous devez configurer les principaux de service que les connexions utilisent pour accéder aux ressources Azure. Vous pouvez créer une connexion de deux manières :

- Créer ensemble un principal de service et une connexion à l'aide de Web Studio
- Créer une connexion à l'aide d'un principal de service créé précédemment

Cette section explique comment effectuer les tâches suivantes :

- Créer un principal de service et une connexion à l'aide de Web Studio
- Créer un principal de service à l'aide de PowerShell
- Obtenir le secret d'application dans Azure
- Créer une connexion à l'aide d'un principal de service existant

Considérations

- Citrix recommande d'utiliser le principal du service avec un rôle de contributeur. Consultez toutefois la section Autorisations minimales pour obtenir la liste des autorisations minimales.
- Lorsque vous créez la première connexion, Azure vous invite à leur accorder les autorisations nécessaires. Vous devrez toujours vous authentifier pour les futures connexions, mais Azure mémorise votre accord préalable et n'affiche plus l'invite.
- Les comptes utilisés pour l'authentification doivent être des co-administrateurs de l'abonnement.
- Le compte utilisé pour l'authentification doit être un membre du répertoire de l'abonnement. Il existe deux types de comptes : « Professionnel ou école » et « compte Microsoft personnel ». Voir CTX219211 pour plus de détails.
- Bien que vous puissiez utiliser un compte Microsoft existant en l'ajoutant en tant que membre du répertoire de l'abonnement, cela peut entraîner des complications si un accès invité à l'une des ressources du répertoire a précédemment été accordé à l'utilisateur. Dans ce cas, le répertoire peut contenir une entrée fictive qui ne lui accorde pas les autorisations nécessaires, et une erreur est renvoyée.

Corrigez cela en supprimant les ressources du répertoire et en les rajoutant explicitement. Soyez toutefois prudent, car cela a des effets indésirables sur d'autres ressources auxquelles ce compte peut accéder.

- Il existe un problème connu dans lequel certains comptes sont détectés en tant qu'invités du répertoire alors qu'ils en sont membres. Des configurations comme celle-ci se produisent généralement avec d'anciens comptes de répertoire établis. Solution : ajoutez un compte au répertoire, qui prend la valeur d'appartenance appropriée.
- Les groupes de ressources sont des conteneurs de ressources qui peuvent contenir des ressources provenant de régions autres que leur propre région. Cela peut porter à confusion si vous vous attendez à ce que les ressources affichées dans la région d'un groupe de ressources soient disponibles.
- Assurez-vous que votre réseau et sous-réseau sont suffisamment grands pour héberger le nombre de machines dont vous avez besoin. Cela nécessite une démarche prospective, mais Microsoft vous permet de spécifier les valeurs correctes, en fournissant des conseils sur la capacité de l'espace d'adressage.

Créer un principal de service et une connexion à l'aide de Web Studio

> **Important :**
>
> Cette fonctionnalité n'est pas encore disponible pour les abonnements Azure Chine.

Avec Web Studio, vous pouvez créer à la fois un principal de service et une connexion dans un seul flux de travail. Les principaux de service permettent aux connexions d'accéder aux ressources Azure. Lorsque vous vous authentifiez auprès d'Azure pour créer un principal de service, une application est enregistrée dans Azure. Une clé secrète (appelée clé secrète client ou secret d'application) est créée pour l'application enregistrée. L'application enregistrée (une connexion dans ce cas) utilise la clé secrète client pour s'authentifier auprès d'Azure AD.

Avant de commencer, assurez-vous de remplir les conditions préalables suivantes :

- Vous disposez d'un compte utilisateur dans le locataire Azure Active Directory de votre abonnement.
- Le compte d'utilisateur Azure AD est également un co-administrateur pour l'abonnement Azure que vous utiliserez pour les ressources de provisioning.
- Vous disposez d'autorisations d'administrateur global, d'administrateur d'application ou de développeur d'applications pour l'authentification. Ces autorisations peuvent être révoquées après la création d'une connexion hôte. Pour plus d'informations sur les rôles, consultez la section Rôles intégrés d'Azure AD.

Utilisez l'assistant **Ajouter une connexion et des ressources** pour créer simultanément un principal de service et une connexion :

1. Sur la page **Connexion**, sélectionnez **Créer une connexion**, le type de connexion **Microsoft Azure** et votre environnement Azure.
2. Sélectionnez les outils à utiliser pour créer les machines virtuelles, puis cliquez sur **Suivant**.
3. Sur la page **Détails de la connexion**, entrez votre ID d'abonnement Azure et un nom pour la connexion. Lorsque vous entrez l'ID d'abonnement, le bouton **Créer nouveau** est activé.

   > **Remarque :**
   >
   > Le nom de la connexion peut contenir entre 1 et 64 caractères, et ne peut pas contenir uniquement des espaces ou les caractères `\/;:#.*?=<>|[]{ } "'()'`.

4. Sélectionnez **Créer**, puis entrez le nom d'utilisateur et le mot de passe du compte Azure Active Directory.
5. Sélectionnez **Se connecter**.
6. Sélectionnez **Accepter** pour donner à Citrix Virtual Apps and Desktops les autorisations répertoriées. Citrix Virtual Apps and Desktops crée un principal de service qui lui permet de gérer les ressources Azure pour le compte d'utilisateur spécifié.
7. Une fois que vous avez sélectionné **Accepter**, vous revenez à la page **Connexion** de l'assistant.

   > **Remarque :**
   >
   > Une fois que vous vous êtes authentifié auprès d'Azure, les boutons **Créer** et **Utiliser existant** disparaissent. Le texte **Connexion établie avec succès** apparaît, avec une coche verte indiquant la connexion réussie à votre abonnement Azure.

8. Sur la page **Détails de la connexion**, sélectionnez **Suivant**.

   > **Remarque :**
   >
   > Vous ne pouvez pas passer à la page suivante tant que vous ne vous êtes pas correctement authentifié auprès d'Azure et n'avez pas consenti à accorder les autorisations requises.

9. Configurez les ressources pour la connexion. Les ressources comprennent la région et le réseau.
   - Sur la page **Région**, sélectionnez une région.
   - Sur la page **Réseau**, procédez comme suit :
     - tapez un nom de ressource comportant entre 1 et 64 caractères pour vous aider à identifier la combinaison région/réseau. Un nom de ressource ne peut contenir que des espaces vides ni les caractères `\/;:#.*?=<>|[]{ } "'()'`.
     - Sélectionnez une paire réseau virtuel/groupe de ressources (si vous avez plusieurs réseaux virtuels avec le même nom, le couplage du nom du réseau avec le groupe de

ressources fournit des combinaisons uniques). Si la région que vous avez sélectionnée sur la page précédente ne dispose pas de réseaux virtuels, retournez à cette page et sélectionnez une région contenant des réseaux virtuels.

10. Sur la page **Résumé**, affichez un résumé des paramètres et sélectionnez **Terminer** pour terminer votre configuration.

Afficher l'ID de l'application Après avoir créé une connexion, vous pouvez voir l'ID de l'application que la connexion utilise pour accéder aux ressources Azure.

Dans la liste **Ajouter une connexion et des ressources**, sélectionnez la connexion pour afficher les détails. L'onglet **Détails** affiche l'ID de l'application.

Créer un principal de service à l'aide de PowerShell

Pour créer un principal de service à l'aide de PowerShell, connectez-vous à votre abonnement Azure Resource Manager et utilisez les applets de commande PowerShell fournies dans les sections suivantes.

Assurez-vous que les éléments suivants sont prêts :

- **SubscriptionId :** `SubscriptionID` Azure Resource Manager pour l'abonnement sur lequel vous souhaitez provisionner les VDA.
- **ActiveDirectoryID :** ID de locataire de l'application que vous avez enregistrée auprès d'Azure AD.
- **ApplicationName :** nom de l'application à créer dans Azure AD.

Les étapes détaillées sont les suivantes :

Connectez-vous à votre abonnement Azure Resource Manager.

```
1 `Connect-AzAccount`
```

1. Sélectionnez l'abonnement Azure Resource Manager sur lequel vous souhaitez créer le principal de service.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

2. Créez l'application dans votre locataire AD.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. Créez un principal de service.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```


4. Attribuez un rôle au principal de service.

```
New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
 $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
```

5. Dans la sortie de la fenêtre de la console PowerShell, notez la valeur ApplicationId. Vous fournissez cet ID lors de la création de la connexion hôte.

Obtenir le secret d'application dans Azure

Pour créer une connexion à l'aide d'un principal de service existant, vous devez d'abord obtenir l'ID d'application et le code secret du principal du service sur le portail Azure.

Les étapes détaillées sont les suivantes :

1. Obtenez l'**ID de l'application** dans Web Studio ou à l'aide de PowerShell.
2. Connectez-vous au portail Azure.
3. Dans Azure, sélectionnez **Azure Active Directory**.
4. Dans **Inscriptions des applications** dans Azure AD, sélectionnez votre application.
5. Accédez à **Certificats et secrets**.
6. Cliquez sur **Clés secrètes client**.

Créer une connexion à l'aide d'un principal de service existant

Si vous disposez déjà d'un principal de service, vous pouvez l'utiliser pour créer une connexion à l'aide de Web Studio.

Assurez-vous que les éléments suivants sont prêts :

- ID d'abonnement
- ID Active Directory (ID du locataire)
- ID de l'application
- Secret d'application

  Pour plus d'informations, consultez la section Obtenir le secret d'application.
- Date d'expiration du secret

Les étapes détaillées sont les suivantes :

Dans l'assistant **Ajouter une connexion et des ressources** :

1. Sur la page **Connexion**, sélectionnez **Créer une connexion**, le type de connexion **Microsoft Azure** et votre environnement Azure.

2. Sélectionnez les outils à utiliser pour créer les machines virtuelles, puis cliquez sur **Suivant**.
3. Sur la page **Détails de la connexion**, entrez votre ID d'abonnement Azure et un nom pour la connexion.

   > **Remarque :**
   >
   > Le nom de la connexion peut contenir entre 1 et 64 caractères, et ne peut pas contenir uniquement des espaces ou les caractères `\/;:#.*?=<>|[]{ } "'()'`.

4. Sélectionnez **Utiliser existant**. Dans la fenêtre **Détails du principal de service existant**, entrez les paramètres suivants pour le principal de service existant. Une fois que vous avez saisi les détails, le bouton **Enregistrer** est activé. Sélectionnez **Save**. Vous ne pouvez pas avancer au-delà de cette page tant que vous n'avez pas fourni de détails valides.

   - **ID d'abonnement**. Saisissez votre identifiant d'abonnement Azure. Pour obtenir votre ID d'abonnement, connectez-vous au portail Azure et accédez à **Abonnements > Vue d'ensemble**.
   - **ID Active Directory** (ID du locataire). Entrez l'ID du répertoire (locataire) de l'application que vous avez enregistrée auprès d'Azure AD.
   - **ID de l'application**. Entrez l'ID d'application (client) de l'application que vous avez enregistrée auprès d'Azure AD.
   - **Secret d'application**. Créez une clé secrète (secret client). L'application enregistrée utilise la clé pour s'authentifier auprès d'Azure AD. Nous vous recommandons de modifier régulièrement les clés pour des raisons de sécurité. Assurez-vous d'enregistrer la clé car vous ne pouvez pas la récupérer ultérieurement.
   - **Date d'expiration du secret**. Entrez la date après laquelle le secret d'application expire. Vous recevez une alerte sur la console avant l'expiration de la clé secrète. Toutefois, si la clé secrète expire, des erreurs s'affichent.

     > **Remarque :**
     >
     > Pour des raisons de sécurité, la période d'expiration ne peut pas dépasser deux ans.

   - **URL d'authentification**. Ce champ est automatiquement renseigné et n'est pas modifiable.
   - **URL de gestion**. Ce champ est automatiquement renseigné et n'est pas modifiable.
   - **Suffixe de stockage**. Ce champ est automatiquement renseigné et n'est pas modifiable.

     L'accès aux points de terminaison suivants est requis pour créer un catalogue MCS dans Azure. L'accès à ces points de terminaison optimise la connectivité entre votre réseau et le portail Azure et ses services.

- URL d'authentification : https://login.microsoftonline.com/.
- URL de gestion : https://management.azure.com/. Il s'agit d'une URL de demande pour les API du fournisseur Azure Resource Manager. Le point de terminaison dédié à la gestion dépend de l'environnement. Par exemple, pour Azure Global, il s'agit de https://management.azure.com/, et pour Azure US Government, il s'agit de https://management.usgovcloudapi.net/.
- Suffixe de stockage : `https://*.core.windows.net/`. Ce (*) est un caractère générique pour le suffixe de stockage. Par exemple, `https://demo.table.core.windows.net/`.

5. Après avoir sélectionné **Enregistrer**, vous revenez à la page **Détails de la connexion** . Sélectionnez **Suivant** pour passer à la page suivante.
6. Configurez les ressources pour la connexion. Les ressources comprennent la région et le réseau.
   - Sur la page **Région**, sélectionnez une région.
   - Sur la page **Réseau**, procédez comme suit :
     - tapez un nom de ressource comportant entre 1 et 64 caractères pour vous aider à identifier la combinaison région/réseau. Un nom de ressource ne peut contenir que des espaces vides ni les caractères `\/;:#.*?=<>|[]{ } "'()'`.
     - Sélectionnez une paire réseau virtuel/groupe de ressources (si vous avez plusieurs réseaux virtuels avec le même nom, le couplage du nom du réseau avec le groupe de ressources fournit des combinaisons uniques). Si la région que vous avez sélectionnée sur la page précédente ne dispose pas de réseaux virtuels, retournez à cette page et sélectionnez une région contenant des réseaux virtuels.
7. Sur la page **Résumé**, affichez un résumé des paramètres et sélectionnez **Terminer** pour terminer votre configuration.

Gérer les principaux de service et les connexions

Cette section explique comment gérer les principaux de service et les connexions :

- Configurer les paramètres de limitation d'Azure
- Activer le partage d'images dans Azure
- Ajouter des locataires partagés à une connexion à l'aide de la configuration complète
- Mettre en œuvre le partage d'images à l'aide de PowerShell
- Gérer le secret d'application et la date d'expiration du secret

Configurer les paramètres de limitation d'Azure

Azure Resource Manager limite les demandes d'abonnements et de locataires, en acheminant le trafic en fonction de limites définies, adaptées aux besoins spécifiques du fournisseur. Pour plus d'informations, consultez la section Limitation des demandes Resource Manager sur le site Microsoft. Il existe des limites pour les abonnements et les locataires, où la gestion de nombreuses machines peut devenir problématique. Par exemple, un abonnement contenant un grand nombre de machines peut rencontrer des problèmes de performances liés aux opérations d'alimentation.

> **Conseil :**
>
> Pour plus d'informations, consultez la section Amélioration des performances Azure avec Machine Creation Services.

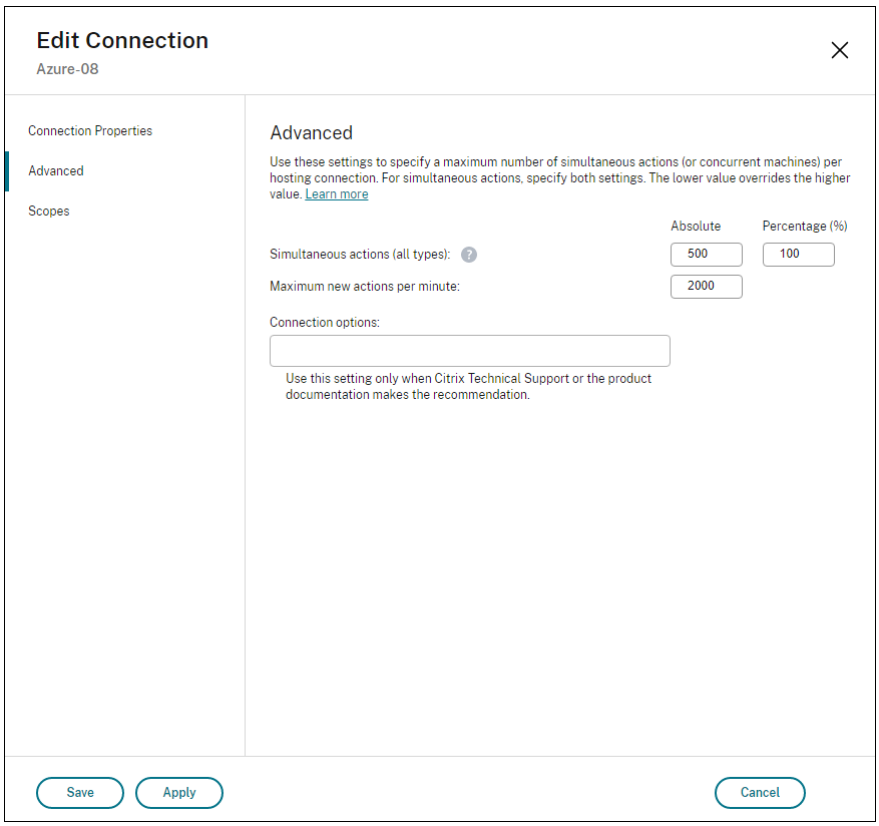
Pour aider à atténuer ces problèmes, vous pouvez supprimer la limitation interne de MCS pour utiliser une plus grande partie du quota de demandes disponible d'Azure.

Nous recommandons les paramètres optimaux suivants lors de la mise hors/sous tension de machines virtuelles dans les abonnements volumineux, par exemple ceux contenant 1,000 machines virtuelles :

- Opérations simultanées absolues : 500
- Nombre maximal de nouvelles opérations par minute : 2000
- Nombre maximal d'opérations simultanées : 500

Utilisez Web Studio pour configurer les opérations Azure pour une connexion Azure donnée :

1. Dans Web Studio, sélectionnez **Hébergement** dans le volet de gauche.
2. Sélectionnez la connexion.
3. Dans l'assistant **Modifier la connexion**, sélectionnez **Avancé**.
4. Dans la page **Avancé**, utilisez les options de configuration pour spécifier le nombre d'actions simultanées, le nombre maximal de nouvelles actions par minute et toutes les options de connexion supplémentaires.



MCS prend en charge 500 opérations simultanées maximum par défaut. Vous pouvez également utiliser le SDK Remote PowerShell distant pour définir le nombre maximal d'opérations simultanées.

Utilisez la propriété **PowerShell**, `MaximumConcurrentProvisioningOperations`, pour spécifier le nombre maximal d'opérations de provisioning Azure simultanées. Lorsque vous utilisez cette propriété, prenez en compte des éléments suivants :

- La valeur par défaut de `MaximumConcurrentProvisioningOperations` est 500.
- Configurez le paramètre `MaximumConcurrentProvisioningOperations` à l'aide de la commande PowerShell `Set-item`.

Activer le partage d'images dans Azure

Lorsque vous créez ou mettez à jour des catalogues de machines, vous pouvez sélectionner des images partagées à partir de différents locataires et abonnements Azure (partagées via la galerie Azure Compute Gallery). Pour activer le partage d'images au sein des locataires ou entre eux, vous devez définir les paramètres nécessaires dans Azure :

- Partager des images au sein d'un locataire (entre abonnements)
- Partager des images entre locataires

Partager des images au sein d'un locataire (entre abonnements) Pour sélectionner une image dans Azure Compute Gallery qui appartient à un autre abonnement, l'image doit être partagée avec le service principal (SPN) de cet abonnement.

Par exemple, s'il existe un principal de service (SPN 1) configuré dans Studio comme suit :

Principal de service : SPN 1

Abonnement : abonnement 1

Locataire : locataire 1

L'image se trouve dans un abonnement différent, qui est configuré dans Studio comme suit :

Abonnement : abonnement 2

Locataire : locataire 1

Si vous souhaitez partager l'image de l'abonnement 2 avec l'abonnement 1 (SPN 1), accédez à l'abonnement 2 et partagez le groupe de ressources avec SPN1.

L'image doit être partagée avec un autre SPN à l'aide du contrôle d'accès basé sur les rôles Azure (RBAC). Azure RBAC est le système d'autorisation utilisé pour gérer l'accès aux ressources Azure. Pour plus d'informations sur Azure RBAC, consultez le document Microsoft Qu'est-ce que le contrôle d'accès en fonction du rôle Azure (RBAC Azure). Pour accorder l'accès, vous attribuez des rôles aux principaux de service au niveau du groupe de ressources avec le rôle Contributeur. Pour attribuer des rôles Azure, vous devez disposer d'une autorisation `Microsoft.Authorization/roleAssignments/write`, telle que le rôle Administrateur de l'accès utilisateur ou Propriétaire. Pour plus d'informations sur le partage d'images avec un autre SPN, consultez le document Microsoft Attribuer des rôles Azure à l'aide du portail Azure.

Pour plus d'informations sur la sélection d'une image provenant d'un autre abonnement à l'aide de commandes PowerShell, consultez la section Sélectionner une image provenant d'un autre abonnement.

Partager des images entre locataires Pour partager des images entre locataires avec Azure Compute Gallery, créez un enregistrement d'application.

Par exemple, s'il y a deux locataires (Tenant 1 et Tenant 2) et que vous souhaitez partager votre galerie d'images avec Tenant 1, alors :

1. Créez une demande d'enregistrement pour Tenant 1. Pour plus d'informations, voir Créer l'enregistrement de l'application.
2. Donnez à Tenant 2 l'accès à l'application en demandant une connexion à l'aide d'un navigateur. Remplacez `Tenant2 ID` par l'identifiant de Tenant 1. Remplacez `Application (client) ID` par l'ID de l'application de l'enregistrement d'application que vous avez créé. Lorsque

vous avez terminé d'effectuer les remplacements, collez l'URL dans un navigateur et suivez les instructions de connexion pour vous connecter à Tenant 2. Par exemple :

```
https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
    client_id=<Application (client) ID>&response_type=code&
    redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
<!--NeedCopy-->
```

Pour plus d'informations, consultez la section Donner accès à Tenant 2.

3. Donnez à l'application l'accès au groupe de ressources Tenant 2. Connectez-vous en tant que Tenant 2 et autorisez l'enregistrement d'application à accéder au groupe de ressources contenant l'image de la galerie. Pour plus d'informations, consultez Authentifier les demandes auprès des locataires.

Pour créer un catalogue à partir d'une image provenant d'un autre locataire à l'aide de commandes PowerShell :

1. Mettre à jour les propriétés personnalisées de la connexion d'hébergement avec des ID de locataire partagés.
2. Sélectionner une image provenant d'un autre locataire.

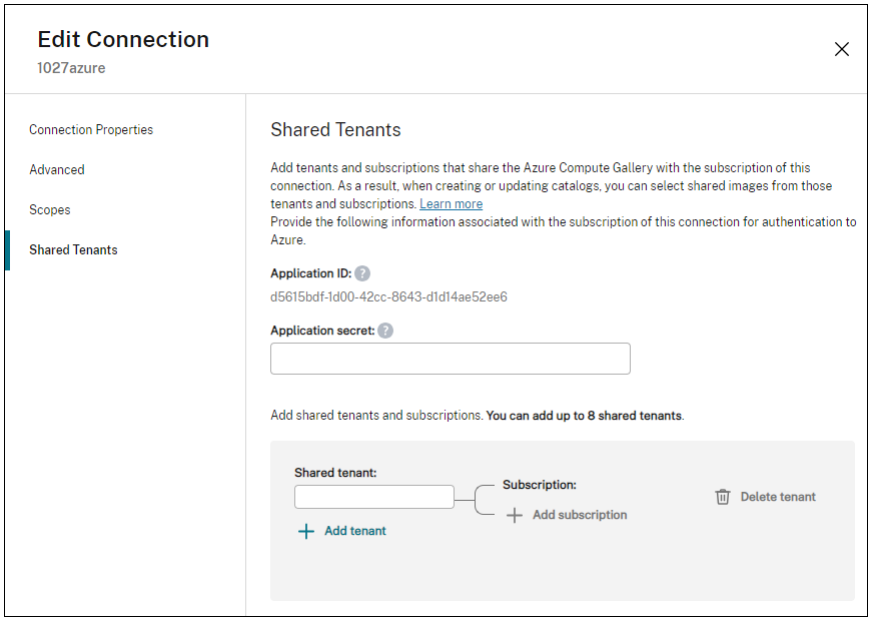
Ajouter des locataires partagés à une connexion à l'aide de la configuration complète

Lorsque vous créez ou mettez à jour des catalogues de machines dans Web Studio, vous pouvez sélectionner des images partagées à partir de différents locataires et abonnements Azure (partagées via la galerie Azure Compute Gallery). Cette fonctionnalité exige que vous fournissiez des informations partagées sur les locataires et les abonnements pour les connexions hôtes associées.

> **Remarque :**
>
> Vérifiez que vous avez configuré les paramètres nécessaires dans Azure pour permettre le partage d'images entre les locataires. Pour plus d'informations, consultez la section Partager des images entre les locataires.

Pour établir une connexion, procédez comme suit :

1. Dans Web Studio, sélectionnez **Hébergement** dans le volet de gauche.
2. Sélectionnez la connexion, puis sélectionnez **Modifier la connexion** dans le volet Actions.



3. Dans **Locataires partagés**, procédez comme suit :

   - Fournissez l'ID d'application et le secret d'application associés à l'abonnement de la connexion. Citrix Virtual Apps and Desktops utilise ces informations pour s'authentifier auprès d'Azure AD.
   - Ajoutez des locataires et des abonnements qui partagent Azure Compute Gallery avec l'abonnement de la connexion. Vous pouvez ajouter jusqu'à huit locataires partagés et huit abonnements pour chaque locataire.

4. Lorsque vous avez terminé, sélectionnez **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou sélectionnez **OK** pour appliquer les modifications et fermer la fenêtre.

Mettre en œuvre le partage d'images à l'aide de PowerShell

Cette section décrit les processus à suivre pour le partage d'images à l'aide de PowerShell :

- Sélectionner une image provenant d'un autre abonnement
- Mettre à jour les propriétés personnalisées de la connexion d'hébergement avec des ID de locataire partagés
- Sélectionner une image provenant d'un autre locataire

Sélectionner une image provenant d'un autre abonnement Vous pouvez sélectionner une image dans Azure Compute Gallery qui appartient à un abonnement partagé différent dans le même locataire Azure pour créer et mettre à jour des catalogues MCS à l'aide de commandes PowerShell.

1. Citrix crée un nouveau dossier d'abonnement partagé appelé `sharedsubscription` dans le dossier racine de l'unité d'hébergement.
2. Répertoriez tous les abonnements partagés d'un client.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.
    folder"
<!--NeedCopy-->
```

3. Sélectionnez un abonnement partagé, puis répertoriez tous les groupes de ressources partagés de cet abonnement partagé.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription"
<!--NeedCopy-->
```

4. Sélectionnez un groupe de ressources, puis répertoriez toutes les galeries de ce groupe de ressources.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\ xyz.resourcegroup"
<!--NeedCopy-->
```

5. Sélectionnez une galerie, puis répertoriez toutes les définitions d'images de cette galerie.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\testgallery.gallery"
<!--NeedCopy-->
```

6. Sélectionnez une définition d'image, puis répertoriez toutes les versions d'image de cette définition d'image.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\sigtestdef.
    imagedefinition"
<!--NeedCopy-->
```

7. Créez et mettez à jour un catalogue MCS à l'aide des éléments suivants :

   - Groupe de ressources
   - Galerie
   - Définition de l'image de la galerie
   - Version d'image de la galerie

   Pour plus d'informations sur la création d'un catalogue à l'aide du SDK Remote PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Mettre à jour les propriétés personnalisées de la connexion d'hébergement avec des ID de locataire partagés Utilisez `Set-Item` pour mettre à jour les propriétés personnalisées de connexion d'hébergement avec des ID de locataire et des identifiants d'abonnement partagés. Ajoutez une propriété `SharedTenants` dans `CustomProperties`. Le format de `Shared Tenants` est le suivant :

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
 ,{
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
 ]
<!--NeedCopy-->
```

Par exemple :

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
   citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
   /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
   123`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
   =`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
   Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
   core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
   " />
<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"`[
    {
  'Tenant':'123abc', 'Subscriptions':['345', '567']  }
  ]`"` />
</CustomProperties>"
-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "
   advc345" -SecurePassword
$psd
<!--NeedCopy-->
```

> **Remarque :**
>
> Vous pouvez ajouter plusieurs locataires. Chaque locataire peut avoir plusieurs abonnements.

Sélectionner une image provenant d'un autre locataire Vous pouvez sélectionner une image dans Azure Compute Gallery qui appartient à un autre locataire Azure pour créer et mettre à jour des catalogues MCS à l'aide de commandes PowerShell.

1. Citrix crée un nouveau dossier d'abonnement partagé appelé `sharedsubscription` dans le dossier racine de l'unité d'hébergement.

2. Répertoriez tous les abonnements partagés.

```
Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
<!--NeedCopy-->
```

3. Sélectionnez un abonnement partagé, puis répertoriez tous les groupes de ressources partagés de cet abonnement partagé.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription
<!--NeedCopy-->
```

4. Sélectionnez un groupe de ressources, puis répertoriez toutes les galeries de ce groupe de ressources.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\ xyz.resourcegroup
<!--NeedCopy-->
```

5. Sélectionnez une galerie, puis répertoriez toutes les définitions d'images de cette galerie.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery
<!--NeedCopy-->
```

6. Sélectionnez une définition d'image, puis répertoriez toutes les versions d'image de cette définition d'image.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
    imagedefinition
<!--NeedCopy-->
```

7. Créez et mettez à jour un catalogue MCS à l'aide des éléments suivants :

   - Groupe de ressources
   - Galerie
   - Définition de l'image de la galerie
   - Version d'image de la galerie

   Pour plus d'informations sur la création d'un catalogue à l'aide du SDK Remote PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Gérer le secret d'application et la date d'expiration du secret

Veillez à modifier le secret de l'application pour une connexion avant son expiration. Vous recevez une alerte sur Studio Web avant l'expiration de la clé secrète.

Créer un secret d'application dans Azure Vous pouvez créer un secret d'application pour une connexion via le portail Azure.

1. Sélectionnez **Azure Active Directory**.
2. Dans **Inscriptions des applications** dans Azure AD, sélectionnez votre application.
3. Accédez à **Certificats et secrets**.
4. Cliquez sur **Clés secrètes client > Nouvelle clé secrète client**.
5. Fournissez une description du secret et spécifiez une durée. Lorsque vous avez terminé, sélectionnez **Ajouter**.

   > **Remarque :**
   >
   > Veillez à enregistrer le secret client car vous ne pouvez pas le récupérer ultérieurement.

6. Copiez la valeur du secret client et la date d'expiration.
7. Dans Web Studio, modifiez la connexion correspondante et remplacez le contenu du champ **Secret de l'application** et **Date d'expiration du secret** par la valeur que vous avez copiée.

Modifier la date d'expiration du secret Vous pouvez utiliser Studio Web pour ajouter ou modifier la date d'expiration du secret d'application utilisé.

1. Dans l'assistant **Ajouter une connexion et des ressources**, cliquez avec le bouton droit sur une connexion, puis cliquez sur **Modifier la connexion**.
2. Sur la page **Propriétés de la connexion**, cliquez sur **Date d'expiration du secret** pour ajouter ou modifier la date d'expiration du secret d'application utilisé.

Autorisations Azure requises

Cette section contient les autorisations minimales et générales requises pour Azure.

Autorisations minimales

Les autorisations minimales offrent un meilleur contrôle de la sécurité. Toutefois, les nouvelles fonctionnalités qui nécessitent des autorisations supplémentaires échouent si seules des autorisations minimales sont utilisées.

Création d'une connexion hôte Ajoutez une nouvelle connexion hôte à l'aide des informations obtenues auprès d'Azure.

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
<!--NeedCopy-->
```

Gestion de l'alimentation des machines virtuelles Mettez les instances de machine sous tension ou hors tension.

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
<!--NeedCopy-->
```

Création, mise à jour ou suppression de machines virtuelles Créez un catalogue de machines, puis ajoutez, supprimez, mettez à jour des machines et supprimez le catalogue de machines.

Voici la liste des autorisations minimales requises lorsque l'image principale est un disque géré ou que les instantanés se trouvent dans la même région que la connexion d'hébergement.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
```



```
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
<!--NeedCopy-->
```

Vous avez besoin des autorisations supplémentaires suivantes basées sur des autorisations minimales pour les fonctionnalités suivantes :

- Si l'image principale est un disque dur virtuel dans un compte de stockage situé dans la même région que la connexion d'hébergement :

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
<!--NeedCopy-->
```

- Si l'image principale est une ImageVersion de Shared Image Gallery :

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
<!--NeedCopy-->
```

- Si l'image principale est un disque géré, les instantanés ou un disque dur virtuel se trouvent dans une région différente de celle de la connexion d'hébergement :

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
<!--NeedCopy-->
```

- Si vous utilisez un groupe de ressources géré par Citrix :

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
<!--NeedCopy-->
```

- Si vous placez l'image principale dans Shared Image Gallery :

```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
<!--NeedCopy-->
```

- Si vous utilisez la prise en charge des hôtes dédiés Azure :

```
"Microsoft.Compute/hostGroups/read",
```



```
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
<!--NeedCopy-->
```

- Si vous utilisez le chiffrement côté serveur (SSE) avec des clés gérées par le client (CMK) :

```
"Microsoft.Compute/diskEncryptionSets/read",
<!--NeedCopy-->
```

- Si vous déployez des machines virtuelles à l'aide de modèles ARM (profil de machine) :

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
<!--NeedCopy-->
```

- Si vous utilisez la spécification de modèle Azure comme profil de machine :

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

Création, mise à jour et suppression de machines dotées d'un disque non géré Voici la liste des autorisations minimales requises lorsque l'image principale est un disque dur virtuel et utilise un groupe de ressources fourni par l'administrateur :

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action"
<!--NeedCopy-->
```


Autorisation générale

Le rôle de contributeur dispose d'un accès complet pour gérer toutes les ressources. Cet ensemble d'autorisations ne vous empêche pas d'obtenir de nouvelles fonctionnalités.

L'ensemble d'autorisations suivant fournit la meilleure compatibilité à l'avenir, même s'il inclut plus d'autorisations que nécessaire avec l'ensemble de fonctionnalités actuel :

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
```



```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

Autres ressources

- Si vous êtes dans le processus de déploiement initial, consultez la section Créer des catalogues de machines.
- Pour obtenir des informations spécifiques à Azure, consultez la section Créer un catalogue Microsoft Azure.

Informations supplémentaires

- Connexions et ressources
- Créer des catalogues de machines

Connexion à Microsoft System Center Virtual Machine Manager

June 27, 2024

La section Créer et gérer des connexions et des ressources décrit les assistants qui créent une connexion. Les informations suivantes couvrent les détails spécifiques à Microsoft System Center Virtual Machine Manager (VMM).

> **Remarque :**
>
> Avant de créer une connexion à VMM, vous devez d'abord terminer la configuration de votre compte VMM en tant qu'emplacement de ressources. Voir Environnements de virtualisation Microsoft System Center Virtual Machine Manager.

Créer une connexion

Si vous utilisez MCS pour provisionner des VM, procédez comme suit dans l'assistant de création de connexion :

- Entrez l'adresse en tant que nom de domaine complet du serveur hôte.
- Entrez les informations d'identification du compte d'administrateur créé préalablement. Ce compte doit être autorisé à créer des VM.
- Dans la boîte de dialogue Détails d'hôte, sélectionnez le cluster ou l'hôte autonome à utiliser pour créer vos VM.

> **Important**
>
> Recherchez un cluster ou un hôte autonome, même si vous utilisez un déploiement d'hôte Hyper-V unique.

Autres ressources

- Si vous êtes dans le processus de déploiement initial, consultez la section Créer des catalogues de machines.
- Pour créer des catalogues de machines avec le partage de fichiers MCS sur SMB 3, consultez la section Créer un catalogue Microsoft System Center Virtual Machine Manager.

Informations supplémentaires

- Connexions et ressources
- Créer des catalogues de machines

Connexion à Nutanix

June 27, 2024

La section Créer et gérer des connexions et des ressources décrit les assistants qui créent une connexion. Les informations suivantes couvrent les détails spécifiques à Nutanix.

> **Remarque :**
>
> Avant de créer une connexion à Nutanix, vous devez d'abord terminer la configuration de votre compte Nutanix en tant qu'emplacement de ressources. Voir Environnements de virtualisation Nutanix.

Créer une connexion à Nutanix

Les informations suivantes étayent les conseils disponibles dans la section Connexions et ressources. Pour créer une connexion Nutanix, suivez les instructions générales de cet article, en tenant compte

des détails spécifiques à Nutanix.

Dans l'assistant **Ajouter une connexion et des ressources**, sélectionnez le type de connexion Nutanix sur la page **Connexion**, puis spécifiez l'adresse et les informations d'identification, ainsi qu'un nom pour la connexion. Sur la page **Réseau**, sélectionnez un réseau pour l'unité d'hébergement.

Les types de connexion suivants sont disponibles pour la sélection : **Nutanix AHV**, **Nutanix AHV Xi** et **Nutanix AHV PC**.

- Pour **Nutanix AHV**, spécifiez l'adresse et les informations d'identification du cluster Prism Element (PE).
- Pour **Nutanix AHV PC**, spécifiez l'adresse et les informations d'identification de Prism Central (PC).

  > **Remarque :**
  >
  > Actuellement, le type de connexion Nutanix AHV PC ne s'utilise que pour créer une connexion à Nutanix Cloud Cluster (NC2) sur Azure. En outre, un catalogue de machines ne peut être hébergé que sur un seul cluster dans une connexion NC2 on Azure.

- Pour **Nutanix AHV DRaaS**, spécifiez l'adresse et le nom d'utilisateur du locataire DRaaS. Importez vos fichiers d'informations d'identification Nutanix DRaaS privés et publics (`.pem`).

> **Conseil :**
>
> Si vous déployez des machines en utilisant Nutanix AHV (Prism Element) comme ressource, sélectionnez le conteneur dans lequel réside le disque de la machine virtuelle.

Autres ressources

- Si vous êtes dans le processus de déploiement initial, consultez la section Créer des catalogues de machines.
- Pour obtenir des informations spécifiques à Nutanix, consultez la section Créer un catalogue Nutanix.

Informations supplémentaires

- Connexions et ressources
- Créer des catalogues de machines

Connexion aux solutions partenaires et cloud Nutanix

June 27, 2024

La section Créer et gérer des connexions et des ressources décrit les assistants qui créent une connexion. Les informations suivantes couvrent les détails spécifiques aux solutions partenaires et cloud Nutanix.

Citrix Virtual Apps and Desktops prend en charge les solutions cloud Nutanix et partenaires suivantes :

- Nutanix Cloud Clusters sur AWS

> **Remarque :**
>
> Avant de créer une connexion à une solution partenaire et cloud Nutanix, vous devez d'abord terminer la configuration de votre compte respectif en tant qu'emplacement de ressources. Découvrez les solutions partenaires et cloud Nutanix.

Se connecter à Nutanix Prism

Après avoir créé un cluster Nutanix, connectez-vous à Nutanix Prism.

Pour vous connecter à Nutanix Prism :

1. Créez une machine virtuelle bastion dans le sous-réseau 10.0.129.0/24.
2. Effectuez une connexion RDP à la machine virtuelle bastion, accédez à l'URL de **Prism Element** que vous avez copié dans la section précédente.
3. Connectez-vous à l'aide des informations d'identification par défaut : `admin:nutanix/4u`. N'oubliez pas de modifier le mot de passe.

Créer une machine virtuelle sur le cluster Nutanix

Après vous être connecté à **Nutanix Prism**, créez des machines virtuelles sur le cluster Nutanix.

Si la machine virtuelle a besoin d'un accès Internet

1. Accédez à la console AWS.
2. Créez un nouveau sous-réseau 10.0.130.0/24 dans le même VPC que celui créé par Nutanix CFS.
3. Ajoutez une route à la table de routage de ce sous-réseau pour diriger tout le trafic local nul vers la passerelle NAT ci-dessus.

4. Effectuez une connexion RDP à la machine virtuelle bastion, accédez à l'URL de **Prism Element** que vous avez copié dans la section précédente et connectez-vous.
5. Ajoutez un nouveau réseau. Accédez à **Settings>Network Configuration>Create Subnet**. Utilisez le même sous-réseau 10.0.130.0/24 que celui utilisé dans AWS.
6. Créez toutes les machines virtuelles (AD, CC, VDA, etc.) dans ce nouveau sous-réseau.

Si la machine virtuelle n'a pas besoin d'un accès Internet

1. Effectuez une connexion RDP à la machine virtuelle bastion, accédez à l'URL de **Prism Element** que vous avez copié dans la section précédente et connectez-vous.
2. Ajoutez un nouveau réseau. Accédez à **Settings>Network Configuration>Create Subnet**. Utilisez le sous-réseau 10.0.129.0/24.
3. Créez toutes les machines virtuelles (AD, CC, VDA, etc.) de ce sous-réseau.

> **Conseil :**
>
> Assurez-vous que les informations relatives à l'heure et au fuseau horaire des machines virtuelles sont correctement configurées, en particulier pour AD.

Créer une connexion hôte

1. Lancez Web Studio.
2. Sélectionnez le nœud d'hébergement, puis cliquez sur **Ajouter une connexion et des ressources**.
3. Sur l'écran **Connexion**, sélectionnez **Créer une nouvelle connexion** et, dans l'**adresse de connexion**, entrez `https://xxx.xxx.xxx.xxx:9440`.
4. Suivez l'interface utilisateur pour terminer l'Assistant.

> **Remarque :**
>
> Pour que l'option pour Nutanix dans Web Studio soit visible, le plug-in Nutanix doit être installé sur toutes les machines virtuelles de connecteur, même si elles ne sont pas utilisées dans la zone Nutanix.

Autres ressources

- Si vous êtes dans le processus de déploiement initial, consultez la section Créer des catalogues de machines.
- Pour obtenir des informations spécifiques à Nutanix, consultez la section Créer un catalogue Nutanix.

Informations supplémentaires

- Connexions et ressources
- Créer des catalogues de machines

Connexion à VMware

June 27, 2024

La section Créer et gérer des connexions et des ressources décrit les assistants qui créent une connexion. Les informations suivantes couvrent les détails spécifiques aux environnements de virtualisation VMware.

> **Remarque :**
>
> Avant de créer une connexion à VMware, vous devez d'abord terminer la configuration de votre compte VMware en tant qu'emplacement de ressources. Voir Environnements de virtualisation VMware.

Créer une connexion

Dans l'assistant de création de connexion :

1. Sélectionnez le type de connexion VMware.
2. Entrez l'adresse du point d'accès pour le kit de développement vCenter.
3. Entrez les informations d'identification d'un compte d'utilisateur VMware configuré précédemment qui dispose des permissions nécessaires à la création de VM. Spécifiez le nom d'utilisateur au format domaine/nomutilisateur.

Empreinte numérique SSL VMware

La fonction d'empreinte numérique VMware SSL élimine la nécessité de créer manuellement une connexion hôte à un hyperviseur VMware vSphere. Il n'est plus nécessaire de créer manuellement une relation d'approbation entre les Delivery Controller du site et le certificat de l'hyperviseur avant de créer une connexion.

La fonctionnalité d'empreinte numérique VMware SSL stocke l'empreinte numérique du certificat non approuvé dans la base de données du site. Cette configuration garantit que l'hyperviseur peut être identifié en permanence comme fiable par Citrix Virtual Apps and Desktops, même s'il ne l'est pas par les Controller.

Lors de la création d'une connexion hôte vSphere dans Studio, une boîte de dialogue vous permet d'afficher le certificat de la machine à laquelle vous vous connectez. Vous pouvez alors choisir de l'approuver.

Privilèges requis

Créez un compte d'utilisateur VMware et un ou plusieurs rôles VMware avec un ensemble, ou la totalité, des autorisations répertoriées dans cet article. Créez des rôles en fonction du niveau de granularité requis en plus des autorisations utilisateur pour demander les diverses opérations de Citrix DaaS à tout moment. Pour accorder des autorisations spécifiques à l'utilisateur à tout moment, associez-les au rôle correspondant, au niveau du centre de données au minimum , en sélectionnant l'option **Propagate to children**.

Les tableaux suivants répertorient les correspondances entre les opérations Citrix Virtual Apps and Desktops et les privilèges VMware requis au minimum.

> **Remarque :**
>
> Le nom d'affichage de la liste des autorisations, en particulier *User Interface*, est différent pour certaines versions de vSphere. Par exemple, dans vSphere 6.7, l'autorisation *User Interface* est **Change Memory** and **Change Settings**, plutôt que **Settings** et **Memory** comme décrit dans les privilèges requis indiqués sur cette page.

Ajouter des connexions et des ressources

SDK	Interface utilisateur
System. Anonymous, System. Read, et System.View	Ajouté automatiquement. Peut utiliser le rôle lecture seule intégré.

Gestion de l'alimentation

SDK	Interface utilisateur
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend

SDK	Interface utilisateur
Datastore.Browse	Datastore > Browse datastore

Provisionner des machines (Machine Creation Services)

Pour provisionner des machines à l'aide de MCS, les autorisations suivantes sont obligatoires :

SDK	Interface utilisateur
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
Virtual machine.Config.Add or remove device	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Change memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Change settings
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing

SDK	Interface utilisateur
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2, vSphere 5.1, Update 1, and vSphere 6.x, Update 1: Virtual machine > State > Create snapshot; vSphere 5.5: Virtual machine > Snapshot management > Create snapshot

Mise à jour et restauration de l'image

SDK	Interface utilisateur
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove

SDK	Interface utilisateur
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine

Supprimer des machines provisionnées

SDK	Interface utilisateur
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove

Profil de stockage (vSAN)

Pour afficher, créer ou supprimer des stratégies de stockage lors de la création de catalogues sur un datastore vSAN, les autorisations suivantes sont obligatoires :

SDK	Interface utilisateur
StorageProfile.Update	PROFILE-DRIVEN STORAGE > Profile-driven storage update. Pour vSphere 8 : VM storage policies > Update VM storage policies
StorageProfile.View	PROFILE-DRIVEN STORAGE > Profile-driven storage view. Pour vSphere 8 : VM storage policies > View VM storage policies

Balises et attributs personnalisés

Les balises et les attributs personnalisés vous permettent de joindre des métadonnées aux machines virtuelles créées dans l'inventaire vSphere, et de faciliter la recherche et le filtrage de ces objets. Pour créer, modifier, attribuer et supprimer des balises ou des catégories, les autorisations suivantes sont obligatoires :

SDK	Interface utilisateur
InventoryService.Tagging.CreateTag	vSphere Tagging > Create vSphere Tag
InventoryService.Tagging.CreateCategory	vSphere Tagging > Create vSphere Tag Category
InventoryService.Tagging.EditTag	vSphere Tagging > Edit vSphere Tag
InventoryService.Tagging.EditCategory	vSphere Tagging > Edit vSphere Tag Category
InventoryService.Tagging.DeleteTag	vSphere Tagging > Delete vSphere Tag
InventoryService.Tagging.DeleteCategory	vSphere Tagging > Delete vSphere Tag Category
InventoryService.Tagging.AttachTag	vSphere Tagging > Assign or Unassign vSphere Tag
InventoryService.Tagging.ObjectAttachable	vSphere Tagging > Assign or Unassign vSphere Tag on Object
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

> **Remarque :**
>
> Lorsque MCS crée un catalogue de machines, les machines virtuelles cibles sont étiquetées avec des balises de nom spéciales. Ces balises différencient l'image principale des machines virtuelles créées par MCS et empêchent l'utilisation de machines virtuelles créées par MCS pour la préparation de l'image. La différence est affichée via la valeur de l'attribut `XdProvisioned` dans vCenter. L'attribut est défini sur **True** si MCS crée des machines virtuelles.

Opérations cryptographiques

Les privilèges relatifs aux opérations cryptographiques contrôlent qui peut effectuer un certain type d'opération cryptographique sur un certain type d'objet. vSphere Native Key Provider utilise les privilèges `Cryptographer.*`. Les autorisations minimales suivantes sont requises pour les opérations cryptographiques :

> **Remarque :**
>
> Ces autorisations sont requises pour créer des catalogues de machines MCS avec une machine virtuelle équipée de vTPM.

SDK	Interface utilisateur
Cryptographer.Access	Privileges > All Privileges > Cryptographic operations > Direct Access
Cryptographer.AddDisk	Privileges > All Privileges > Cryptographic operations > Add disk
Cryptographer.Clone	Privileges > All Privileges > Cryptographic operations > Clone
Cryptographer.Encrypt	Privileges > All Privileges > Cryptographic operations > Encrypt
Cryptographer.EncryptNew	Privileges > All Privileges > Cryptographic operations > Encrypt new
Cryptographer.Decrypt	Privileges > All Privileges > Cryptographic operations > Decrypt
Cryptographer.Migrate	Privileges > All Privileges > Cryptographic operations > Migrate
Cryptographer.ReadKeyServersInfo	Privileges > All Privileges > Cryptographic operations > Read KMS information

Provisionner des machines (Citrix Provisioning)

Ces autorisations pour cloner et déployer un modèle sont requises pour provisionner des machines virtuelles à l'aide de l'assistant d'installation Citrix Virtual Apps and Desktops et de l'assistant d'exportation de périphériques via la console Citrix Provisioning. Définissez les autorisations lors de la création d'une connexion d'hébergement. Vous devez disposer de toutes les autorisations de Provisionner des machines (Machine Creation Services) et de ce qui suit.

SDK	Interface utilisateur
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Provisioning.CloneTemplate	Virtual machine > Provisioning > Clone template
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template

SDK	Interface utilisateur
VApp.Export	vApp > Export

> **Remarque :**
>
> `VApp.Export` est nécessaire pour créer des catalogues de machines MCS à l'aide du profil de machine.

Obtenir et importer un certificat

Pour protéger les communications vSphere, Citrix vous recommande d'utiliser HTTPS plutôt que HTTP.

HTTPS requiert des certificats numériques. Utilisez un certificat numérique émis par une autorité de certification qui respecte la stratégie de sécurité de votre organisation.

Si vous ne pouvez pas utiliser un certificat numérique émis par une autorité de certification, vous pouvez utiliser le certificat auto-signé installé par VMware. Utilisez cette méthode uniquement si la stratégie de sécurité de votre organisation l'autorise. Ajoutez le certificat VMware vCenter à chaque Delivery Controller.

1. Ajoutez le nom de domaine complet (FQDN) de l'ordinateur exécutant vCenter Server dans le fichier hôtes de ce serveur, à l'emplacement `%SystemRoot%/WINDOWS/system32/Drivers/etc/`. Cette étape est uniquement nécessaire que si le nom de domaine complet de l'ordinateur exécutant vCenter Server n'est pas déjà présent dans le DNS.
2. Obtenez le certificat vCenter à l'aide de l'une des trois méthodes suivantes :

   Depuis le serveur vCenter.

   a) Copiez le fichier rui.crt depuis le serveur vCenter vers un emplacement accessible sur vos Delivery Controller.
   b) Sur le Controller, naviguez vers l'emplacement du certificat exporté et ouvrez le fichier rui.crt.

   Téléchargez le certificat à l'aide d'un navigateur Web. Si vous utilisez Internet Explorer, il se peut que vous deviez cliquer avec le bouton droit de la souris sur Internet Explorer et choisir **Exécuter en tant qu'administrateur** pour pouvoir télécharger et installer le certificat.

   a) Ouvrez votre navigateur Web et créez une connexion Web sécurisée vers le serveur vCenter (par exemple https://server1.domain1.com)).
   b) Acceptez les avertissements relatifs à la sécurité.
   c) Cliquez sur la barre d'adresse sur laquelle l'erreur de certificat est affichée.

d) Affichez le certificat puis cliquez sur l'onglet Détails.
e) Sélectionnez **Copier dans un fichier puis effectuez l'exportation au format .CER**, en fournissant un nom lorsque vous êtes invité à le faire.
f) Enregistrez le certificat exporté.
g) Naviguez vers l'emplacement du certificat exporté et ouvrez le fichier .CER.

Importez directement depuis Internet Explorer exécuté en tant qu'administrateur.

- Ouvrez votre navigateur Web et créez une connexion Web sécurisée vers le serveur vCenter (par exemple https://server1.domain1.com)).
- Acceptez les avertissements relatifs à la sécurité.
- Cliquez sur la barre d'adresse sur laquelle l'erreur de certificat est affichée.
- Affichez le certificat.

3. Importez le certificat dans le magasin de certificats sur chacun de vos Controller.

a) Cliquez sur l'option **Installer le certificat**, sélectionnez **Machine locale**, puis cliquez sur **Suivant**.
b) Sélectionnez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur **Parcourir**. Sélectionnez **Personnes autorisées**, puis cliquez sur **OK**. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

Si vous modifiez le nom du serveur vSphere après l'installation, vous devez générer un nouveau certificat auto-signé sur ce serveur avant d'importer le nouveau certificat.

Autres ressources

- Si vous êtes dans le processus de déploiement initial, consultez la section Créer des catalogues de machines.
- Pour obtenir des informations spécifiques à VMware, consultez la section Créer un catalogue VMware.

Informations supplémentaires

- Connexions et ressources
- Créer des catalogues de machines

Connexion aux solutions partenaires et cloud VMware

June 27, 2024

Après avoir configuré le cluster Azure VMware Solution (AVS), Google Cloud VMware Engine et VMware Cloud sur AWS, créez les connexions. Reportez-vous à la section Connexion à VMware pour créer des connexions.

Autres ressources

- Si vous êtes dans le processus de déploiement initial, consultez la section Créer des catalogues de machines.
- Pour obtenir des informations spécifiques à VMware, consultez la section Créer un catalogue VMware.

Informations supplémentaires

- Connexions et ressources
- Créer des catalogues de machines

Gestion des images (Technical Preview)

June 27, 2024

Introduction

Le processus de création ou de mise à jour du catalogue MCS comporte deux phases :

- Mastering : une image source est convertie en image publiée.
- Clonage : de nouvelles machines virtuelles sont créées à partir de l'image publiée.

Grâce à la fonctionnalité de gestion des images, MCS sépare la phase de mastering du workflow global de provisioning.

Vous pouvez préparer différentes versions d'image MCS (Image préparée) à partir d'une seule image source et les utiliser dans plusieurs catalogues de machines MCS différents. Cette implémentation réduit considérablement les coûts en stockage et en temps, et simplifie le déploiement des machines virtuelles et le processus de mise à jour des images.

Les avantages de cette fonctionnalité de gestion d'images sont les suivants :

- Générez des images préparées à l'avance sans créer de catalogue.
- Réutilisez les images préparées dans plusieurs scénarios, tels que la création et la mise à jour d'un catalogue.

- Réduisez considérablement le temps de création ou de mise à jour du catalogue.

> **Remarque :**
>
> - Cette fonctionnalité est actuellement applicable aux environnements de virtualisation Azure et VMware.
> - Vous pouvez créer un catalogue de machines MCS sans utiliser d'images préparées. Dans ce cas, vous ne pourrez pas bénéficier des avantages de cette fonctionnalité.

Cas d'utilisation

Voici certains des cas d'utilisation de la fonctionnalité de gestion des images :

- *Gestion des versions* : les versions d'image vous permettent de :
  - Gérer les différentes itérations ou mises à jour d'une image particulière.
  - Gérer plusieurs versions d'une image à des fins différentes.
- *Regroupement logique*: vous pouvez créer plusieurs définitions d'images pour :
  - Regrouper logiquement les versions d'images en fonction de différents critères tels que le projet, le département ou le type d'application et de bureau.
  - gérer les images plus efficacement au sein d'une organisation.

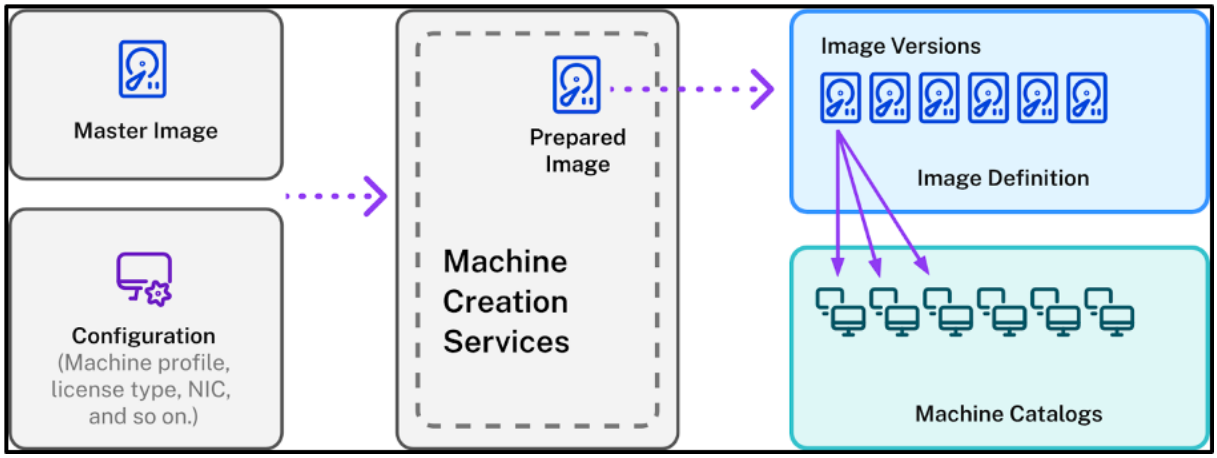
Qu'est-ce qu'une image préparée ?

Grâce à la fonctionnalité de gestion des images, MCS dissocie la phase de mastering du workflow global de création ou de mise à jour du catalogue et divise le processus en deux étapes :

1. Créer des images préparées à partir d'une seule image source.
2. Utiliser l'image préparée pour créer ou mettre à jour un catalogue de machines MCS.

Vous pouvez créer les images préparées à l'avance. Vous pouvez utiliser une seule image préparée pour créer ou mettre à jour plusieurs catalogues de machines provisionnées par MCS.

Découvrez comment une image préparée est utilisée dans plusieurs catalogues de machines MCS lorsque vous utilisez Web Studio à partir de l'image :



Définition d'image : les définitions d'image constituent un regroupement logique de versions d'une image. La définition d'image contient les informations suivantes :

- Pourquoi l'image a été créée.
- À quel système d'exploitation il est destiné.
- Autres informations relatives à l'utilisation de l'image.

Un catalogue n'est pas créé à partir d'une définition d'image, mais à partir des versions d'image créées en fonction de cette définition.

Version d'image : les versions d'image gèrent les versions pour la définition d'image. Une définition d'image peut avoir plusieurs versions d'image. Utilisez les versions d'image en tant qu'images préparées pour créer ou mettre à jour un catalogue.

Sinon, si vous souhaitez utiliser les commandes PowerShell pour créer un schéma de provisioning afin de créer ou de mettre à jour un catalogue, vous devez créer une spécification de version d'image préparée basée sur la spécification de version d'image principale, selon les besoins de votre environnement.

Testez les fonctionnalités Technical Preview

Si vous souhaitez tester les fonctionnalités Technical Preview, veuillez indiquer vos coordonnées ici.

Nous vous aiderons à configurer l'environnement de test et vous fournirons une assistance technique si nécessaire.

Exigences

- Pour l'image principale Windows, seules les images VDA avec la version 2311 et versions ultérieures, et compatibles MCS/IO sont prises en charge.

Limitations

Actuellement, cette fonctionnalité ne prend pas en charge les éléments suivants :

- Plusieurs cartes d'interface réseau dans Azure
- Fonctionnalité de disque de données persistant
- Hibernation pour plusieurs sessions
- Changement de type d'image

Gestion du cycle de vie des images à l'aide de Web Studio

Le cycle de vie de l'image lorsque vous utilisez Web Studio est le suivant :

1. Créez une image préparée : créez une définition d'image et sa version d'image initiale.
2. Créez des versions d'image à partir de la version d'image initiale.
3. Utilisez une version d'image comme image préparée pour créer des catalogues.
4. Mettez à jour un catalogue de machines avec une autre image préparée.
5. Gérez les définitions et les versions des images : modifiez le nom et la description des versions d'image, ainsi que la description d'une définition d'image.
6. Supprimez une version d'image.
7. Supprimez une définition d'image.

Vous pouvez également gérer les images à l'aide de PowerShell. Consultez la section Gestion du cycle de vie des images à l'aide de PowerShell.

Créer ou mettre à jour un catalogue à l'aide d'une image préparée

Créez des images préparées et utilisez-les pour créer ou mettre à jour un catalogue de machines MCS en utilisant :

- Web Studio
- Les commandes PowerShell

Utiliser Web Studio

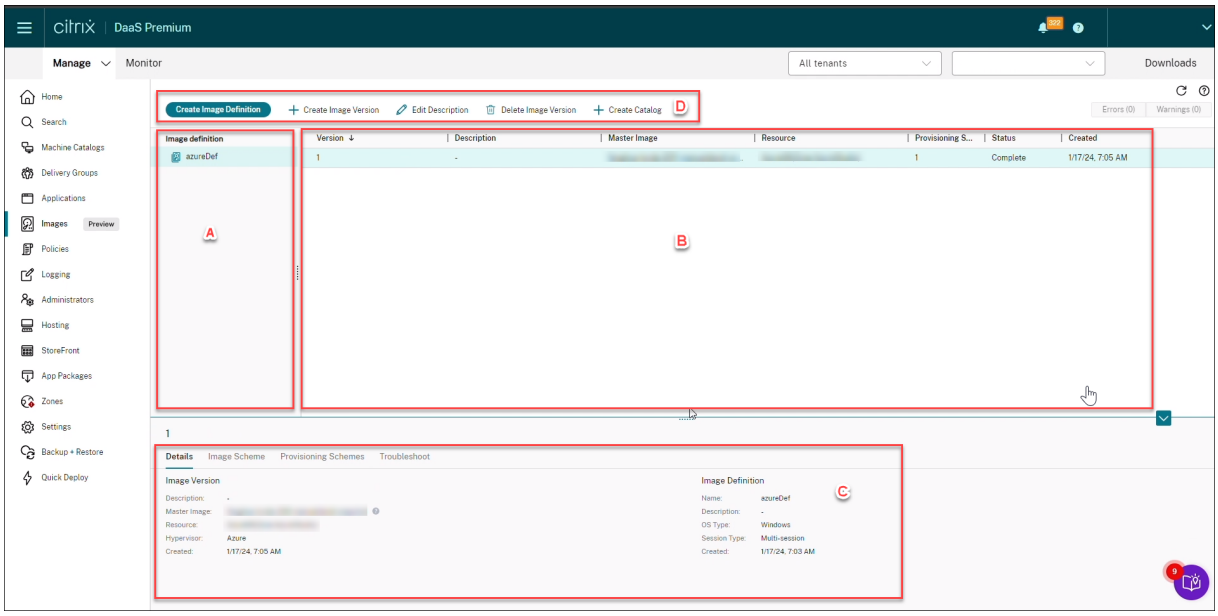
Consultez les sections suivantes :

- Présentation du nœud Images
- Créer une définition d'image et une version d'image initiale
- Créer des versions d'images
- Créer un catalogue de machines à partir du nœud Images

- Créer un catalogue de machines à partir du nœud Catalogues de machines
- Mettre à jour un catalogue de machines avec une autre image préparée
- Gérer les définitions et les versions d'image

Présentation du nœud Images

Utilisez le nœud **Images** pour créer et gérer des images préparées par MCS. La vue principale est divisée en quatre parties :



Étiquette	Partie	Description
A	Définitions d'image	Répertorie les définitions d'image créées précédemment.
B	Versions d'image	Affiche les versions d'image de la définition d'image sélectionnée.
C	Détails	• L'onglet **Détails** affiche des informations détaillées sur la définition ou la version d'image sélectionnée, telles que l'image principale, la ressource, l'hyperviseur, le nom de la définition d'image, le type de système d'exploitation et le type de session. • L'onglet **Schéma d'image** affiche des informations sur le modèle utilisé pour

Étiquette	Partie	Description
D	Barre d'action	Répertorie les actions que vous pouvez effectuer sur les définitions et les versions d'image, telles que **Créer une version d'image**, **Modifier la description**, **Supprimer la version d'image**et **Créer un catalogue**.

Créer un catalogue de machines à l'aide d'une image préparée

Les étapes clés pour créer un catalogue de machines MCS à l'aide de l'image préparée sont les suivantes :

1. Créez la définition d'image et les versions d'image initiales.
2. Utilisez la version d'image comme image préparée pour créer un catalogue.

Créer une définition d'image et une version d'image initiale

Pour créer une définition d'image et la version d'image initiale, procédez comme suit :

1. Connectez-vous à Web Studio et sélectionnez le nœud **Images**. Cliquez sur **Suivant** sur la page **Introduction**.
2. Sur la page **Définition d'image**, spécifiez le **Type d'OS** et le **Type de session** pour la définition d'image.
3. Sur la page **Image**, sélectionnez **Ressources** et une image principale à utiliser comme modèle pour créer la version d'image. Vous pouvez cocher la case **Utiliser un profil de machine** et sélectionner un profil de machine.

   > **Remarque :**
   >
   > Avant de sélectionner une image, vérifiez que le VDA 2311 ou version ultérieure est installé sur l'image principale et que le pilote MCSIO est installé sur le VDA.

4. (Uniquement pour Azure) Sur la page **Types de stockage et de licence**, sélectionnez le type de stockage et de licence à utiliser dans le cadre du processus de préparation de l'image.

> **Remarque :**
>
> Si vous sélectionnez un profil de machine sur la page **Image**, le type de licence du profil de machine est présélectionné en fonction du paramètre de profil.

5. Sur la page **Spécification de machine** :
   - Pour Azure, sélectionnez une taille de machine. Si vous sélectionnez un profil de machine sur la page **Image**, la taille de machine du profil de machine est sélectionnée par défaut.
   - Pour VMware, si vous sélectionnez un profil de machine, vous pouvez voir le nombre de processeurs virtuels dérivé du profil de machine. Ce nombre ne peut pas être modifié. Si vous ne sélectionnez aucun profil de machine, vous ne pouvez voir que la taille de la mémoire dérivée de l'image principale.
6. Sur la page **Cartes d'interface réseau**, sélectionnez ou ajoutez des cartes d'interface réseau pour l'image de préparation. Pour chaque carte d'interface réseau, sélectionnez un réseau virtuel associé.

   Pour VMware, si vous ne sélectionnez aucun profil de machine, la carte d'interface réseau associée à l'image principale est sélectionnée par défaut. Si vous sélectionnez un profil de machine, les cartes d'interface réseau sont dérivées du profil de machine et le nombre ne peut pas être modifié.

   > **Remarque :**
   >
   > Les cartes d'interface réseau multiples ne sont pas prises en charge dans Azure.

7. (Uniquement pour Azure) Sur la page **Paramètres du disque**, sélectionnez la clé de cryptage gérée par le client (CMEK). Si le profil de la machine ne comprend pas de CMEK, mais que l'image principale en possède une, il présélectionne la CMEK à partir de l'image principale.
8. Sur la page **Description de la version**, entrez une description de la version d'image initiale créée.
9. Sur la page **Résumé**, vérifiez les détails de la définition d'image et de la version d'image initiale créée. Entrez un nom et une description pour la définition d'image. Cliquez sur **Terminer**.

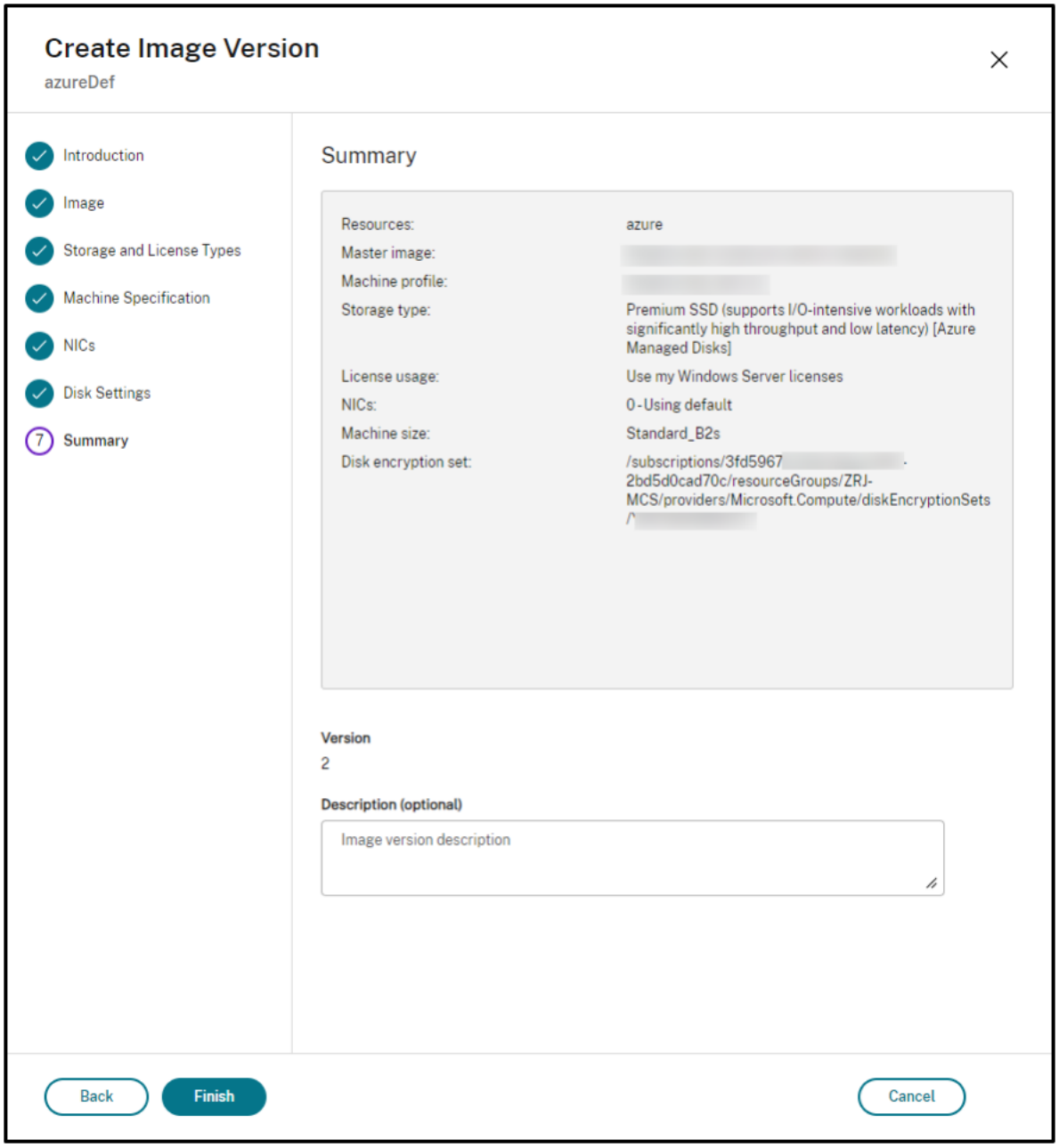
Créer des versions d'images

Les versions d'image permettent de gérer différentes itérations ou mises à jour d'une image particulière. Cette fonctionnalité vous permet de gérer plusieurs versions d'une image à différentes fins.

Pour créer des versions d'image à partir de la version d'image initiale, procédez comme suit :

> **Remarque :**
>
> L'unité d'hébergement de toutes les versions d'image doit être la même.

1. Accédez au nœud **Images**, sélectionnez une version d'image, puis sélectionnez **Créer version d'image**.
2. Si vous souhaitez que la configuration de la version d'image soit différente de la version d'image configurée initialement, configurez les paramètres sur les pages **Image**, **Types de stockage et de licence**, **Spécification de machine**, **Cartes d'interface réseau**et **Paramètres du disque** de la boîte de dialogue **Créer version d'image**.
3. Ajoutez une description pour la version d'image. Cliquez sur **Terminer**.



Créer un catalogue de machines à partir du nœud Images

Utilisez l'option **Créer un catalogue** dans le nœud **Images** pour créer un catalogue à l'aide de la version d'image.

Vous pouvez également sélectionner la version lors de la création d'un catalogue dans le nœud **Catalogues de machines**, en établissant un lien vers l'option d'image préparée dans le workflow de création de catalogue. Consultez la section Créer un catalogue de machines à partir du nœud Catalogues de machines.

Pour créer un catalogue de machines MCS à partir du nœud **Images**, procédez comme suit :

1. Sélectionnez une version d'image e, puis cliquez sur **Créer un catalogue**. Cliquez sur **Suivant** sur la page **Introduction**.
2. Sur la page **Expérience de bureau**, sélectionnez l'expérience de bureau requise.
3. De la page **Image** à la page **Paramètres du disque**, les paramètres sont présélectionnés en fonction de la version d'image sélectionnée.
4. (Pour Azure) Sur la page **Groupe de ressources**, vous pouvez choisir de créer un groupe de ressources ou d'utiliser un groupe de ressources existant dans lequel placer les ressources de ce catalogue.
5. Complétez les paramètres sur les pages suivantes.
6. Sur la page **Résumé**, vérifiez les détails du catalogue de machines. Entrez un nom et une description pour le catalogue. Cliquez sur **Terminer**.
7. Accédez au nœud **Catalogues de machines** pour voir le catalogue de machines créé.

Créer un catalogue de machines à partir du nœud Catalogues de machines

Pour créer un catalogue de machines MCS à partir du nœud **Catalogues de machines**, procédez comme suit :

1. Cliquez sur **Catalogues de machines** dans le panneau de navigation de gauche.
2. Cliquez sur **Créer un catalogue de machines**. La page **Création d'un catalogue de machines** s'affiche. Dans les pages **Introduction**, **Type de machine** et **Gestion des machines**, cliquez sur **Suivant**.
3. Sur la page **Image** :

    a) Sélectionnez une **Image préparée**.
    b) Sous **Image préparée**, sélectionnez une version d'image d'une définition d'image.
    c) Cliquez sur le nom de la version d'image. Pour afficher plus de détails sur la version d'image sélectionnée, cliquez sur le numéro de version, qui est souligné.
    d) Si la version d'image sélectionnée est configurée avec un profil de machine, sélectionnez un profil de machine. Si la version d'image sélectionnée n'est pas configurée avec un profil de machine, vous ne pouvez pas choisir de profil de machine.

4. Configurez les paramètres sur les pages suivantes.
5. Sur la page **Paramètres du disque**, si l'image préparée sélectionnée utilise un jeu de cryptage de disque, vous ne pouvez pas supprimer le jeu de cryptage, mais vous pouvez remplacer la clé par une autre clé de cryptage.
6. (Pour Azure) Sur la page **Groupe de ressources**, vous pouvez choisir de créer un groupe de ressources ou d'utiliser un groupe de ressources existant dans lequel placer les ressources de ce catalogue.

7. Complétez les paramètres sur les pages suivantes.
8. Sur la page **Résumé**, vérifiez les détails du catalogue de machines. Entrez un nom et une description pour le catalogue. Cliquez sur **Terminer**.

Mettre à jour un catalogue de machines avec une autre image préparée

Pour mettre à jour un catalogue de machines MCS existant avec une autre image préparée, procédez comme suit :

1. Cliquez sur **Catalogues de machines** dans le panneau de navigation de gauche et sélectionnez le catalogue de machines que vous souhaitez mettre à jour. Cliquez avec le bouton droit de la souris et sélectionnez **Modifier l'image préparée**.
2. Sur la page **Image**, sélectionnez une image préparée.
3. Sur la page **Stratégie de déploiement**, sélectionnez le moment où vous souhaitez mettre à jour ce catalogue avec l'image préparée sélectionnée.
4. Sur la page **Résumé**, vérifiez les détails. Cliquez sur **Terminer**.

Vous pouvez consulter l'historique des modifications d'image apportées à un catalogue. Pour consulter l'historique, procédez comme suit :

1. Sélectionnez un catalogue de machines.
2. Dans l'onglet **Propriétés du modèle**, dans le champ **Image préparée**, cliquez sur **Afficher l'historique des images**.

Gérer les définitions et les versions d'image

Vous pouvez modifier et supprimer les définitions et les versions d'image pour gérer l'utilisation des différentes versions et définitions d'image créées.

Modifier une définition d'image Vous pouvez modifier le nom et la description d'une définition d'image.

Pour modifier une définition d'image, procédez comme suit :

1. Accédez au nœud **Images**, sélectionnez une définition d'image, puis sélectionnez **Modifier la définition d'image**.

Modifier la version d'image Vous pouvez modifier la description d'une version d'image pour spécifier l'objectif de celle-ci.

Pour modifier une version d'image, procédez comme suit :

1. Accédez au nœud **Images**, sélectionnez une version d'image, puis sélectionnez **Modifier la description**.

Supprimer une version d'image Pour supprimer une version d'image, procédez comme suit :

1. Accédez au nœud **Images**, sélectionnez une version d'image, puis sélectionnez **Supprimer la version d'image**.

> **Remarque :**
>
> Vous ne pouvez pas supprimer une version d'image si elle est utilisée par un catalogue de machines.

Supprimer une définition d'image Pour supprimer une définition d'image, procédez comme suit :

1. Accédez au nœud **Images**, sélectionnez une définition d'image, puis sélectionnez **Supprimer la définition d'image**.

> **Remarque :**
>
> Vous ne pouvez pas supprimer une définition d'image si elle contient une version d'image.

Gestion du cycle de vie des images à l'aide de PowerShell Si vous souhaitez utiliser les commandes PowerShell pour créer un schéma de provisioning, vous devez créer une spécification de version d'image préparée basée sur la spécification de version d'image principale, selon les besoins de votre environnement.

Spécification de version d'image principale : une spécification de version d'image principale est une image spécifique ajoutée ou créée sous une version d'image. Vous pouvez ajouter une image existante dans l'hyperviseur en tant que spécification de version d'image principale ou créer une spécification de version d'image préparée basée sur la spécification de version d'image principale, selon les besoins de votre environnement. La spécification de version d'image préparée peut être utilisée pour plusieurs schémas de provisioning.

Le cycle de vie d'une image lors de l'utilisation des commandes PowerShell est le suivant :

1. Créez une image :
    a) Créez une définition d'image.
    b) Créez une version d'image.
    c) Ajoutez une spécification de version d'image principale.
    d) Créez une spécification de version d'image préparée.

2. Créez un catalogue de machines MCS à l'aide d'une spécification de version d'image préparée :

    a) Créez un catalogue de brokers.
    b) Créez un pool d'identités.
    c) Créez un schéma de provisioning avec le paramètre UID de la spécification de version d'image préparée à l'aide de la commande `New-ProvScheme`.
    d) Liez le catalogue des brokers au schéma de provisioning.

3. Créez des machines virtuelles dans le catalogue de machines MCS.
4. Modifiez la spécification de version d'image préparée d'un schéma de provisioning à l'aide de la commande `Set-ProvScheme`.
5. Gérez les définitions et les versions d'image : modifiez les versions d'image et les définitions d'image.
6. Supprimez un catalogue de machines MCS : l'ordre de suppression est Spécification de version d'image préparée > Spécification de version d'image principale > Version d'image > Définition d'image. Avant de supprimer la spécification de version d'image, assurez-vous que la spécification de version d'image préparée n'est associée à aucun catalogue de machines MCS.

Utiliser PowerShell

Vous pouvez effectuer les opérations suivantes à l'aide des commandes PowerShell :

- Créer une image préparée
- Créer un catalogue à l'aide de la spécification de version d'image préparée
- Mettre à jour un catalogue à l'aide d'une spécification de version d'image préparée
- Supprimer la définition d'image, la version d'image et la spécification de version d'image préparée
- Gérer la définition d'image et la version d'image
- Obtenir la définition d'image, la version d'image, la spécification de version d'image préparée et les détails du schéma de provisioning

Créer une image préparée

Les commandes PowerShell détaillées permettant de créer une spécification de version d'image préparée sont les suivantes :

1. Vérifiez les noms de définition d'image disponibles à l'aide de `Test-ProvImageDefinitionNameAvai` `command`. Par exemple,


```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string
    []>
<!--NeedCopy-->
```

2. Créez une définition d'image à l'aide de la commande `New-ProvImageDefinition`. Par exemple,

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType
    Windows -VdaSessionSupport MultiSession
<!--NeedCopy-->
```

3. Créez une version d'image à l'aide de la commande `New-ProvImageVersion`. Par exemple,

```
New-ProvImageVersion -ImageDefinitionName image1 -Description "
    version 1"
<!--NeedCopy-->
```

4. Ajoutez une spécification de version d'image principale à la version d'image à l'aide de la commande `Add-ProvImageVersionSpec`. Par exemple,

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
    ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "
    XDHyp:\HostingUnits\azure\image.folder\azureresourcegroup.
    resourcegroup\win2022-snapshot.snapshot"
<!--NeedCopy-->
```

> **Remarque :**
>
> Vous ne pouvez ajouter qu'une seule spécification de version d'image principale à une version d'image pour une unité d'hébergement.

5. Créez une spécification de version d'image préparée à partir de la spécification de version d'image principale à l'aide de la commande `New-ProvImageVersionSpec`. Par exemple,

```
New-ProvImageVersionSpec
-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network"
-ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder
    \Standard_B2ms.serviceoffering" -CustomProperties "<
    CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`"></CustomProperties>" -RunAsynchronously
<!--NeedCopy-->
```

> **Remarque :**
>
> Une unité d'hébergement et un type de préparation ne peuvent avoir qu'une seule in-

> stance préparée.

Exemple d'ensemble complet de commandes Powershell permettant de créer une définition d'image, une version d'image et une spécification de version d'image préparée dans Azure :

```
$ImageDefintion = New-ProvImageDefinition
-ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
    MultiSession
 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
     $ImageDefintion.ImageDefinitionName -Description "version 1"
$MasterImagePath = "XDHyp:\HostingUnits\azure\image.folder\
    azureresourcegroup.resourcegroup\win2022-snapshot.snapshot"
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
     $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName azure -MasterImagePath
    $MasterImagePath
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network" }
  -ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder\
      Standard_B2ms.serviceoffering" -CustomProperties "<
      CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
      machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
      instance`"></CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
<!--NeedCopy-->
```

Exemple d'ensemble complet de commandes Powershell permettant de créer une définition d'image, une version d'image et une spécification de version d'image préparée dans VMware :

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2 -
    OsType Windows -VdaSessionSupport SingleSession
$ImageVersion = New-ProvImageVersion -ImageDefinitionName
    $ImageDefintion.ImageDefinitionName -Description "version 1"
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
    master-snap.snapshot"
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
     $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName vmware -MasterImagePath
    $MasterImagePath
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
<!--NeedCopy-->
```


> **Remarque :**
>
> - Toutes les spécifications de version d'image figurant dans une définition d'image doivent appartenir à la même unité d'hébergement.
> - Une version d'image ne peut avoir qu'une seule spécification de version d'image principale et une seule spécification de version d'image préparée.
> - Toutes les spécifications de version d'image doivent avoir un profil de machine ou aucune des spécifications de version d'image ne doit avoir un profil de machine.
> - Vous ne pouvez pas spécifier de groupe de ressources lors de la création d'une spécification de version d'image.

Créer un catalogue à l'aide d'une spécification de version d'image préparée

Créez un catalogue de machines MCS à partir de la spécification de version d'image préparée à l'aide de la commande `New-ProvScheme`. Par exemple,

```
1 New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
      Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <
      int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <
      Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable
      >] [-ServiceOffering <string>] [-SecurityGroup <string[]>] [-
      TenancyType <string>] [-MachineProfile <string>] [-CustomProperties
      <string>] [-ResetAdministratorPasswords] [-
      UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
      PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
      >]
2 <!--NeedCopy-->
```

Ou

```
1 New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
      Guid> -HostingUnitName <string> -IdentityPoolName <string> [-
      VMCpuCount <int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-
      NetworkMapping <Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-
      Metadata <Hashtable>] [-ServiceOffering <string>] [-SecurityGroup <
      string[]>] [-TenancyType <string>] [-MachineProfile <string>] [-
      CustomProperties <string>] [-ResetAdministratorPasswords] [-
      UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
      PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
      >]
2 <!--NeedCopy-->
```

Exemple d'ensemble complet de commandes Powershell permettant de créer un catalogue dans Azure :

```
1 $Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC
      $False  -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -
```



```
    PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
    SessionSupport "MultiSession"
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.
    local" -IdentityPoolName "azurecatalog" -IdentityType "
    ActiveDirectory"  -NamingScheme "azure##" -NamingSchemeType "Numeric
    " -Scope @()
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -
    Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits\
    azure\serviceoffering.folder\Standard_B2s.serviceoffering" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network" }
  -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.
     com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
     XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
     StorageAccountType`" Value=`"StandardSSD_LRS`" /></
     CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
    .ProvisioningSchemeUid
<!--NeedCopy-->
```

Exemple d'ensemble complet de commandes Powershell permettant de créer un catalogue dans VMware :

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC
    $False  -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -
    PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
    SessionSupport "MultiSession"
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "vmware.
    local" -IdentityPoolName "vmwarecatalog" -IdentityType "
    ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "
    Numeric" -Scope @()
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image2 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
    -Scope @() -SecurityGroup @() -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog
Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
    .ProvisioningSchemeUid
```



```
<!--NeedCopy-->
```

Mettre à jour un catalogue à l'aide d'une spécification de version d'image préparée

Vous pouvez mettre à jour un catalogue à l'aide de la commande `Set-ProvSchemeImage`. Par exemple,

```
Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
    <Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-
    PurgeJobOnSuccess]
<!--NeedCopy-->
```

Ou

```
Set-ProvSchemeImage -ProvisioningSchemeName <string> -
    ImageVersionSpecUid <Guid> [-DoNotStoreOldImage] [-RunAsynchronously
    ] [-PurgeJobOnSuccess]
<!--NeedCopy-->
```

Exemple d'ensemble complet de commandes Powershell permettant de mettre à jour un catalogue :

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 2 -Filter "
    PreparationType -eq 'Mcs'"
Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
<!--NeedCopy-->
```

Supprimer la définition d'image, la version d'image et la spécification de version d'image préparée

Avant de supprimer une définition d'image, une version d'image et une spécification de version d'image préparée, tenez compte des points suivants :

- Une définition d'image ne peut pas être supprimée si elle contient une version d'image.
- Une version d'image ne peut pas être supprimée si elle contient une spécification de version d'image.
- Une spécification de version d'image principale ne peut pas être supprimée si elle est utilisée par une autre spécification de version d'image préparée.
- Une spécification de version d'image préparée ne peut pas être supprimée si elle est utilisée par un schéma de provisioning.

Voici le détail des étapes :

1. Supprimez une spécification de version d'image préparée. Par exemple,

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
<!--NeedCopy-->
```

> **Remarque :**
>
> La spécification de version d'image principale ne peut être supprimée que lorsqu'aucune spécification de version d'image préparée ne lui est associée.

2. Supprimez la spécification de version d'image principale. Par exemple,

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'None'"
Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
<!--NeedCopy-->
```

3. Supprimez une version d'image. Par exemple,

```
Remove-ProvImageVersion -ImageDefinitionName image1 -
    ImageVersionNumber 1
<!--NeedCopy-->
```

4. Supprimez une définition d'image. Par exemple,

```
Remove-ProvImageDefinition -ImageDefinitionName image1
<!--NeedCopy-->
```

Exemple d'ensemble complet de commandes PowerShell :

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
    image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"
$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
    1
Remove-ProvImageDefinition -ImageDefinitionName image1
<!--NeedCopy-->
```


Gérer la définition d'image et la version d'image

Vous pouvez renommer et modifier une définition d'image, et modifier une version d'image.

- Renommez une définition d'image à l'aide de la commande `Rename-ProvImageDefinition`. Par exemple :

```
Rename-ProvImageDefinition -ImageDefinitionUid <Guid> -
    NewImageDefinitionName <string>
<!--NeedCopy-->
```

Ou

```
Rename-ProvImageDefinition -ImageDefinitionName <string> -
    NewImageDefinitionName <string>
<!--NeedCopy-->
```

- Modifiez une définition d'image à l'aide de la commande `Set-ProvImageDefinition`. Par exemple :

```
Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
    <string>]
<!--NeedCopy-->
```

Ou

```
Set-ProvImageDefinition -ImageDefinitionName <string> [-
    Description <string>]
<!--NeedCopy-->
```

- Modifiez une version d'image à l'aide de la commande `Set-ProvImageVersion`. Par exemple :

```
Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <
    string>]
<!--NeedCopy-->
```

Ou

```
Set-ProvImageVersion -ImageDefinitionName <string> -
    ImageVersionNumber <int> [-Description <string>]
<!--NeedCopy-->
```

Obtenir la définition d'image, la version d'image, la spécification de version d'image préparée et les détails du schéma de provisioning

- Obtenez les détails de définition d'image à l'aide de la commande `Get-ProvImageDefinition`. Par exemple :


```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
    ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-
    MaxRecordCount <int>] [-Skip <int>] [-SortBy <string>] [-
    Filter <string>]
<!--NeedCopy-->
```

- Obtenez les détails de la version d'image à l'aide de la commande `Get-ProvImageVersion`. Par exemple :
  - Pour répertorier les versions d'image dans une définition d'image :

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    <!--NeedCopy-->
    ```

    Ou

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    <!--NeedCopy-->
    ```

  - Pour obtenir le détail d'une version d'image :

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    <!--NeedCopy-->
    ```

    Ou

    ```
    Get-ProvImageVersion -ImageDefinitionName <string> -
        ImageVersionNumber <int>
    <!--NeedCopy-->
    ```

- Obtenez la spécification de version d'image préparée à l'aide de la commande `Get-ProvImageVersionSpec`. Par exemple :
  - Pour répertorier toutes les spécifications de version d'image préparée dans une version d'image :

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid>
    <!--NeedCopy-->
    ```

  - Pour répertorier les spécifications de version d'image principale dans une spécification de version d'image préparée :

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
        PreparationType -eq "None"'
    <!--NeedCopy-->
    ```

  - Pour répertorier les spécifications de version d'image préparée dans une version d'image associée à une image principale :


```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
<!--NeedCopy-->
```

- Pour obtenir les spécifications d'une version d'image préparée avec succès dans une version d'image :

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and
    ImageVersionSpecStatus -eq "Complete"'
<!--NeedCopy-->
```

- Pour obtenir le détail de la spécification de version d'image préparée :

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
<!--NeedCopy-->
```

- Obtenez les détails du schéma de provisioning à l'aide de la commande `Get-ProvScheme`. Par exemple :

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
    ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <
    String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>]
    [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-
    FilterScope <Guid>]
<!--NeedCopy-->
```

- Obtenez l'historique des spécifications de version d'image préparée d'un schéma de provisioning à l'aide de la commande `Get-ProvSchemeImageVersionSpecHistory`. Par exemple :

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName <
    String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid
     <Guid>] [-ImageVersionSpecHistoryUid <Guid>] [-
    ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <
    Int32>] [-SortBy <String>] [-Filter <String>] [-FilterScope <
    Guid>]
<!--NeedCopy-->
```

Créer des catalogues de machines

June 28, 2024

> **Important :**
>
> Depuis Citrix Virtual Apps and Desktops 7 2006, si votre déploiement actuel utilise l'une des technologies suivantes, vous pouvez mettre à niveau votre déploiement vers la version actuelle uniquement après avoir supprimé les éléments en fin de vie qui utilisent ces technologies.
>
> - Personal vDisk (PvD)
> - AppDisks
> - Types d'hôtes de cloud public : Citrix CloudPlatform, Microsoft Azure Classic
>
> Pour de plus amples informations, consultez la section Suppression de PvD, AppDisks et d'hôtes non pris en charge.
>
> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Si vous souhaitez utiliser des connexions hôtes de cloud public pour votre déploiement, vous avez besoin d'une licence de droits hybrides pour effectuer votre nouvelle installation ou mettre à niveau vers la version actuelle.

Lorsque le programme d'installation détecte une ou plusieurs technologies ou connexions hôtes non prises en charge sans licence de droits hybrides, la mise à niveau est suspendue ou s'arrête. Un message explicatif s'affiche. Les journaux du programme d'installation contiennent des détails. Pour plus d'informations, veuillez consulter la section Mettre un déploiement à niveau.

Introduction

Des collections de machines virtuelles ou physiques sont gérées comme une seule entité appelée catalogue de machines. Toutes les machines d'un catalogue ont le même type de système d'exploitation : OS multi-session ou OS mono-session, et machines Windows ou Linux.

Web Studio vous guide dans le processus de création du premier catalogue de machines après la création du site. Après la création du premier catalogue, Web Studio vous guide dans le processus de création du premier groupe de mise à disposition. Plus tard, vous pourrez modifier le catalogue que vous avez créé et créer des catalogues supplémentaires.

> **Conseil :**
>
> La mise à niveau d'un déploiement existant active la fonctionnalité d'optimisation du stockage MCS (Machine Creation Services), aucune configuration supplémentaire n'est requise. Le Virtual

> Delivery Agent (VDA) et la mise à niveau du Delivery Controller gèrent la mise à niveau des E/S de MCS.

Vue d'ensemble

Lorsque vous créez un catalogue de machines virtuelles, vous spécifiez comment provisionner ces ordinateurs virtuels. Vous pouvez utiliser Machine Creation Services (MCS). Ou vous pouvez utiliser vos propres outils pour fournir des machines.

Tenez compte des éléments suivants :

- MCS prend en charge un seul disque système à partir de l'image de la machine virtuelle. Il ignore le reste des disques de données attachés à cette image.
- Si vous utilisez MCS pour provisionner des machine virtuelle, vous devez fournir une image principale (ou un instantané d'image) pour créer des machines virtuelles identiques dans le catalogue. Avant de créer le catalogue, vous devez utiliser des outils pour créer et configurer l'image principale. Ce processus comprend l'installation d'un Virtual Delivery Agent (VDA) sur l'image. Vous créez ensuite le catalogue de machines dans Web Studio. Vous sélectionnez cette image (ou un instantané), spécifiez le nombre de machines virtuelles à créer dans le catalogue et configurez les informations supplémentaires.
- Si vos machines sont déjà disponibles, vous devez quand même créer un ou plusieurs catalogues pour ces machines.
- Si vous créez un catalogue directement à l'aide du SDK du PowerShell, vous pouvez spécifier un modèle d'hyperviseur (**VMTemplates**), plutôt qu'une image ou un instantané.
- L'utilisation d'un modèle pour provisionner un catalogue est considérée comme une fonctionnalité expérimentale. Lorsque vous utilisez cette méthode, la préparation de la machine virtuelle peut échouer. Par conséquent, le catalogue ne peut pas être publié à l'aide du modèle.

Lorsque vous utilisez MCS ou Citrix Provisioning pour créer le premier catalogue, vous pouvez utiliser la connexion hôte que vous avez configurée lors de la création du site. Plus tard (après avoir créé votre premier catalogue et groupe de mise à disposition), vous pouvez modifier les informations concernant cette connexion ou créer d'autres connexions.

Une fois que vous avez créé un catalogue à l'aide de l'assistant, des tests sont exécutés automatiquement pour vous assurer qu'il est correctement configuré. Lorsque les tests sont terminés, vous pouvez afficher un rapport de test. Exécutez les tests à tout moment à partir de Web Studio.

> **Remarque :**
>
> MCS ne prend pas en charge Windows 10 IoT Standard et Windows 10 IoT Entreprise. Consultez le site Microsoft pour obtenir des informations supplémentaires.

Pour plus de détails techniques sur les outils Citrix Provisioning, consultez la section Gestion des images Citrix Virtual Apps and Desktops.

Vérification des licences RDS

Web Studio n'effectue pas la vérification des licences Microsoft RDS valides lors de la création d'un catalogue de machines contenant des machines avec OS multi-session Windows. Pour afficher l'état de la licence Microsoft RDS pour une **machine avec OS multi- session** Windows, accédez à Citrix Director. Affichez l'état de la licence Microsoft RDS sur le panneau **Détails de la machine**. Ce panneau se trouve dans la page **Détails de la machine et Détails de l'utilisateur**. Pour plus d'informations, consultez la section Intégrité des licences Microsoft RDS.

Enregistrement de VDA

Un VDA doit être enregistré auprès d'un Delivery Controller lors du lancement de sessions négociées. Des VDA non enregistrés peuvent entraîner une sous-utilisation des ressources disponibles. Il existe un certain nombre de raisons pour lesquelles un VDA peut ne pas être enregistré, un grand nombre d'entre elles pouvant être résolues par un administrateur. Web Studio fournit des informations de dépannage dans l'assistant de création de catalogue, et après l'ajout de machines depuis un catalogue à un groupe de mise à disposition.

Lorsque vous ajoutez des machines existantes à l'aide de l'assistant, la liste des noms de compte d'ordinateur indique si chaque machine peut être ajoutée au catalogue. Placez le pointeur de la souris sur l'icône située en regard de chaque machine pour afficher un message informatif sur cette machine.

Si le message identifie une machine problématique, supprimez cette machine ou ajoutez la machine. Par exemple, si un message indique qu'il est impossible d'obtenir des informations sur une machine, ajoutez quand même la machine.

Pour plus d'informations, consultez :

- CTX136668 pour obtenir des conseils sur le dépannage de l'enregistrement de VDA
- Versions de VDA et niveaux fonctionnels
- Méthodes d'enregistrement de VDA

Résumé de la création d'un catalogue MCS

Vous trouverez ci-après une brève présentation des actions MCS par défaut à exécuter après avoir fourni les informations dans l'assistant de création d'un catalogue.

- Si vous avez sélectionné une image principale (plutôt qu'un instantané), MCS crée un instantané.
- MCS crée une copie complète de l'instantané et la place sur chaque emplacement de stockage défini dans la connexion hôte.
- MCS ajoute les machines à Active Directory, qui crée des identités uniques.

- MCS crée le nombre de machine virtuelle spécifiées dans l'assistant, avec deux disques pour chaque machine virtuelle. Outre les deux disques par machine virtuelle, une image principale est également stockée dans le même emplacement de stockage. Si vous avez défini plusieurs emplacements de stockage, chacun obtient les types de disque suivants :
  - La copie complète de l'instantané, qui est en lecture seule et partagée entre les machine virtuelle qui viennent d'être créées.
  - Un disque d'identité 16 Mo unique qui attribue à chaque machine virtuelle une identité unique. Chaque machine virtuelle dispose d'un disque d'identité.
  - Un disque de différence unique pour stocker les écritures effectuées sur la machine virtuelle. Ce disque est provisionné par allocation dynamique (si elle est prise en charge par le stockage hôte) et augmente la taille maximale de l'image principale, si nécessaire. Chaque machine virtuelle dispose d'un disque de différence. Le disque de différence conserve les modifications apportées au cours de sessions. Il est permanent pour les postes de travail dédiés. Pour les bureaux regroupés, il est supprimé et un autre est créé après chaque redémarrage via le Delivery Controller.

Éventuellement, lors de la création de machines virtuelles pour mettre à disposition des bureaux statiques, vous pouvez spécifier (sur la page **Machines** de l'assistant de création d'un catalogue de machines) des clones de machine virtuelle lourds (copie complète). Les clones complets ne requièrent pas la rétention de l'image principale sur chaque magasin de données. Chaque machine virtuelle dispose de son propre fichier.

Considérations sur le stockage MCS

De nombreux facteurs doivent être pris en compte lors de la prise de décisions concernant les solutions, les configurations et les capacités de stockage pour MCS. Les informations suivantes fournissent des considérations appropriées pour la capacité de stockage :

Considérations relatives à la capacité :

- Disques

  Les disques Delta ou Differencing (Diff) consomment la plus grande quantité d'espace dans la plupart des déploiements MCS pour chaque machine virtuelle. Chaque machine virtuelle créée par MCS se voit attribuer au minimum 2 disques lors de la création.

  - Disk0 = disque Diff –Contient le système d'exploitation lors de la copie à partir de l'image de base principale.
  - Disk1 = disque d'identité : 16 Mo –Contient des données Active Directory pour chaque machine virtuelle.

À mesure que le produit évolue, vous devrez peut-être ajouter des disques supplémentaires pour répondre à certains cas d'utilisation et à la consommation de fonctionnalités. Par exemple :

- MCS Storage Optimization crée un disque de style cache en écriture pour chaque machine virtuelle.
- MCS a ajouté la possibilité d'utiliser des clones complets par opposition au scénario de disque Delta décrit dans la section précédente.

Les fonctionnalités d'hyperviseur peuvent également entrer en considération. Par exemple :

- XenServer IntelliCache crée un disque de lecture sur le stockage local pour chaque XenServer. Cette option s'enregistre sur IOPS sous l'image principale et qui peut être conservé sur l'emplacement de stockage partagé.

- Surcharges liées à l'hyperviseur

  Différents hyperviseurs utilisent des fichiers spécifiques qui créent des surcharges pour les machines virtuelles. Les hyperviseurs utilisent également le stockage pour la gestion et les opérations générales de journalisation. Calculez l'espace pour inclure les surcharges relatives aux éléments suivants :

  - Fichiers journaux
  - Fichiers spécifiques à l'hyperviseur. Par exemple :
    * VMware ajoute des fichiers supplémentaires au dossier de **stockage de la machine virtuelle**. Consultez les meilleures pratiques de VMware.
    * Calculez la taille totale de votre machine virtuelle requise. Considérez une machine virtuelle avec 20 Go pour le disque virtuel, 16 Go pour le fichier d'échange de la machine virtuelle et 100 Mo pour les fichiers journaux, consommant 36,1 Go au total.
  - Instantanés pour XenServer ; Instantanés pour VMware

- Surcharges liées au processus

  La création d'un catalogue, l'ajout d'une machine et la mise à jour d'un catalogue ont des implications de stockage uniques. Par exemple :

  - La création initiale du catalogue nécessite une copie du disque de base à copier sur chaque emplacement de stockage.
    * Vous devez également créer temporairement une machine virtuelle de préparation.
  - L'ajout d'une machine à un catalogue ne nécessite pas la copie du disque de base sur chaque emplacement de stockage. La création du catalogue varie en fonction des fonctionnalités sélectionnées.
  - Mise à jour du catalogue pour créer un disque de base supplémentaire sur chaque emplacement de stockage. Les mises à jour du catalogue connaissent également un pic de

stockage temporaire lorsque chaque machine virtuelle du catalogue dispose de 2 disques Diff pour un certain temps.

Autres considérations :

- **Taille de la RAM :** affecte la taille de certains fichiers et disques de l'hyperviseur, y compris les disques d'optimisation des E/S, le cache en écriture et les fichiers d'instantané.
- **Allocation dynamique/Provisioning fixe :** le stockage NFS est préféré en raison des capacités d'allocation dynamique.

Optimisation du stockage MCS (Machine Creation Services)

Avec la fonctionnalité d'optimisation du stockage MCS (Machine Creation Services), appelée E/S de MCS :

- Le conteneur de cache en écriture est *basé sur fichier*, comme dans Citrix Provisioning. Par exemple, le nom de fichier du cache en écriture Citrix Provisioning est `D:\vdiskdif.vhdx` et le nom de fichier du cache en écriture d'E/S MCS est `D:\mcsdif.vhdx`.
- Vous pouvez améliorer le diagnostic avec la prise en charge d'un fichier de vidage sur incident Windows écrit sur le disque du cache en écriture.
- E/S de MCS conserve la technologie *Cache in RAM with overflow to hard disk* pour fournir une solution de cache en écriture multi-niveaux optimale. Cette fonctionnalité permet à un administrateur de trouver un équilibre entre le coût de chaque niveau, RAM et disque et les performances permettant de répondre aux charges de travail attendues.

Le changement de méthode de cache en écriture de *basé sur disque* vers *basé sur fichier* nécessite les modifications suivantes :

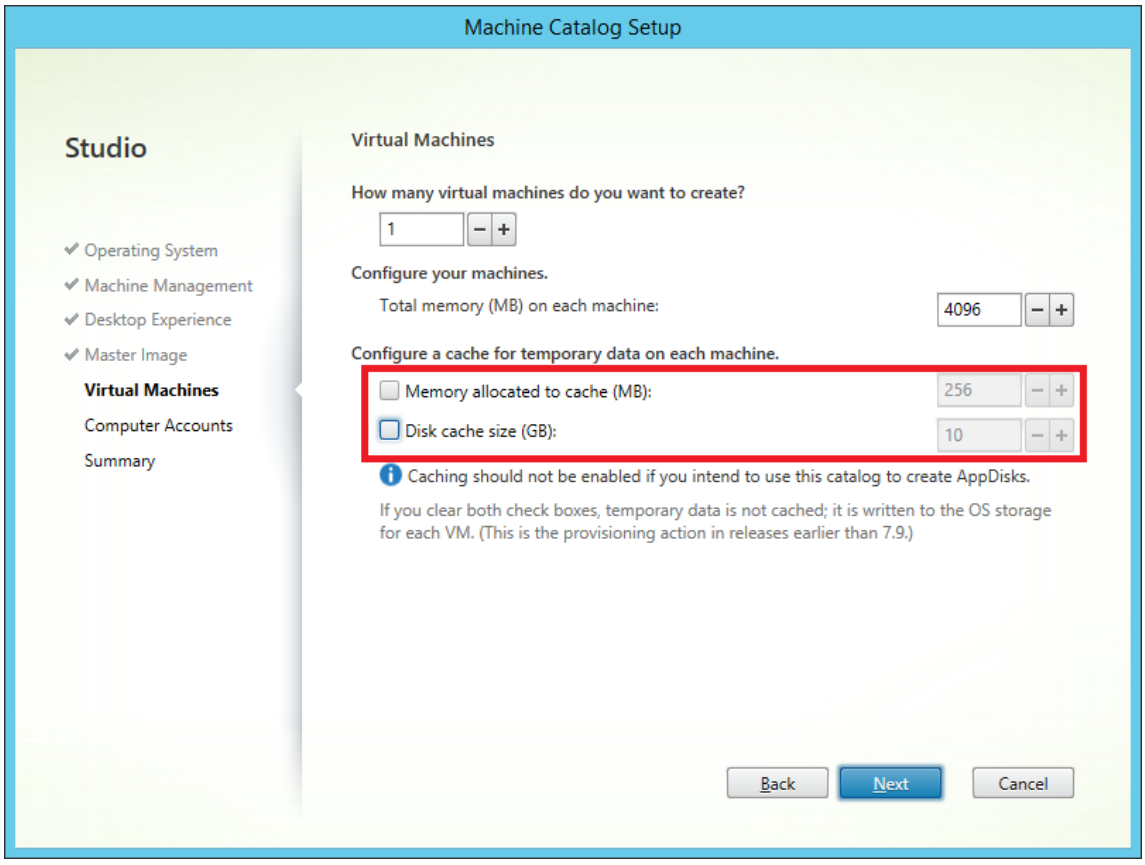
1. Les E/S MCS ne prennent plus en charge le cache RAM uniquement. Spécifiez une taille de disque dans Web Studio lors de la création du catalogue de machines.
2. Le disque de cache en écriture de machine virtuelle est créé et formaté automatiquement lors du démarrage d'une machine virtuelle pour la première fois. Une fois la machine virtuelle activée, le fichier de cache en écriture `mcsdif.vhdx` est écrit dans le volume formaté `MCSWCDisk`.
3. Le fichier d'échange est redirigé vers ce volume formaté, `MCSWCDisk`. Par conséquent, cette taille de disque tient compte de la quantité totale d'espace disque. Elle inclut l'écart entre la taille du disque et la charge de travail générée plus la taille du fichier d'échange. Elle est généralement associée à la taille de la RAM de la machine virtuelle.

Activation des mises à jour de l'optimisation du stockage MCS Pour activer la fonctionnalité d'optimisation du stockage E/S de MCS, mettez à niveau le Delivery Controller et le VDA vers la dernière version de Citrix Virtual Apps and Desktops.

> **Remarque :**
>
> Si vous mettez à niveau un déploiement existant sur lequel E/S de MCS est activé, aucune configuration supplémentaire n'est requise. Le VDA et la mise à niveau du Delivery Controller gèrent la mise à niveau d'E/S de MCS.

Lors de l'activation de la mise à jour de l'optimisation du stockage MCS, tenez compte des points suivants :

- Lors de la création d'un catalogue de machines, l'administrateur peut configurer la RAM et la taille du disque.



- La mise à jour d'un catalogue de machines existant vers un nouvel instantané de machine virtuelle contenant un VDA configuré pour la version 1903 entraîne le comportement suivant : le nouvel instantané continue d'utiliser le paramètre E/S MCS du catalogue existant pour la RAM et la taille du disque. Le disque brut existant est formaté.

> **Important :**
>
> L'optimisation du stockage MCS a été modifiée avec la version 1903 LTSR de Citrix Virtual Apps and Desktops. Cette version qui prend en charge la technologie de cache en écriture basée sur les fichiers offre de meilleures performances et une stabilité optimisée. Les nouvelles fonction-

> nalités fournies par les E/S de MCS peuvent nécessiter un stockage de cache en écriture plus élevé que les versions précédentes de Citrix Virtual Apps and Desktops. Citrix vous recommande de réévaluer la taille du disque pour vous assurer que l'espace disque est suffisant pour le flux de travail et la taille de fichier d'échange alloués. La taille du fichier d'échange est généralement liée à la quantité de RAM système. Si la taille existante du disque du catalogue est insuffisante, créez un catalogue de machines et attribuez un disque de cache en écriture plus grand.

Attribuer une lettre de lecteur spécifique au disque de cache en écriture différée des E/S de MCS

Vous pouvez attribuer une lettre de lecteur spécifique au disque de cache en écriture différée des E/S de MCS. Cette mise en œuvre vous permet d'éviter les conflits entre la lettre de lecteur de toutes les applications que vous utilisez et la lettre de lecteur du disque de cache en écriture différée des E/S de MCS. Pour attribuer une lettre de lecteur au disque de cache en écriture différée des E/S de MCS, vous pouvez utiliser les commandes PowerShell. Les hyperviseurs pris en charge sont Azure, GCP, VMware, SCVMM et XenServer.

> **Remarque :**
>
> Cette fonctionnalité nécessite la version 2305 ou ultérieure du VDA.

Limitations

- Applicable uniquement au système d'exploitation Windows
- Lettre de lecteur applicable pour le disque de cache en écriture différée : E vers Z
- Non applicable lorsque le disque temporaire Azure est utilisé comme disque de cache en écriture différée
- Applicable uniquement lorsque vous créez un catalogue de machines

Attribuer une lettre de lecteur au disque de cache en écriture différée

Pour attribuer une lettre de lecteur à un disque de cache en écriture différée :

1. Ouvrez la fenêtre **PowerShell**.
2. Exécutez `asnp citrix*`.
3. Créez un pool d'identités s'il n'a pas déjà été créé.
4. Créez un schéma de provisioning à l'aide de la commande `New-ProvScheme` associée à la propriété `WriteBackCacheDriveLetter`. Par exemple :


```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
-MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa145ec77.
   manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\abcd-resources.resourcegroup
    \abcd-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\<name>\serviceoffering.
   folder\Standard_D2s_v5.serviceoffering" `
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.
   com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
   true" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
   />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Premium_LRS"/>
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false
   " />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
   false" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"
    />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
   ="false" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   abcd-group1" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
    />
</CustomProperties>'
<!--NeedCopy-->
```

5. Terminez la création du catalogue. Pour de plus amples informations, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Préparer une image principale

Pour de plus amples informations sur la création d'hôtes de connexions, consultez la section Connexions et ressources.

L'image principale contient le système d'exploitation, les applications non virtualisées, le VDA, et d'autres logiciels.

À savoir :

- Une image principale peut également être appelée image clone, image principale, machine virtuelle de base ou image de base. Les fournisseurs d'hôte utilisent des termes différents.
- Assurez-vous que l'hôte a suffisamment de processeurs, de mémoire et de stockage pour accueillir le nombre de machines créées.
- Configurez la bonne taille d'espace disque dur nécessaire pour les ordinateurs de bureau et les applications. Cette valeur ne peut pas être modifiée ultérieurement ou dans le catalogue de machines.
- Les catalogues de machines Remote PC Access ne requièrent pas d'images principales.

Installez et configurez le logiciel suivant sur l'image principale :

- Intégration des outils pour votre hyperviseur (tels que Citrix machine virtuelle Tools, Services d'intégration Hyper-V ou VMware Tools). Si vous ignorez cette étape, vos applications et bureaux risquent de ne pas fonctionner correctement.
- Un VDA. Citrix recommande d'installer la version la plus récente pour autoriser l'accès aux dernières fonctionnalités. Si vous ne parvenez pas à installer un VDA sur l'image principale, la création du catalogue échoue.
- Outils tiers en fonction de vos besoins, tels que le logiciel antivirus ou les agents électroniques de distribution de logiciels. Configurez les services avec les paramètres appropriés pour vos utilisateurs et le type de machine (tels que la mise à jour des fonctionnalités).
- Les applications tierces qui ne sont pas virtualisées. Citrix recommande de virtualiser les applications. Virtualiser les applications réduit de manière significative les coûts en éliminant le besoin de mettre à jour l'image principale après l'ajout ou la reconfiguration d'une application. En outre, moins d'applications installées réduisent la taille des disques durs de l'image principale, ce qui économise les coûts de stockage.
- Les clients App-V avec les paramètres recommandés, si vous souhaitez publier des applications App-V. Le client App-V est disponible auprès de Microsoft.
- Lors de l'utilisation de MCS, si vous localisez Microsoft Windows, installez les paramètres régionaux et les packs de langue. Lors du provisioning, lorsqu'un instantané est créé, les machine virtuelle provisionnées utilisent les variables locales installées et les packs de langue.

> **Important :**
>
> Si vous utilisez MCS, n'exécutez pas Sysprep sur les images principales.

Pour préparer une image principale :

1. À l'aide de l'outil de gestion de votre hyperviseur, créez une image principale, puis installez le système d'exploitation, ainsi que tous les service packs et mises à jour. Indiquez le nombre de processeurs virtuels. Vous pouvez également spécifier le nombre de processeurs virtuels si vous créez le catalogue de machines à l'aide de PowerShell. Vous ne pouvez pas spécifier le nombre de processeurs virtuels lors de la création d'un catalogue à l'aide de Web Studio. Configurez la taille d'espace disque dur nécessaire pour les ordinateurs de bureau et les applications. Cette valeur ne peut pas être modifiée ultérieurement ou dans le catalogue.
2. Assurez-vous que le disque dur de votre ordinateur est connecté à l'emplacement de périphérique 0. La plupart des modèles d'image principale standard configurent cet emplacement par défaut, mais ce n'est peut-être pas le cas de certains modèles personnalisés.
3. Installez et configurez les logiciels répertoriés ci-dessus sur l'image principale.
4. Si vous n'utilisez pas MCS, joignez l'image principale au domaine dont les ordinateurs de bureau et les applications sont membres. Assurez-vous que l'image principale est disponible sur l'hôte sur lequel les machines sont créées. Si vous utilisez MCS, joindre l'image principale à un domaine n'est pas nécessaire. Les machines provisionnées rejoignent le domaine spécifié dans l'assistant de création de catalogue.
5. Citrix vous recommande de créer et de nommer un instantané de l'image principale. Si vous spécifiez une image principale plutôt qu'un instantané lors de la création d'un catalogue, Web Studio crée un instantané. Vous ne pouvez pas le renommer.

Activation des licences en volume

MCS prend en charge l'activation des licences en volume pour automatiser et gérer l'activation des systèmes d'exploitation Windows et de Microsoft Office. Les trois modèles pris en charge par MCS pour l'activation des licences en volume sont les suivants :

- Key Management Service (KMS)
- Activation basée sur Active Directory (ADBA)
- Multiple Activation Key (MAK)

Vous pouvez modifier le paramètre d'activation après avoir créé le catalogue de machines.

Key Management Service (KMS)

KMS est un service léger qui ne nécessite pas de système dédié et peut facilement être co-hébergé sur un système fournissant d'autres services. Cette fonctionnalité est prise en charge sur toutes les ver-

sions de Windows prises en charge par Citrix. Lors de la préparation de l'image, MCS réarme le KMS de Microsoft Windows et Microsoft Office. Vous pouvez ignorer le réarmement en exécutant la commande `Set-Provserviceconfigurationdata`. Pour plus d'informations sur le réarmement du service KMS de Microsoft Windows et Microsoft Office lors de la préparation de l'image, consultez l'article Machine Creation Services: Image Preparation Overview and Fault-Finding. Pour plus d'informations sur l'activation de KMS, consultez Activer à l'aide du service Gestion des clés.

> **Remarque :**
>
> Tous les catalogues de machines créés après l'exécution de la commande `Set-Provserviceconfigurati` ont les mêmes paramètres que ceux fournis dans la commande.

Activation basée sur Active Directory (ADBA)

ADBA vous permet d'activer des machines via leurs connexions de domaine. Les machines sont immédiatement activées lorsqu'elles rejoignent le domaine. Ces machines restent activées tant qu'elles restent jointes au domaine et en contact avec celui-ci. Cette fonctionnalité est prise en charge sur toutes les versions de Windows prises en charge par Citrix, sauf Windows Server 2022. Pour plus d'informations sur l'activation basée sur Active Directory, consultez Effectuer une activation basée sur Active Directory.

Multiple Activation Key (MAK)

La clé MAK permet d'activer le volume et d'authentifier le système Windows à l'aide du serveur Microsoft. Vous devez acheter la clé MAK auprès de Microsoft, à laquelle est attribuée un nombre fixe d'activations. Chaque fois qu'un système Windows est activé, le nombre d'activations diminue. Il existe deux manières d'activer le système :

- Activation en ligne : si le système Windows que vous souhaitez activer dispose d'un accès à Internet, le système active automatiquement Windows lors de l'installation de la clé de produit. Ce processus réduit le nombre d'activations de 1 pour la clé MAK correspondante.
- Activation hors ligne : si le système Windows ne parvient pas à se connecter à Internet pour effectuer l'activation en ligne, MCS obtient un identifiant de confirmation et un identifiant d'installation du serveur Microsoft pour activer le système Windows. Ce mode d'activation est utile pour les catalogues de machines non persistants.

> **Remarque :**
>
> - MCS ne prend pas en charge l'activation de Microsoft Office à l'aide d'une clé d'activation multiple.
> - La version minimale requise du VDA est 2303.

Configuration requise

- Le Delivery Controller doit disposer d'un accès à Internet.
- Créez un nouveau catalogue si la nouvelle image à mettre à jour possède une clé MAK différente de celle d'origine.
- Installez la clé MAK sur l'image principale. Voir Déployer l'activation MAK pour connaître les étapes d'installation de la clé MAK sur un système Windows.
- Si vous n'utilisez pas la préparation d'image :

  1. Ajoutez la valeur DWORD du registre `Manual` sous `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation`.
  2. Définissez la valeur sur 1.

Nombre d'activations Pour afficher le nombre d'activations restantes pour MAK Key ou pour vérifier si une machine virtuelle utilise deux activations ou plus, utilisez l'outil de gestion d'activation de volume (VAMT). Consultez Installer VAMT.

Activer le système Windows à l'aide de MAK Pour activer le système Windows à l'aide de MAK :

1. Installez la clé de produit sur l'image principale. Cette étape utilise une activation.
2. Créez un catalogue de machines MCS.
3. Si vous n'utilisez pas la préparation d'image :

   a) Ajoutez la valeur DWORD du registre `Manual` sous `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation`.
   b) Définissez la valeur sur 1.

   Cette méthode désactive l'option d'activation en ligne.
4. Ajoutez des machines virtuelles au catalogue de machines.
5. Mettez les machines virtuelles sous tension.
6. Selon qu'il s'agit d'une activation en ligne ou hors ligne, le système Windows est activé.

   - Si l'activation est en ligne, le système Windows est activé après l'installation de la clé de produit.
   - Si l'activation est hors ligne, MCS communique avec les machines virtuelles provisionnées pour obtenir l'état d'activation du système Windows. MCS récupère ensuite un identifiant de confirmation et un identifiant d'installation à partir du serveur Microsoft. Ces identifiants sont utilisés pour activer le système Windows.

Dépannage Si la machine virtuelle provisionnée n'est pas activée avec la clé MAK installée, exécutez la commande `Get-ProvVM` ou `Get-ProvScheme`dans une fenêtre PowerShell.

- La commande `Get-ProvScheme` : consultez le paramètre `WindowsActivationType` associé au catalogue de machines MCS à partir de la dernière image principale.
- La commande `Get-ProvVM`. Consultez les paramètres `WindowsActivationType`, `WindowsActivationStatus`, `WindowsActivationStatusErrorCode` et `WindowsActivationStatusError`.

Vous pouvez vérifier l'erreur et vérifier les étapes à suivre pour résoudre le problème.

Créer un catalogue de machines à l'aide de Web Studio

Avant de créer un catalogue :

- Consultez cette section pour en savoir plus sur les choix à effectuer et les informations que vous devez fournir.
- Assurez-vous d'avoir créé une connexion à l'hyperviseur, au service de cloud et aux autres ressources qui hébergent vos machines.
- Si vous avez créé une image principale pour provisionner des machines, assurez-vous d'avoir installé un VDA sur cette image.

Pour lancer l'assistant de création de catalogues :

1. S'il s'agit du premier catalogue que vous créez, vous êtes guidé vers la bonne sélection (telle que « Configurer les machines et créer des catalogues de machines pour exécuter les applications et les bureaux »). L'assistant de création de catalogues s'ouvre.
2. Si vous avez déjà créé un catalogue et que vous souhaitez en créer un autre, procédez comme suit :

    a) Connectez-vous à Web Studio, sélectionnez **Catalogues de machines** dans le volet de gauche, puis sélectionnez **Créer un catalogue de machines** dans la barre d'actions.

    b) Pour organiser les catalogues sous forme de dossiers, créez des dossiers dans le dossier **Catalogues de machines** par défaut. Pour plus d'informations, consultez la section Créer un dossier de catalogues.

    c) Sélectionnez le dossier dans lequel vous souhaitez créer le catalogue, puis cliquez sur **Créer un catalogue de machines**. L'assistant de création de catalogues s'ouvre.

L'assistant vous guide à travers les éléments suivants. Les pages de l'assistant qui s'affichent sont différentes selon les sélections que vous effectuez.

Système d'exploitation

Chaque catalogue contient des machines d'un seul type. Effectuez une sélection.

- **OS multi-session :** un catalogue de systèmes d'exploitation multi-session fournit des bureaux partagés hébergés. Les machines peuvent exécuter des versions prises en charge des systèmes d'exploitation Windows ou Linux, mais le catalogue ne peut pas contenir les deux. (Consultez la documentation VDA Linux pour de plus amples informations sur ce système d'exploitation.)
- **OS mono-session :** un catalogue d'OS mono-session fournit des bureaux VDI que vous pouvez affecter à différents utilisateurs.
- **Remote PC Access :** un catalogue Remote PC Access permet aux utilisateurs d'accéder à distance à leurs machines de bureau de bureau physique. Remote PC Access ne requiert pas de VPN pour fournir la sécurité.

Gestion de machine

Cette page ne s'affiche pas lorsque vous créez des catalogues Remote PC Access.

La page **Gestion des machines** indique la manière dont les machines sont gérées et l'outil que vous utilisez pour déployer les machines.

Indiquez si la gestion de l'alimentation des machines du catalogue est effectuée au travers de Web Studio.

- Machines dont la gestion de l'alimentation est effectuée au travers de Web Studio, des machine virtuelle ou des PC lames par exemple. Cette option n'est disponible que si vous avez déjà configuré une connexion à un hôte.
- La gestion de l'alimentation des machines n'est pas effectuée au travers de Web Studio, les machines physiques par exemple.

Si vous avez indiqué que l'alimentation des machines est gérée au travers de Web Studio, choisissez l'outil à utiliser pour créer des machines virtuelles.

- **Citrix Machine Creation Services (MCS) :** utilise une image principale pour créer et gérer les machines virtuelles. MCS n'est pas disponible pour les machines physiques.
- **Autres :** un outil qui permet de gérer les machines se trouvant déjà dans le centre de données. Citrix vous recommande d'utiliser Microsoft System Center Configuration Manager ou une autre application tierce pour vous assurer que les machines du catalogue sont cohérentes.

Types de bureau (expérience de bureau)

Cette page s'affiche uniquement lors de la création d'un catalogue de machines contenant des machines avec OS mono-session.

La page **Expérience de bureau** détermine ce qui se produit chaque fois qu'un utilisateur ouvre une session. Sélectionnez l'une des options suivantes :

- Les utilisateurs se connectent à un nouveau bureau (aléatoire) chaque fois qu'ils ouvrent une session
- Les utilisateurs se connectent au même bureau (statique) chaque fois qu'ils ouvrent une session.

Image

Cette page s'affiche uniquement lorsque vous utilisez MCS pour créer des machine virtuelle.

1. Sélectionnez un type d'image pour le catalogue de machines, puis sélectionnez une image. Deux types d'images sont disponibles :

   - **Image principale.** Image qui n'a pas été soumise au processus de préparation de l'image. Le processus de préparation de l'image est automatiquement lancé au début de la création du catalogue.

     > **Remarque :**
     >
     > – Lorsque vous utilisez MCS, n'exécutez pas Sysprep sur les images principales.
     > – Si vous spécifiez une image principale plutôt qu'un instantané, Web Studio crée un instantané, mais vous ne pouvez pas le renommer.

   - **Image préparée.** Image soumise au processus de préparation de l'image qui peut être utilisée directement pour la création de machines virtuelles. Opter pour des images préparées plutôt que pour des images principales lors de la création de catalogues garantit une création de catalogues de machines plus rapide et plus fiable, ainsi qu'une gestion rationalisée du cycle de vie des images.

     > **Remarque :**
     >
     > – Les machines virtuelles créées à l'aide d'images préparées ne prennent pas en charge la mise en veille prolongée.
     > – Actuellement, la création de catalogues à l'aide d'images préparées n'est disponible que dans les environnements Azure et VMware.

   Pour plus d'informations sur la création d'images préparées, consultez Gestion des images (Technical Preview).

   Lorsque vous sélectionnez une image, vous pouvez ajouter une note pour l'image sélectionnée si nécessaire.

Pour pouvoir utiliser les dernières fonctionnalités des produits, assurez-vous que la dernière version de VDA est installée sur l'image principale. Ne modifiez pas la sélection de VDA minimale par défaut. Toutefois, si vous devez utiliser une version de VDA antérieure, consultez Versions VDA et niveaux fonctionnels.

Un message d'erreur s'affiche si vous sélectionnez un instantané ou une machine virtuelle qui n'est pas compatible avec la technologie de gestion de machines que vous avez sélectionnée précédemment dans l'assistant.

2. Pour utiliser une machine virtuelle existante comme profil de machine, sélectionnez **Utiliser un profil de machine**, puis sélectionnez la machine virtuelle.

   > **Remarque :**
   >
   > Actuellement, l'utilisation de profils de machine est limitée aux machines virtuelles Azure, AWS, GCP et VMware.

   Pour les déploiements VMware, lorsque vous créez un catalogue de machines à l'aide d'un profil de machine, vous devez spécifier le dossier dans lequel vous souhaitez conserver les machines virtuelles.

   Pour indiquer l'emplacement du dossier de la machine virtuelle, dans l'assistant de création de catalogue, accédez à la page **Machines virtuelles**, puis à la section **Sélectionnez un dossier dans lequel vous souhaitez placer les machines virtuelles**, puis sélectionnez l'emplacement du dossier de la machine virtuelle. S'il n'est pas spécifié, le système considère le dossier du profil de machine sélectionné comme emplacement par défaut.

3. Sélectionnez le niveau fonctionnel minimum pour le catalogue. Pour pouvoir utiliser les dernières fonctionnalités des produits, assurez-vous que la dernière version de VDA est installée sur l'image principale.

Machines

Cette page ne s'affiche pas lorsque vous créez des catalogues Remote PC Access.

Le titre de cette page dépend de ce que vous avez sélectionné sur la page **Gestion des machines** : **Machines**, **Machines virtuelles** ou **machine virtuelle et utilisateurs**.

Lors de l'utilisation de MCS :

- Spécifiez le nombre de machines virtuelles à créer. Entrez **0** (zéro) si vous ne souhaitez pas en créer. Pour créer par la suite des machines virtuelles pour un catalogue vide, effectuez l'opération **Ajouter des machines**.
- Choisissez la quantité de mémoire (Mo) pour chaque machine virtuelle.

- Chaque machine virtuelle créée possède un disque dur. Leur taille est définie dans l'image principale. Vous ne pouvez pas modifier la taille du disque dur dans le catalogue.
- Si votre déploiement contient plusieurs zones, vous pouvez sélectionner une zone pour le catalogue.
- Si vous créez des machines virtuelles de bureau statique, sélectionnez le mode de copie de la machine virtuelle. Voir Mode de copie des machines virtuelles.
- Si vous créez des machines virtuelles de bureau aléatoire qui n'utilisent pas de vDisks, vous pouvez configurer un cache à utiliser pour les données temporaires sur chaque machine. Voir Configurer un cache pour les données temporaires.

Lors de l'utilisation d'autres outils :

Ajoutez (ou importez une liste) les noms de compte de machine Active Directory. Vous pouvez modifier le nom de compte Active Directory pour une machine virtuelle après l'avoir ajoutée/importée. Si vous avez spécifié des machines statiques sur la page **Expérience de bureau**, vous pouvez également spécifier le nom de l'utilisateur Active Directory pour chaque machine virtuelle que vous ajoutez.

Une fois que vous avez ajouté ou importé les noms, vous pouvez utiliser le bouton **Supprimer** pour supprimer les noms de la liste lorsque vous vous trouvez encore sur cette page.

Lors de l'utilisation d'autres outils (mais pas MCS) :

Une icône et une info-bulle pour chaque machine ajoutée (ou importée) vous aident à identifier les machines qu'il peut ne pas être possible d'ajouter au catalogue, ou d'enregistrer auprès d'un Delivery Controller. Pour de plus amples informations, consultez la section Versions VDA et niveaux fonctionnels.

Ajouter des SID lors de la création de machines virtuelles

Vous pouvez désormais ajouter le paramètre `ADAccountSid` pour identifier de manière unique les machines lors de la création de nouvelles machines virtuelles.

Pour ce faire :

1. Créez un catalogue avec le type d'identité pris en charge.
2. Ajoutez des machines au catalogue à l'aide de `NewProvVM`. Par exemple :

```
1 New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID "
     )  -RunAsynchronously
2 <!--NeedCopy-->
```

Toutefois, vous ne pouvez pas provisionner une machine avec :

- Un compte AD qui ne figure pas dans le pool d'identités du catalogue
- Un compte AD qui n'est pas disponible

Mode de copie des machines virtuelles

Le mode de copie que vous spécifiez sur la page **Machines** détermine si MCS crée des clones légers (copie rapide) ou lourds (copie complète) de l'image principale. (Valeur par défaut=clones légers)

- Utilisez le clonage rapide pour créer des machines plus rapidement et utiliser le stockage de manière plus efficace.
- Utilisez la copie complète pour profiter de meilleures performances en matière de recouvrement et de migration des données, tout en réduisant les opérations E/S par seconde une fois que les machines sont créées.

Versions de VDA et niveaux fonctionnels

Le niveau fonctionnel d'un catalogue détermine les fonctionnalités du produit qui sont disponibles pour les machines du catalogue. L'utilisation de fonctionnalités introduites dans les nouvelles versions de produit nécessite un nouveau VDA. Définir un niveau fonctionnel met toutes les fonctionnalités introduites dans cette version (et les versions ultérieures, si le niveau fonctionnel ne change pas) à disposition des machines du catalogue. Toutefois, les machines de ce catalogue avec une version antérieure de VDA ne peuvent pas s'enregistrer.

Un menu dans la partie inférieure de la page **Machines** (ou **Périphériques**) vous permet de sélectionner le niveau minimum de VDA. Cela définit le niveau fonctionnel minimal du catalogue. Par défaut, le niveau fonctionnel le plus courant est sélectionné pour les déploiements locaux. Si vous observez les recommandations de Citrix pour installer et mettre à niveau les composants principaux et les VDA vers la version la plus récente, vous n'avez pas besoin de modifier cette sélection. Toutefois, si vous devez continuer à utiliser des versions antérieures de VDA, sélectionnez la valeur appropriée.

Il est possible qu'une version de Citrix Virtual Apps and Desktops ne comprenne pas une nouvelle version du VDA, ou que le nouveau VDA n'affecte pas le niveau fonctionnel. Dans de tels cas, le niveau fonctionnel peut indiquer une version du VDA antérieure aux composants installés ou mis à niveau. L'article Nouveautés de chaque version indique toute modification du niveau fonctionnel par défaut.

Le niveau fonctionnel sélectionné affecte la liste des machines. Dans la liste, une info-bulle en regard de chaque entrée indique si le VDA de la machine est compatible avec le catalogue à ce niveau fonctionnel.

Des messages sont publiés sur la page si le VDA de chaque machine ne correspond pas ou est supérieur au numéro minimal de niveau fonctionnel sélectionné. Vous pouvez continuer avec l'assistant. Il est probable que ces machines ne puissent pas s'enregistrer auprès d'un Controller ultérieurement. Vous pouvez également effectuer les opérations suivantes :

- Supprimer de la liste les machines contenant une version plus ancienne de VDA, mettre à niveau leurs VDA et les ajouter de nouveau au catalogue.

- Choisissez un niveau fonctionnel bas ; cela empêche l'accès aux dernières fonctionnalités du produit.

Un message est également affiché si une machine n'a pas été ajoutée au catalogue car il ne s'agit pas d'un type de machine correct. Cela peut se produire lors de la tentative d'ajout d'un serveur à un catalogue avec OS mono session ou d'ajout d'une machine avec OS mono-session créée initialement pour une allocation aléatoire à un catalogue de machines statiques.

> **Important :**
>
> Pour la version 1811, un niveau fonctionnel supplémentaire a été ajouté : **1811 (ou plus récent)**. Ce niveau est destiné à être utilisé avec de futures fonctionnalités de Citrix Virtual Apps and Desktops. La valeur par défaut reste **7.9 (ou plus récente)**. Cette valeur par défaut est valide pour tous les déploiements à partir de maintenant.
>
> Si vous sélectionnez **1811 (ou plus récent)**, les versions antérieures de VDA de ce catalogue ne peuvent pas s'enregistrer auprès d'un Controller. Toutefois, si le catalogue ne contient que des VDA de la version 1811 ou ultérieure, ils pourront tous être enregistrés. Cela inclut les catalogues contenant des VDA configurés pour les versions ultérieures de Citrix Virtual Apps and Desktops, y compris la version 1903 et d'autres versions 19XX antérieures à la version actuelle.

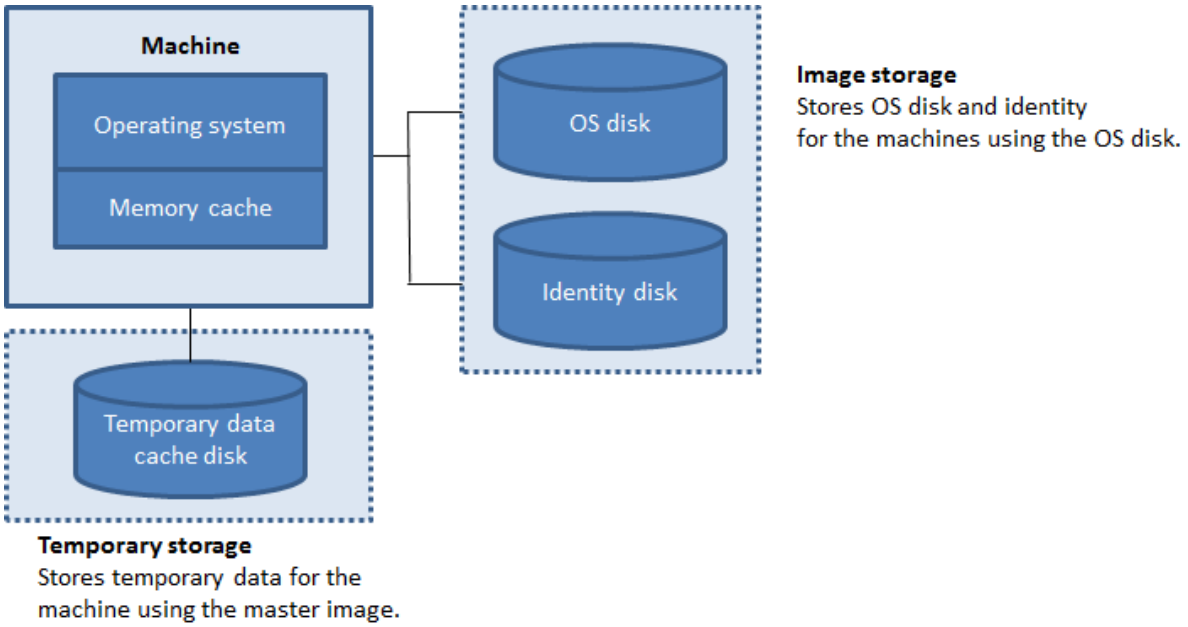
Configurer un cache pour les données temporaires

La mise en cache locale des données temporaires sur la machine virtuelle est facultative. Vous pouvez activer le stockage des données temporaires sur le cache de la machine lorsque vous utilisez MCS pour gérer les machines regroupées (non dédiées) dans un catalogue. Si le catalogue utilise une connexion qui spécifie un stockage des données temporaires, vous pouvez activer et configurer les informations de mise en cache des données temporaires lorsque vous créez le catalogue.

> **Important :**
>
> Cette fonctionnalité nécessite un pilote E/S MCS actuel. L'installation de ce pilote est une option lorsque vous installez ou mettez à niveau un VDA. Par défaut, ce pilote n'est pas installé.

Vous spécifiez si les données temporaires utilisent le stockage local ou partagé lorsque vous créez la connexion que le catalogue utilise. Pour de plus amples informations, consultez les articles Connexions et ressources. Pour configurer un cache pour les données temporaires sur chaque machine, vous pouvez utiliser les deux options suivantes : **Mémoire allouée au cache (Mo)** et **Taille du cache disque (Go)**. Par défaut, les deux options sont désactivées. Pour activer l'option Mémoire allouée au cache (Mo), activez la case à cocher Taille du cache disque (Go). Si la case **Taille du cache disque** n'est pas cochée, l'option **Mémoire allouée au cache** est grisée. Selon le type de connexion, les valeurs par défaut de ces options peuvent différer. Les valeurs par défaut sont suffisantes dans la plupart des cas. Cependant, vous devez prendre en compte l'espace nécessaire pour les éléments suivants :

- Fichiers de données temporaires créés par Windows, y compris le fichier d'échange Windows.
- Données du profil utilisateur.
- Données ShareFile qui sont synchronisées sur les sessions des utilisateurs.
- Données qui peuvent être créées ou copiées par un utilisateur de session ou toute application que les utilisateurs peuvent installer dans la session.



Pour configurer un cache pour les données temporaires sur chaque machine, prenez note des trois scénarios suivants :

- Si vous ne cochez pas la case Taille du cache disque et la case Mémoire allouée au cache, les données temporaires ne sont pas mises en cache. Elles sont écrites sur le disque de différence (situé dans l'espace de stockage du système d'exploitation) pour chaque machine virtuelle. (Il s'agit de l'action de provisioning dans la version 7.8 et les versions antérieures).
- Si vous cochez la case Taille du cache disque et la case Mémoire allouée au cache, les données temporaires sont initialement écrites dans la mémoire cache. Lorsque le cache mémoire atteint sa limite configurée (la valeur Mémoire allouée au cache), les données les plus anciennes sont déplacées vers le cache disque de données temporaire.

> **Important :**
>
> - Si le cache disque vient à manquer d'espace, la session de l'utilisateur devient inutilisable.
> - Cette fonctionnalité n'est pas disponible lors de l'utilisation d'une connexion hôte Nutanix.
> - Vous ne pouvez pas modifier les valeurs de cache dans un catalogue de machines après sa création.
>
> **Remarque :**

- La configuration du cache en écriture différée avec uniquement un cache disque et aucun cache mémoire est obsolète. Pour activer un cache pour les données temporaires, nous vous recommandons de sélectionner à la fois les options **Taille du cache disque (Go)** et **Mémoire allouée au cache (Mo)**, et de spécifier une taille supérieure à 0 pour le cache mémoire.
- La mémoire cache est prise en compte dans le calcul de la quantité totale de mémoire sur chaque machine. Par conséquent, si vous activez l'option Mémoire allouée au cache, envisagez d'augmenter la quantité totale de mémoire sur chaque machine.
- La modification de la taille du cache disque par défaut peut affecter les performances. La taille doit correspondre aux besoins des utilisateurs et à la charge de travail placée sur la machine.

Carte d'interface réseau

Cette page ne s'affiche pas lorsque vous créez des catalogues Remote PC Access.

Sur la page **Cartes d'interface réseau**, si vous prévoyez d'utiliser plusieurs cartes d'interface réseau (NIC), vous devez associer un réseau virtuel avec chaque carte. Par exemple, vous pouvez attribuer une carte pour accéder à un réseau sécurisé spécifique, et une autre carte pour accéder à un réseau plus courant. Vous pouvez également ajouter ou supprimer les cartes d'interface réseau à partir de cette page.

Comptes de machines

Cette page s'affiche uniquement lors de la création de catalogues Remote PC Access.

Sur la page **Comptes de machines**, spécifiez les comptes de machines Active Directory ou des unités d'organisation (OU) à ajouter qui correspondent à des utilisateurs ou des groupes d'utilisateurs. N' utilisez pas de barre oblique (/) dans un nom d'unité d'organisation.

Lorsque vous ajoutez des unités d'organisation, vous pouvez effectuer les opérations suivantes si le domaine n'apparaît pas dans la liste :

- Recherchez-le à l'aide d'une correspondance exacte.
- Parcourez tous les domaines pour le trouver.

Vous pouvez choisir une connexion de gestion de l'alimentation configurée précédemment ou choisir de ne pas utiliser la gestion de l'alimentation. Si vous souhaitez utiliser la gestion de l'alimentation, mais une connexion adéquate n'a pas encore été configurée, vous pouvez créer cette connexion plus tard, puis modifiez le catalogue de machines pour mettre à jour les paramètres de gestion de l'alimentation.

Identités des machines

Cette page s'affiche uniquement lorsque vous utilisez MCS pour créer des machine virtuelle.

Chaque machine du catalogue doit posséder une identité unique. Cette page vous permet de configurer les identités des machines du catalogue. Les machines sont associées à l'identité une fois provisionnées. Vous ne pouvez pas modifier le type d'identité après avoir créé le catalogue.

Veuillez trouver ci-dessous un workflow général pour configurer les paramètres sur cette page :

1. Sélectionnez une identité dans la liste.
2. Indiquez s'il faut créer des comptes ou utiliser des comptes existants, ainsi que l'emplacement (domaine) de ces comptes.

Vous pouvez choisir parmi les options suivantes :

- **Répertoire Active Directory local**. Machines appartenant à une organisation et connectées avec un compte Active Directory appartenant à cette organisation. Elles existent sur site.
- **Joint à Azure Active Directory Hybride**. Machines appartenant à une organisation et connectées avec un compte des services de domaine Active Directory appartenant à cette organisation. Elles existent dans le cloud et sur site. Pour plus d'informations sur les exigences, les limites et les considérations, consultez la section Joint à Azure Active Directory Hybride.

  > **Remarque :**
  >
  > - Avant de pouvoir utiliser Joint à Azure Active Directory Hybride, assurez-vous que votre environnement Azure répond aux conditions préalables. Voir https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains.
  > - Cette option nécessite que l'image principale réponde aux exigences du système d'exploitation. Pour de plus amples informations, consultez la documentation de Microsoft : https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid.

> **Important :**
>
> - Si vous sélectionnez **Active Directory local** ou **Joint à Azure Active Directory Hybride** comme type d'identité, chaque machine du catalogue doit avoir un compte d'ordinateur Active Directory correspondant.

Si vous créez des comptes, vous devez être autorisé à créer des comptes d'ordinateur dans l'unité d'organisation où les machines résident. Chaque machine du catalogue doit porter un nom unique. Spécifiez le schéma de dénomination des comptes pour les machines que vous souhaitez créer. Pour plus d'informations, consultez Schéma d'affectation de nom de comptes de machines.

> **Remarque :**
>
> Assurez-vous que les noms des unités d'organisation n'utilisent pas de barres obliques (/).

Si vous utilisez des comptes existants, vous pouvez sélectionner les comptes ou cliquez sur **Importer** et spécifiez un fichier .csv contenant les noms de compte. Le contenu du fichier importé doit utiliser le format suivant :

- [ADComputerAccount]nomcompteordinateurAD.domaine

Assurez-vous qu'il existe suffisamment de comptes pour toutes les machines que vous ajoutez. L'interface Web Studio gère ces comptes. Par conséquent, autorisez cette interface à réinitialiser les mots de passe de tous les comptes ou spécifiez le mot de passe de compte (qui doit être le même pour tous les comptes).

Pour les catalogues contenant des machines physiques ou des machines existantes, sélectionnez ou importez des comptes existants et attribuez chaque machine à un compte d'ordinateur Active Directory et à un compte d'utilisateur.

Schéma d'affectation de nom de comptes de machines

Chaque machine d'un catalogue doit porter un nom unique. Vous devez spécifier un schéma d'affectation de nom de comptes de machines lors de la création d'un catalogue. Utilisez des caractères génériques (marques de hachage) comme espaces réservés pour les chiffres ou les lettres séquentiels qui apparaissent dans le nom.

Lorsque vous spécifiez un schéma d'affectation de nom, tenez compte des règles suivantes :

- Le schéma d'affectation de nom doit contenir au moins un caractère générique. Vous devez rassembler tous les caractères génériques.
- Le nom complet, y compris les caractères génériques, doit contenir au moins 2 mais pas plus de 15 caractères. Il doit inclure au moins un caractère non numérique et un caractère # (générique).
- Le nom ne doit pas contenir d'espace ni aucun des caractères suivants : `,~!@'$%^&.()} {\/*?"<>|=+[];:_".`.
- Le nom ne peut pas se terminer par un trait d'union (-).

En outre, laissez suffisamment de place à la croissance lorsque vous spécifiez le schéma d'affectation de nom. Prenons l'exemple suivant : si vous créez 1 000 comptes de machines avec le schéma « veryverylong# », le dernier nom de compte créé (veryverylong1000) contient 16 caractères. Le schéma d'affectation de nom produit donc un ou plusieurs noms de machines qui dépassent le maximum de 15 caractères.

Vous pouvez indiquer si les valeurs séquentielles sont des chiffres (0-9) ou des lettres (A-Z) :

- **0-9**. Si cette option est sélectionnée, les caractères génériques spécifiés sont résolus en numéros séquentiels.

  > **Remarque :**
  >
  > S'il n'y a qu'un seul caractère générique (#), les noms de compte commencent par 1. S'il y en a deux, les noms de compte commencent par 01. S'il y en a trois, les noms de compte commencent par 001, et ainsi de suite.

- **A-Z**. Si cette option est sélectionnée, les caractères génériques spécifiés sont résolus en lettres séquentielles.

Par exemple, un principe de dénomination de PC-Sales-## (avec **0-9** sélectionné) dans les comptes d'ordinateur nommés PC-Sales-01, PC-Sales-02, PC-Sales-03, etc.

Vous pouvez également spécifier par quoi commencent les noms de compte.

- Si vous sélectionnez **0 à 9**, les comptes sont nommés de manière séquentielle, en commençant par les numéros spécifiés. Entrez un ou plusieurs chiffres, selon le nombre de caractères génériques que vous utilisez dans le champ précédent. Par exemple, si vous utilisez deux caractères génériques, saisissez deux chiffres ou plus.
- Si vous sélectionnez **A à Z**, les comptes sont nommés de manière séquentielle, en commençant par les lettres spécifiées. Entrez une ou plusieurs lettres, selon le nombre de caractères génériques que vous utilisez dans le champ précédent. Par exemple, si vous utilisez deux caractères génériques, saisissez deux lettres ou plus.

Informations d'identification du domaine

Sélectionnez **Entrer informations d'identification**, puis entrez les informations d'identification d'un administrateur autorisé à effectuer des opérations de compte dans le domaine Active Directory cible.

Utilisez l'option **Vérifier le nom** pour vérifier si le nom d'utilisateur est valide ou unique. Cette option est utile, par exemple, lorsque :

- Le même nom d'utilisateur existe dans plusieurs domaines. Vous êtes invité à sélectionner l'utilisateur souhaité.
- Vous ne vous souvenez pas du nom de domaine. Vous pouvez saisir le nom d'utilisateur sans spécifier le nom de domaine. Si la vérification réussit, le nom de domaine est automatiquement renseigné.

> **Remarque :**
>
> Si le type d'identité que vous avez sélectionné dans **Identités des machines** est défini sur **Joint**

> **à Azure Active Directory Hybride**, les informations d'identification que vous entrez doivent avoir reçu l'autorisation `Write userCertificate`.

Résumé, nom et description

Sur la page **Résumé**, vérifiez les paramètres que vous avez spécifiés. Entrez un nom et une description pour le catalogue. Ces informations s'affichent dans Web Studio.

Lorsque vous avez terminé, cliquez sur **Terminer** pour démarrer la création du catalogue.
Lorsque vous avez terminé, sélectionnez **Terminer** pour démarrer la création du catalogue.

Dans **Catalogues de machines**, le nouveau catalogue apparaît avec une barre de progression intégrée.

Pour afficher les détails de la progression de la création :

1. Passez la souris sur le catalogue de machines.
2. Dans l'info-bulle qui apparaît, cliquez sur **Afficher les détails**.

   Un graphique de progression étape par étape apparaît dans lequel vous pouvez voir les éléments suivants :

   - Historique des étapes
   - Progression et durée de l'étape en cours
   - Étapes restantes

Synchronisation de l'heure MCS

La synchronisation de l'heure est déterminée par l'image principale et le type de catalogue joint aux identités de machines. Vous obtenez la méthode de synchronisation de l'heure suivante en fonction de l'image principale et du catalogue :

L'image principale	Catalogue	Méthode de synchronisation de l'heure résultante
NDJ	AD ou Azure AD Hybride	Par défaut, NT5DS. Vous pouvez empêcher MCS de modifier les paramètres de synchronisation de l'heure à l'aide des paramètres de registre de l'image principale

L'image principale	Catalogue	Méthode de synchronisation de l'heure résultante
NDJ	NDJ ou Azure AD	Identique au paramètre de synchronisation de l'heure d'origine
AD ou Azure AD Hybride	AD ou Azure AD Hybride	Identique au paramètre de synchronisation de l'heure d'origine
Azure AD	Azure AD	Identique au paramètre de synchronisation de l'heure d'origine

> **Remarque :**
>
> La synchronisation de l'heure d'origine est contrôlée par le paramètre de registre suivant et ne peut pas être modifiée :
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config
>
> Valeur : MaxAllowedPhaseOffset, MaxNegPhaseCorrection et MaxPosPhaseCorrection
>
> - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters
>
> Valeur : Type

Pour empêcher MCS de modifier le paramètre de synchronisation de l'heure, définissez la valeur du paramètre de registre suivant dans l'image principale :

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- Nom : TimeSyncMethodKeep
- Type : DWORD
- 0 (ou valeur de TimeSyncMethodKeep non configurée) : ne conserve pas le paramètre de synchronisation de l'heure d'origine.
- 1 : conserve le paramètre de synchronisation de l'heure d'origine et les valeurs des paramètres par défaut.

Considérations importantes concernant la définition de propriétés personnalisées

Les propriétés personnalisées doivent être définies correctement sur `New-ProvScheme` et `Set-ProvScheme` dans les environnements GCP et Azure. Si vous spécifiez une ou plusieurs propriétés

personnalisées inexistantes, le message d'erreur suivant s'affiche et les commandes ne s'exécutent pas.

- Dans Azure : `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`
- Dans GCP : `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`

Dépannage

> **Important :**
>
> Après avoir créé le catalogue de machines à l'aide de Web Studio, vous ne pouvez plus utiliser la commande PowerShell `Get-ProvTask` pour récupérer les tâches associées à la création de catalogues de machines. Cette restriction résulte du fait que Web Studio supprime ces tâches après la création du catalogue de machines, que le catalogue soit créé avec succès ou non.

Citrix recommande de collecter des journaux pour aider l'équipe de support à fournir des solutions. Utilisez la procédure suivante pour générer des fichiers journaux lors de l'utilisation de Citrix Provisioning :

1. Sur l'image principale, créez la clé de Registre suivante avec la valeur 1 (pour valeur DWORD (32 bits)) : `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Arrêtez l'image principale et créez un instantané.
3. Exécutez la commande PowerShell suivante sur le Delivery Controller : `Set-ProvServiceConfigurati -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Créez un catalogue basé sur cet instantané.
5. Lorsque la machine virtuelle de préparation est créée sur l'hyperviseur, connectez-vous et extrayez les fichiers suivants dans la racine de C:\: Image-prep.log and Pvsmachine virtuelleAgent-Log.txt.
6. Arrêtez la machine ; à ce stade, elle signale l'échec.
7. Exécutez la commande PowerShell suivante pour réactiver l'arrêt automatique des machines de préparation d'image : `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`.

Problèmes de préparation d'image

Étant donné que MCS crée de nombreuses machines à partir d'une seule image, certaines étapes sont nécessaires pour s'assurer que toutes les machines sont uniques et disposent des licences appro-

priées. La préparation de l'image fait partie du processus de création du catalogue. Cette préparation garantit que toutes les machines provisionnées ont des adresses IP uniques et s'annoncent correctement auprès du serveur KMS en tant qu'instances uniques. Dans MCS, la préparation de l'image se produit après la sélection de l'instantané de l'image principale. Une copie est effectuée pour permettre au catalogue de s'isoler de la machine sélectionnée. Une machine virtuelle de *préparation* est créée, basée sur la machine virtuelle d'origine, mais sans connexion réseau. La déconnexion du réseau empêche les conflits avec d'autres machines, tout en s'assurant que la machine virtuelle préparée est uniquement attachée au disque nouvellement copié.

Un petit disque *d'instruction* contenant les étapes requises pour exécuter la préparation de l'image est attaché à la machine virtuelle préparée. Cette machine virtuelle préparée démarre et le processus de préparation de l'image commence. La préparation de l'image comprend les processus suivants :

- Activer DHCP. L'activation de DHCP garantit que les machines provisionnées ne provoquent pas de conflits d'adresses IP. DHCP est activé sur toutes les cartes réseau.
- Réarmer Microsoft Windows KMS. La réarmement de KMS garantit que Microsoft Windows fonctionne sous la licence appropriée. Le système d'exploitation réarmé est invoqué de sorte qu'il est correctement signalé comme nouvelle instance au serveur de licences KMS.
- Réarmer Microsoft Office KMS (si Microsoft Office est installé). Réarmer Microsoft Office garantit que toute version de Microsoft Office (2010+) est correctement enregistrée auprès de son serveur KMS. Lorsque Microsoft Office est appelé, une fois réarmé, il est signalé comme nouvelle instance au serveur de licences KMS.

> **Conseil :**
>
> Lorsque le processus de préparation de l'image se termine, le disque d'instruction est obtenu à partir de l'hyperviseur. L'hyperviseur contient les informations recueillies lors du processus de préparation de l'image.

Il y a diverses raisons pour lesquelles l'étape de préparation de l'image peut échouer. Un message d'échec similaire au suivant s'affiche : « Échec du réarmement de préparation de l'image Office ».

Ces échecs sont abordés dans les sections suivantes.

Activer DHCP Ces échecs sont causés par des cartes réseau qui ne prennent pas en charge les adresses IP statiques. Par exemple, les versions antérieures des cartes réseau Dell SonicWall. L'opération a échoué car une carte SonicWall est une carte réseau de pare-feu. Par conséquent, définir la carte sur DHCP n'a aucun sens car cette configuration ne prend en charge que DHCP. Ce problème a été corrigé dans les versions ultérieures de Citrix Virtual Apps and Desktops. Toutefois, s'il est détecté avec d'autres types d'adaptateurs réseau, il doit être signalé à Citrix via les forums ou votre contact de support.

> **Remarque :**
>
> Ce paramètre PowerShell dans les exemples suivants est appliqué au site Citrix Virtual Apps and Desktops, de sorte qu'il affecte tous les nouveaux catalogues et mises à jour d'images effectuées sur les catalogues existants.

Si vous rencontrez ce problème avec d'autres cartes réseau, vous pouvez le résoudre en exécutant une commande PowerShell sur le Delivery Controller :

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value EnableDHCP
```

Réarmer Microsoft Office Plusieurs échecs de réarmement de KMS peuvent survenir au cours de l'étape de réarmement de Microsoft Office. Les principaux échecs sont :

- Certains runtimes Microsoft Office, par exemple **Access Runtime**, peuvent invoquer le réarmement Office, ce qui provoque un échec.
- Une version KMS de Microsoft Office n'est pas installée.
- Nombre de réarmements dépassé.

Si l'erreur est un faux positif, vous pouvez la résoudre en exécutant la commande PowerShell suivante sur le Delivery Controller :

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OfficeRearm
```

Réarmer Microsoft Windows Divers échecs KMS peuvent survenir au cours de l'étape de réarmement de Microsoft Windows. Les principaux échecs sont :

- La version de Windows installée n'est pas activée à l'aide de KMS. Par exemple, elle utilise une clé d'activation multiple (MAK).
- Nombre de réarmements dépassé.

Si la version de Microsoft Windows est couverte par la licence appropriée, vous pouvez effacer le réarmement du système d'exploitation en exécutant la commande PowerShell suivante sur le Delivery Controller :

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OsRearm
```

Instances d'échec complet La machine de préparation d'image n'étant pas connectée au réseau par sa conception, parfois l'étape de préparation de l'image ne peut signaler qu'un échec complet. Un

exemple de ce type d'échec ressemble à : Échec de préparation de l'image de machine virtuelle principale. Assurez-vous que l'image sélectionnée est dotée d'un système d'exploitation pris en charge (par exemple, Windows 7) et que la version correcte de VDA (7.0 ou version supérieure) est installée.

Les principales raisons d'un échec complet sont :

Virtual Delivery Agent (VDA) n'est pas installé ou VDA version 5.x est installé Si le VDA 7.x n'est pas installé sur l'image principale, la préparation de l'image prend fin au bout de 20 minutes et signale l'erreur ci-dessus. Cela s'explique par le fait qu'aucun logiciel n'est installé sur l'image principale pour exécuter l'étape de préparation de l'image et signaler le succès ou l'échec. Pour résoudre ce problème, assurez-vous que le VDA (version minimale 7) est installé sur l'instantané sélectionné comme image principale.

Stratégie `DISKPART SAN` L'ensemble de l'étape de préparation de l'image peut échouer en raison de la stratégie `DISKPART SAN` définie sur l'image principale. Si elle n'est pas configurée pour mettre en ligne le disque d'instructions de préparation d'image, la machine est arrêtée et la préparation de l'image signale un échec après 20 minutes. Pour vérifier cela sur l'image principale, exécutez les commandes suivantes :

```
C:>; Diskpart.exe
DISKPART>; San
<!--NeedCopy-->
```

Cette commande renvoie la stratégie actuelle. Si ce n'est pas *Mettre en ligne tous les disques*, modifiez-la en exécutant la commande suivante :

```
DISKPART>; San policy=OnlineAll
```

Arrêtez l'image principale, créez un instantané de cette machine, puis utilisez-le comme image MCS de base.

Si la préparation de l'image échoue pour une autre raison Si la préparation de l'image échoue sans raison évidente, vous pouvez contourner le processus de préparation d'image lors de la création d'un catalogue MCS. Toutefois, le contournement de ce processus peut entraîner des problèmes avec les licences et la mise en réseau KMS (DHCP) sur votre site. Utilisez la commande PowerShell suivante :

```
Set-ProvServiceConfigurationData -Name
    ImageManagementPrep_DoImagePreparation -Value $false
<!--NeedCopy-->
```

Dans la mesure du possible, collectez des journaux pour l'équipe de support Citrix. Signalez le problème à Citrix via les forums ou via votre contact de support. Pour collecter les journaux :

1. Sur l'image principale, créez la clé de Registre suivante avec la valeur 1 (pour valeur DWORD (32 bits)) : `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Arrêtez l'image principale et créez un instantané. Sur le Delivery Controller, démarrez PowerShell, avec les composants logiciels enfichables Citrix PowerShell chargés et exécutez `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
3. Créez un catalogue basé sur cet instantané.
4. Lorsque la machine virtuelle de préparation est créée sur l'hyperviseur, connectez-vous et extrayez les fichiers suivants dans la racine de C:\:

```
Image-prep.log
PvsVmAgentLog.txt
<!--NeedCopy-->
```

Arrêtez la machine. À ce stade, l'échec est signalé.

Exécutez la commande PowerShell suivante pour réactiver l'arrêt automatique des machines de préparation d'image :

```
Remove-ProvServiceConfigurationData -Name
ImageManagementPrep_NoAutoShutdown
```

Autres ressources

Pour plus d'informations sur la création de catalogues de services cloud spécifiques, consultez :

- Créer un catalogue AWS
- Créer un catalogue XenServer
- Créer un catalogue Google Cloud Platform
- Créer un catalogue Microsoft Azure
- Créer un catalogue Microsoft System Center Virtual Machine Manager
- Créer un catalogue Nutanix
- Créer un catalogue VMware

S'il s'agit du premier catalogue créé, Web Studio vous explique comment créer un groupe de mise à disposition.

Pour passer en revue l'ensemble du processus de configuration, consultez la section Installer et configurer.

Vous pouvez créer un catalogue Citrix Provisioning à l'aide de l'interface Configuration complète et de PowerShell.
Cette implémentation vous offre les avantages suivants :

- Une console unifiée unique pour gérer à la fois les catalogues MCS et Citrix Provisioning.

- Bénéficiez de nouvelles fonctionnalités pour les catalogues Citrix Provisioning, telles qu'une solution de gestion des identités, un provisioning à la demande, etc.

Actuellement, cette fonctionnalité n'est disponible que pour les charges de travail Azure et VMware. Toutefois, dans les environnements VMware, vous pouvez actuellement créer des catalogues uniquement à l'aide des commandes PowerShell. Pour plus d'informations, consultez la section Créer des catalogues Citrix Provisioning dans Citrix Studio.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de différents types de jointure
- Gérer des catalogues de machines

Créer un catalogue AWS

June 27, 2024

La section Créer des catalogues de machines décrit les assistants qui permettent de créer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements de virtualisation AWS.

> **Remarque :**
>
> Avant de créer un catalogue AWS, vous devez terminer la création d'une connexion à AWS. Voir Connexion à AWS.

Paramètre réseau lors de la préparation de l'image

Lors de la préparation de l'image, une machine virtuelle (machine virtuelle) de préparation est créée sur la base de la machine virtuelle d'origine. Cette machine virtuelle de préparation est déconnectée du réseau. Pour déconnecter le réseau de la machine virtuelle de préparation, un groupe de sécurité réseau est créé pour refuser tout trafic entrant et sortant. Ce groupe de sécurité réseau persiste et est réutilisé. Le nom du groupe de sécurité réseau est `Citrix.XenDesktop.IsolationGroup-GUID` où le GUID est généré de manière aléatoire.

Configurer la location AWS

AWS propose les options de location suivantes :

- Location partagée (type par défaut) : plusieurs instances Amazon EC2 provenant de clients différents peuvent résider sur le même matériel physique.
- Location dédiée : vos instances EC2 s'exécutent uniquement sur du matériel avec d'autres instances que vous avez déployées. Les autres clients n'utilisent pas le même matériel.

Vous pouvez utiliser MCS pour provisionner des hôtes AWS dédiés à l'aide de PowerShell.

Configurer la location d'hôte dédié AWS à l'aide de PowerShell

Un administrateur peut créer un catalogue de machines avec location d'hôte définie via PowerShell.

Un hôte Amazon [EC2] dédié est un serveur physique avec une capacité d'instance [EC2] entièrement dédiée, ce qui vous permet d'utiliser les licences logicielles par socket ou par machine virtuelle.

Les hôtes dédiés ont une utilisation prédéfinie basée sur le type d'instance. Par exemple, un hôte dédié alloué de types d'instance C4 Large ne peut pas exécuter plus de 16 instances. Consultez le site AWS pour plus d'informations.

La configuration requise pour le provisioning des hôtes AWS est la suivante :

- Une image importée (AMI) BYOL (apportez votre propre licence). Avec des hôtes dédiés, utilisez et gérez vos licences existantes.
- Une allocation d'hôtes dédiés avec une utilisation suffisante pour satisfaire les demandes de provisioning.
- Activer le **placement automatique**.

Pour mettre à disposition un hôte dédié dans AWS à l'aide de PowerShell, utilisez l'applet de commande **New-ProvScheme** avec le paramètre `TenancyType` défini sur *Host*.

Pour plus d'informations, reportez-vous à la documentation de développeur Citrix.

Capturez les propriétés des machines à partir d'AMI

Lorsque vous créez un catalogue pour provisionner des machines à l'aide de Machine Creation Services (MCS) dans AWS, vous sélectionnez une AMI pour représenter l'image maître/principale de ce catalogue. À partir de cette AMI, MCS utilise un instantané du disque. Dans les versions précédentes, pour avoir des rôles ou des balises sur vos machines, vous utilisiez la console AWS pour les définir individuellement. Cette fonctionnalité est activée par défaut.

> **Conseil :**
>
> Pour utiliser la capture de propriétés d'instance AWS, une machine virtuelle doit être associée à l'AMI.

Pour améliorer ce processus, **MCS** lit les propriétés de l'instance à partir de laquelle l'AMI a été prise et applique le rôle IAM (Identity Access Management) et les balises de la machine aux machines provisionnées pour un catalogue donné. Lors de l'utilisation de cette fonctionnalité facultative, le processus de création du catalogue recherche l'instance source de l'AMI sélectionnée, en lisant un ensemble limité de propriétés. Ces propriétés sont ensuite stockées dans un modèle de lancement AWS, qui est utilisé pour provisionner des machines pour ce catalogue. Toute machine du catalogue hérite des propriétés d'instance capturées.

Les propriétés capturées incluent :

- Rôles IAM : appliqués aux instances provisionnées
- Balises : appliquées aux instances provisionnées, à leur disque et aux cartes réseau. Ces balises sont appliquées aux ressources Citrix transitoires, notamment : compartiment et objets S3, AMI, instantanés et modèles de lancement.

> **Conseil :**
>
> Le balisage des ressources Citrix transitoires est facultatif et est configurable à l'aide de la propriété personnalisée `AwsOperationalResourcesTagging`.

Capturer les propriétés d'instance AWS

Vous pouvez utiliser cette fonctionnalité en spécifiant une propriété personnalisée, `AwsCaptureInstanceProp`, lors de la création d'un schéma de provisioning pour une connexion d'hébergement AWS :

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
...<standard provscheme parameters
```

Pour plus d'informations, reportez-vous à la documentation de développeur Citrix.

> **Remarque :**
>
> `AwsCaptureInstanceProperties` est obsolète. Nous vous recommandons plutôt d'utiliser des profils de machine pour spécifier les propriétés des machines virtuelles.

Capturez les propriétés des machines à partir de profils de machines

Lorsque vous créez un catalogue pour provisionner des machines AWS à l'aide de MCS, vous pouvez utiliser un profil de machine pour prédéfinir certains paramètres de propriétés de machine.

Pour ce faire, suivez cette procédure :

1. Stockez les profils de machine dans la même zone de disponibilité que les ressources dans lesquelles vous créez ce catalogue.

2. Sur la page **Modèle de machine** de l'assistant de création de catalogue, sélectionnez **Utiliser un profil de machine**. Les profils de machine situés dans la même zone de disponibilité que les ressources que vous avez sélectionnées s'affichent.
3. Sélectionnez un profil de machine selon vos besoins.

> **Remarque :**
>
> Vous pouvez utiliser un profil de machine ou une AMI pour capturer les propriétés de la machine. Dans Web Studio, lorsque vous sélectionnez **Utiliser un profil de machine**, l'option **Appliquer les propriétés du modèle de machine aux machines virtuelles** est automatiquement masquée.

Baliser une ressource opérationnelle

Lorsque vous créez un catalogue pour provisionner des machines dans AWS à l'aide de MCS, vous pouvez contrôler si le rôle IAM et les propriétés de balise doivent être appliqués à ces machines. Vous pouvez également contrôler si vous souhaitez appliquer des balises de machine aux ressources opérationnelles.

Une image de machine Amazon (AMI) représente un type d'appliance virtuelle utilisée pour créer une machine virtuelle dans l'environnement Amazon Cloud, communément appelé EC2. Vous devez utiliser une AMI pour déployer des services qui utilisent l'environnement EC2. Lorsque vous créez un catalogue pour provisionner des machines à l'aide de MCS pour AWS, vous sélectionnez l'**AMI** en tant qu'image principale pour ce catalogue.

> **Important :**
>
> La création de catalogues en capturant une propriété d'instance et un modèle de lancement est nécessaire pour utiliser le balisage des ressources opérationnelles.

Pour créer un catalogue AWS, vous devez d'abord créer une AMI pour l'instance qui sera l'image principale. MCS lit les balises de cette instance et les incorpore dans le modèle de lancement. Les balises du modèle de lancement sont ensuite appliquées à toutes les ressources Citrix créées dans votre environnement AWS, notamment :

- Machines virtuelles
- Disques machine virtuelle
- Interfaces réseau machine virtuelle
- Compartiments S3
- Objets S3
- Modèles de lancement
- AMI

Baliser une ressource opérationnelle

Pour utiliser PowerShell pour baliser des ressources :

1. Ouvrez une fenêtre PowerShell à partir de l'hôte DDC.
2. Exécutez la commande `asnp citrix` pour charger des modules PowerShell spécifiques à Citrix.

Pour baliser une ressource pour une machine virtuelle provisionnée, utilisez la nouvelle propriété personnalisée, `AwsOperationalResourcesTagging`. La syntaxe de cette propriété est la suivante :

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true"...<standard provscheme parameters
>
```

Autres ressources

- S'il s'agit du premier catalogue créé, Web Studio vous explique comment créer un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, consultez la section Installer et configurer.
- Pour gérer les catalogues, consultez Gérer les catalogues de machines et Gérer un catalogue AWS

Copier des balises sur des machine virtuelle

Vous pouvez copier des balises des cartes d'interface réseau et des disques (disque d'identité, disque cache en écriture différée et disque du système d'exploitation) spécifiés dans le profil de la machine vers des machines virtuelles nouvellement créées dans un catalogue de machines MCS. Vous pouvez spécifier ces balises dans n'importe quelle source de profil de machine (instance AWS de machine virtuelle ou version du modèle de lancement AWS). Cette fonctionnalité s'applique aux catalogues de machines et de machine virtuelle persistants et non persistants.

> **Remarque :**
>
> - Sur la console AWS EC2, vous ne pouvez pas voir les valeurs des **interfaces réseau de balises** sous les **balises de ressource de version du modèle de lancement**. Cependant, vous pouvez exécuter la commande PowerShell `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` pour voir les spécifications des balises.

> - Si une source de profil de machine (version de machine virtuelle ou de modèle de lancement) possède deux interfaces réseau (eni-1 et eni-2) et que eni-1 possède la balise t1 et eni-2 la balise t2, la machine virtuelle obtient les balises des deux interfaces réseau.

Créer un catalogue à l'aide d'un profil de machine

Lorsque vous créez un catalogue pour provisionner des machines à l'aide de Machine Creation Services (MCS) dans AWS, vous pouvez désormais utiliser un profil de machine pour capturer les propriétés matérielles d'une instance EC2 (machine virtuelle) ou une version de modèle de lancement et les appliquer aux machines provisionnées. Les propriétés capturées peuvent inclure, par exemple, les propriétés du volume EBS, le type d'instance, l'optimisation EBS et d'autres configurations AWS prises en charge. Lors de la modification du catalogue, le profil des machines provisionnées peut être modifié en fournissant une machine virtuelle ou un modèle de lancement différent.

> **Remarque :**
>
> Les propriétés de volume EBS sont uniquement dérivées d'un profil de machine.

Remarques importantes

Points importants à prendre en considération lors de la création d'un catalogue de machines MCS :

- Si vous ajoutez les paramètres des propriétés matérielles d'une machine dans les commandes `New-ProvScheme` et `Set-ProvScheme`, les valeurs fournies dans les paramètres remplacent les valeurs du profil de la machine.
- Si vous définissez `AwsCaptureInstanceProperties` comme **`true`** et ne définissez pas la propriété `MachineProfile`, seuls les rôles et les balises IAM sont capturés.
- Vous ne pouvez pas régler `AwsCaptureInstanceProperties` et`MachineProfile` en même temps.

  > **Remarque :
  >
  > `AwsCaptureInstanceProperties` est obsolète.

- Vous devez indiquer explicitement les valeurs des propriétés suivantes :
  - TenancyType
  - Groupe de sécurité
  - Carte d'interface réseau ou réseau virtuel
- Vous ne pouvez activer `AwsOperationalResourcesTagging` que si vous activez `AwsCaptureInstanceProperties` ou spécifiez un profil de machine.

Points importants à prendre en considération après la création d'un catalogue de machines MCS :

- Seules les nouvelles machines virtuelles ajoutées au catalogue sont concernées par la modification.
- Vous ne pouvez pas redéfinir un catalogue reposant sur un profil de machine en tant que catalogue ne reposant pas sur un profil de machine.

Créer un catalogue de machines à l'aide d'un profil de machine

Pour créer un catalogue de machines à l'aide d'un profil de machine :

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Créez un pool d'identités s'il n'a pas déjà été créé. Par exemple,

```
1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
     Domain abcdf -NamingSchemeType Numeric
2 <!--NeedCopy-->
```

4. Exécutez la commande New-ProvScheme. Par exemple :

```
1 New-ProvScheme -ProvisioningSchemeName demet-test-1
2 -HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
3 -IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
4 -CleanOnBoot
5 -MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
     demet-ami.0 (ami-0ca813xxxxxx061ef).template'
6 -MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east
     -1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).
     vm'
7 <!--NeedCopy-->
```

5. Terminez la création du catalogue. Pour plus d'informations, accédez à cette page sur le SDK Citrix PowerShell.

Pour mettre à jour le profil de machine sur un catalogue initialement provisionné avec un profil de machine, procédez comme suit :

1. Exécutez la commande `Set-ProvScheme`. Par exemple,

```
1 Set-ProvScheme `
2 -ProvisioningSchemeUid "<ID" `
3 -MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
     availabilityzone\citrix-cvad-machineprofile-instance (i-0
     xxxxxxxx).vm"
4 <!--NeedCopy-->
```


Créer un catalogue avec la version du modèle de lancement

Vous pouvez créer un catalogue de machines MCS avec une version du modèle de lancement comme entrée de profil de machine. Vous pouvez également mettre à jour l'entrée d'un catalogue de profils de machines depuis une machine virtuelle vers une version de modèle de lancement et d'une version de modèle de lancement vers une machine virtuelle.

Sur la console AWS EC2, vous pouvez fournir les informations de configuration de l'instance d'un modèle de lancement ainsi que le numéro de version. Lorsque vous spécifiez la version du modèle de lancement en tant qu'entrée de profil de machine lors de la création ou de la mise à jour d'un catalogue de machines, les propriétés de cette version du modèle de lancement sont copiées sur les machines virtuelles VDA provisionnées.

Les propriétés suivantes peuvent être fournies à l'aide de l'entrée du profil de la machine ou explicitement sous forme de paramètres dans les commandes `New-ProvScheme` ou `Set-ProvScheme`. Si elles sont fournies dans les commandes `New-ProvScheme` ou `Set-ProvScheme`, elles ont la priorité sur les valeurs de profil machine de ces propriétés.

- Offre de services
- Réseaux
- Groupes de sécurité
- Type de location

> **Remarque :**
>
> Si l'offre de service n'est pas fournie dans le modèle de lancement du profil de la machine ou en tant que paramètre de la commande `New-ProvScheme`, vous obtenez une erreur appropriée.

Pour créer un catalogue en utilisant la version du modèle de lancement comme entrée de profil de machine :

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Obtenez la liste des versions d'un modèle de lancement. Par exemple :

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
    ls | Select FullPath
<!--NeedCopy-->
```

4. Créez un pool d'identités s'il n'a pas été créé. Par exemple :

```
New-AcctIdentityPool `
-IdentityPoolName "abc11" `
-NamingScheme "abc1-##" `
-NamingSchemeType Numeric `
-Domain "citrix-xxxxxx.local" `
```



```
6 -ZoneUid "xxxxxxxx" `
7 <!--NeedCopy-->
```

5. Créez un schéma de provisioning avec une version de modèle de lancement comme entrée de profil de machine. Par exemple :

```
1 New-ProvScheme `
2 -ProvisioningSchemeName "MPLT1" `
3 -HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
4 -IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
5 -MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
     persistent-vda-win2022 (ami-0axxxxxxxxxx).template" `
6 -CleanOnBoot `
7 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
     (lt-01xxxx).launchtemplate\lt-01xxxx (1).
     launchtemplateversion"
8 <!--NeedCopy-->
```

Vous pouvez également remplacer des paramètres tels que l'offre de services, les groupes de sécurité, la location et les réseaux. Par exemple :

```
1 New-ProvScheme `
2 -ProvisioningSchemeName "MPLT1" `
3 -HostingUnitUid " c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
4 -IdentityPoolUid " bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
5 -MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
     persistent-vda-win2022 (ami-0axxxxxxxxxx).template" `
6 -CleanOnBoot `
7 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
     (lt-01xxxx).launchtemplate\lt-01xxxx (1).launchtemplateversion"
     `
8 -ServiceOffering "XDHyp:\HostingUnits\xxxd-ue1a\T3 Large Instance.
     serviceoffering"
9 <!--NeedCopy-->
```

6. Enregistrez le schéma de provisioning en tant que catalogue de brokers. Par exemple :

```
1 New-BrokerCatalog -Name "MPLT1" `
2 -AllocationType Random `
3 -Description "Machine profile catalog" `
4 -ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
5 -ProvisioningType Mcs `
6 -SessionSupport MultiSession `
7 -PersistUserChanges Discard
8 <!--NeedCopy-->
```

7. Terminez la création du catalogue. Pour plus d'informations, accédez à cette page sur le SDK Citrix PowerShell.

Vous pouvez également mettre à jour l'entrée d'un catalogue de profils de machines depuis une machine virtuelle vers une version de modèle de lancement et d'une version de modèle de lancement

vers une machine virtuelle. Par exemple :

- Pour mettre à jour l'entrée d'un catalogue de profils de machines depuis une machine virtuelle vers une version de modèle de lancement, procédez comme suit :

```
1 Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
      `
2 -MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
      (lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx (1).
     launchtemplateversion"
3 <!--NeedCopy-->
```

- Pour mettre à jour l'entrée d'un catalogue de profils de machines depuis une version de modèle de lancement vers une machine virtuelle, procédez comme suit :

```
1 Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
      `
2 -MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
     availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
     xxxxxxxxx).vm"
3 <!--NeedCopy-->
```

Filtrer les instances de machines virtuelles

Une instance EC2 AWS que vous utilisez comme machine virtuelle de profil de machine doit être compatible pour créer le catalogue de machines et qu'il fonctionne correctement. Pour répertorier les instances de EC2 AWS pouvant être utilisées comme machine virtuelle d'entrée de profil de machine, vous pouvez utiliser la commande `Get-HypInventoryItem`. La commande permet de consulter et de filtrer l'inventaire des machines virtuelles disponibles sur une unité d'hébergement.

Pagination :

Get-HypInventoryItem prend en charge deux modes de pagination :

- Le mode de pagination utilise les paramètres `-MaxRecords` et `-Skip` pour renvoyer des ensembles d'éléments :
  - `-MaxRecords` : la valeur par défaut est **1**. Ce paramètre permet de contrôler le nombre d'éléments à renvoyer.
  - `-Skip` : la valeur par défaut est **0**. Ce paramètre permet de contrôler le nombre d'éléments à ignorer depuis le début absolu (ou la fin absolue) de la liste dans l'hyperviseur.
- Le mode de défilement utilise les paramètres `-MaxRecords`, `-ForwardDirection` et `-ContinuationToken` pour permettre le défilement des enregistrements :
  - `-ForwardDirection` : la valeur par défaut est **true**. Ce paramètre est utilisé conjointement avec `-MaxRecords` pour renvoyer l'ensemble suivant ou l'ensemble précédent d'enregistrements correspondants.

- `-ContinuationToken` : ce paramètre renvoie les éléments suivants (ou précédents si `ForwardDirection` est défini sur **false**), mais sans inclure l'élément indiqué dans `ContinuationToken`.

Exemples de pagination :

- Pour renvoyer un seul enregistrement du modèle de machine portant le nom figurant en haut de la liste, procédez comme suit. Le champ `AdditionalData` contient `TotalItemsCount` et `TotalFilteredItemsCount` :

```
1  Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
       -ResourceType template
2  <!--NeedCopy-->
```

- Pour renvoyer dix enregistrements du modèle de machine portant le nom figurant en bas de la liste, procédez comme suit :

```
1  Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
       -ResourceType template -MaxRecords 10 | select Name
2  <!--NeedCopy-->
```

- Pour renvoyer un tableau d'enregistrements se terminant par le nom figurant en haut de la liste, procédez comme suit :

```
1  Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
       -ResourceType template -ForwardDirection $False -MaxRecords 10
        | select Name
2  <!--NeedCopy-->
```

- Pour renvoyer un tableau d'enregistrements à partir du modèle de machine associé à la valeur donnée `ContinuationToken`, procédez comme suit :

```
1  Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
       -ResourceType template -ContinuationToken "ami-07xxxxxxxxx" -
       MaxRecords 10
2  <!--NeedCopy-->
```

Filtrage :

Les paramètres facultatifs supplémentaires suivants sont pris en charge pour le filtrage. Vous pouvez combiner ces paramètres avec les options de pagination.

- `-ContainsName "my_name"` : si la chaîne donnée correspond à une partie du nom d'une AMI, l'AMI est incluse dans le résultat `Get`. Par exemple :

```
1  Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
       -ResourceType template -MaxRecords 100 -ContainName ' apollo '
        | select Name
2  <!--NeedCopy-->
```


- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" } '` : si une AMI possède au moins l'une de ces balises, elle est incluse dans le résultat `Get` . Par exemple :

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -Tags '{
"opex owner": "Not tagged" }
' | select Name
<!--NeedCopy-->
```

> **Remarque :**
>
> Deux valeurs de balise sont prises en charge. La valeur de balise **Not Tagged** correspond aux éléments qui ne possèdent pas la balise spécifiée dans leur liste de balises. La valeur de balise **All values** correspond aux éléments qui possèdent la balise, quelle que soit la valeur de la balise. Dans le cas contraire, la correspondance ne se produit que si l'élément possède la balise et que si la valeur est égale à celle indiquée dans le filtre.

- `-Id "ami-0a2d913927e0352f3"` : si l'AMI correspond à l'ID donné, elle est incluse dans le résultat `Get`. Par exemple :

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -Id ami-xxxxxxxxxxxx
<!--NeedCopy-->
```

Filtrage avec le paramètre AdditionalData :

Le paramètre de filtre `AdditionalData` répertorie les modèles ou les machines virtuelles en fonction de leurs capacités, de leur offre de service ou de toute propriété figurant dans le paramètre AdditionalData. Par exemple :

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).
    AdditionalData
<!--NeedCopy-->
```

Vous pouvez également ajouter un paramètre `-Warn` pour spécifier les machines virtuelles incompatibles. Les machines virtuelles sont incluses dans un champ `AdditionalData` nommé **Warning**. Par exemple :

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami
    -015xxxxxxxxx" -Warn $true).AdditionalData
<!--NeedCopy-->
```


Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à AWS
- Créer des catalogues de machines

Créer un catalogue XenServer

June 27, 2024

La section Créer des catalogues de machines décrit les assistants qui permettent de créer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements de virtualisation XenServer.

> **Remarque :**
>
> Avant de créer un catalogue XenServer, vous devez terminer la création d'une connexion à XenServer. Consultez Connexion à XenServer.

Créez un catalogue de machines à l'aide d'une connexion XenServer

Les machines compatibles GPU requièrent une image principale dédiée. Ces machines virtuelles requièrent des pilotes de carte vidéo qui prennent en charge les processeurs graphiques. Configurez des machines prenant en charge les processeurs graphiques pour permettre à la machine virtuelle de fonctionner avec un logiciel qui utilise le processeur graphique pour les opérations.

1. Dans XenCenter, créez une machine virtuelle avec un VGA, des réseaux et un processeur virtuel standard.
2. Mettez à jour la configuration de la machine virtuelle pour activer l'utilisation du GPU (Passthough ou vGPU).
3. Installez un système d'exploitation pris en charge et activez RDP.
4. Installez Citrix machine virtuelle Tools et les pilotes NVIDIA.
5. Désactiver la console Administrateur VNC (Virtual Network Computing) pour optimiser les performances, puis redémarrez la machine virtuelle.
6. Vous êtes invité à utiliser le logiciel RDP (Connexion Bureau à distance). À l'aide de RDP, installez le VDA, puis redémarrez la machine virtuelle.
7. Si vous le souhaitez, vous pouvez créer un instantané de la machine virtuelle en tant que modèle de la ligne de base pour d'autres images principales GPU.
8. À l'aide de RDP, installez des applications spécifiques au client qui sont configurées dans XenCenter et utilisent les capacités de processeur graphique.

Limitations

- Si un déploiement Citrix Virtual Apps and Desktops avec ses machines virtuelles hébergées sur Citrix Hypervisor 8.2 utilise plusieurs SR GFS2 dans un seul catalogue MCS, les machines virtuelles du catalogue ne peuvent pas accéder aux VDI pendant le déploiement. L'erreur « VDI est actuellement en cours d'utilisation » est signalée.
- XenServer ne prend pas en charge les machines virtuelles à clone complet MCS avec SR GFS2.

Pour plus d'informations, consultez la section Contraintes.

Créer un catalogue de machines à l'aide d'un profil de machine

Lorsque vous créez un catalogue pour provisionner des machines à l'aide de MCS, vous pouvez utiliser un profil de machine pour capturer les propriétés matérielles d'une machine virtuelle et les appliquer aux machines virtuelles qui viennent d'être provisionnées dans le catalogue. Si le paramètre `MachineProfile` n'est pas utilisé, les propriétés matérielles sont capturées à partir de la machine virtuelle ou de l'instantané de l'image principale.

> **Remarque :**
>
> Actuellement, vous ne pouvez utiliser qu'une machine virtuelle comme entrée de profil de machine.

Vous pouvez configurer explicitement les paramètres suivants pour remplacer les valeurs des paramètres dans l'entrée du profil de machine :

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

Pour créer un catalogue avec un profil de machine :

1. Ouvrez la fenêtre PowerShell.
2. Exécutez `asnp citrix*`.
3. Créez un pool d'identités. Le pool d'identités est un conteneur pour les comptes Active Directory (AD) des machines virtuelles à créer. Par exemple :

```
1 New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -
      IdentityPoolName "ExampleIdentityPool" -NamingScheme "abc1-##"
      -NamingSchemeType "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
2 <!--NeedCopy-->
```

4. Créez les comptes d'ordinateurs AD requis dans Active Directory.


```
$password = "password123" | ConvertTo-SecureString -AsPlainText -
    Force
New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
    10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
    -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
<!--NeedCopy-->
```

5. Exécutez la commande `New-ProvScheme` pour créer un catalogue. Par exemple :

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
    -IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
     -CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
</CustomProperties>'
-MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
    vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
    " -Scope @() -SecurityGroup @()
-MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfile.vm"
<!--NeedCopy-->
```

6. Enregistrez le schéma de provisioning en tant que catalogue de brokers. Par exemple :

```
$ConfigZone = Get-ConfigZone | Where-Object {
  $_.Name -eq "xxxxxx"  }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
    Description "Machine profile catalog" -ProvisioningSchemeId
    fe7df345-244e-4xxxx-xxxxxxxxx -ProvisioningType Mcs -
    SessionSupport MultiSession -PersistUserChanges Discard -
    ZoneUid ($ConfigZone.Uid)
<!--NeedCopy-->
```

7. Ajoutez des machines virtuelles au catalogue.

Pour mettre à jour un catalogue avec un nouveau profil de machine :

1. Exécutez la commande `Set-ProvScheme`. Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -
    MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.
    snapshot"
<!--NeedCopy-->
```

   Pour plus d'informations sur la commande Set-ProvScheme, consultez Set-ProvScheme.

> **Remarque :**
>
> - Dans ce cas, la commande `Set-ProvScheme` ne modifie pas le profil de machine des machines virtuelles existantes dans le catalogue. Seules les machines virtuelles nouvellement créées ajoutées au catalogue ont le nouveau profil de machine.
> - Vous ne pouvez pas convertir un catalogue de machines basé sur un profil de machine en catalogue de machines non basé sur un profil de machine.

Autres ressources

- S'il s'agit du premier catalogue créé, Web Studio vous explique comment créer un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, consultez la section Installer et configurer.
- Pour gérer les catalogues, consultez Gérer les catalogues de machines et Gérer un catalogue XenServer

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à XenServer
- Créer des catalogues de machines

Créer un catalogue Google Cloud Platform

June 28, 2024

La section Créer des catalogues de machines décrit les assistants qui permettent de créer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements Google Cloud.

> **Remarque :**
>
> Avant de créer un catalogue Google Cloud Platform (GCP), vous devez terminer la création d'une connexion à GCP. Voir Connexion à des environnements Google Cloud.

Préparer une instance de machine virtuelle principale et un disque persistant

> **Conseil :**
>
> « Disque persistant » est le terme Google Cloud désignant un disque virtuel.

Pour préparer votre instance de machine virtuelle principale, créez et configurez une instance de machine virtuelle avec des propriétés correspondant à la configuration souhaitée pour les instances de VDA clonées dans votre catalogue de machines planifié. La configuration ne s'applique pas uniquement à la taille et au type d'instance. Elle inclut également des attributs d'instance tels que les métadonnées, les balises, les attributions de GPU, les balises réseau et les propriétés de compte de service.

Dans le cadre du processus de création d'images, MCS utilise votre instance de machine virtuelle principale pour créer le *modèle d'instance* Google Cloud. Le modèle d'instance est ensuite utilisé pour créer les instances de VDA clonées qui composent le catalogue de machines. Les instances clonées héritent des propriétés de l'instance de machine virtuelle principale (à l'exception des propriétés VPC, du sous-réseau et du disque persistant) à partir de laquelle le modèle d'instance a été créé.

Après avoir configuré les propriétés de l'instance de machine virtuelle principale en fonction de vos besoins spécifiques, démarrez l'instance, puis préparez le disque persistant pour l'instance.

Nous vous recommandons de créer manuellement un instantané du disque. Cela vous permet d'utiliser une convention d'appellation significative pour suivre les versions, vous offre plus d'options pour gérer les versions antérieures de votre image principale et vous permet de gagner du temps pour la création du catalogue de machines. Si vous ne créez pas votre propre instantané, MCS crée un instantané temporaire pour vous (qui est supprimé à la fin du processus de provisioning).

Créer un catalogue de machines

Vous pouvez créer un catalogue de machines de deux manières :

- Créer un catalogue de machines à l'aide de Web Studio
- Créer un catalogue de machines à l'aide de PowerShell

Créer un catalogue de machines à l'aide de Web Studio

> **Remarque :**
>
> Créez vos ressources avant de créer un catalogue de machines. Utilisez les conventions de dénomination établies par Google Cloud lors de la configuration des catalogues de machines. Pour plus d'informations, consultez Consignes de dénomination des buckets.

Suivez les instructions de la section Créer des catalogues de machines. Les informations suivantes sont uniques aux catalogues de Google Cloud.

1. Connectez-vous à Web Studio et sélectionnez **Catalogues de machines** dans le volet de gauche.
2. Sélectionnez **Créer un catalogue de machines** dans la barre d'actions.
3. Sur la page **Système d'exploitation**, sélectionnez **OS multi-session**, puis sélectionnez **Suivant**.
   - Citrix Virtual Apps and Desktops prend également en charge l'OS mono-session.
4. Sur la page **Gestion des machines**, sélectionnez **des machines dont l'alimentation est gérée** et les options **Citrix Machine Creation Services**, puis sélectionnez **Suivant**. S'il existe plusieurs ressources, sélectionnez-en une dans le menu.
5. Sur la page **Image**, effectuez ces étapes selon vos besoins, puis cliquez sur **Suivant**.
   a) Sélectionnez un instantané ou une machine virtuelle comme image principale. Si vous souhaitez utiliser la fonctionnalité de location unique, veillez à sélectionner une image dont la propriété de groupe de nœuds est correctement configurée. Consultez la section Activer la sélection de zone.
   b) Pour utiliser une machine virtuelle existante comme profil de machine, sélectionnez Utiliser un profil de machine, puis sélectionnez la machine virtuelle.

      > **Remarque :**
      >
      > Actuellement, les machines virtuelles de ce catalogue héritent de l'ID du jeu de chiffrement de disque, de la taille de la machine, du type de stockage et des paramètres de zone du profil de machine.

   c) Sélectionnez le niveau fonctionnel minimum pour le catalogue. Si vous souhaitez utiliser la fonctionnalité de location unique, veillez à sélectionner une image dont la propriété de groupe de nœuds est correctement configurée.
6. Sur la page **Types de stockage**, sélectionnez le type de stockage utilisé pour contenir le système d'exploitation de ce catalogue de machines. Chacune des options de stockage suivantes présente des caractéristiques de prix et de performances uniques. (Un disque d'identité est toujours créé à l'aide du disque persistant standard zonal.)
   - Disque persistant standard
   - Disque persistant équilibré
   - Disque persistant SSD

   Pour plus d'informations sur les options de stockage Google Cloud, consultez https://cloud.google.com/compute/docs/disks/.
7. Sur la page **Machines virtuelles**, spécifiez le nombre de machine virtuelle que vous souhaitez créer, affichez la spécification détaillée des machine virtuelle, puis sélectionnez **Suivant**. Si

vous utilisez des groupes de nœuds à locataire unique pour les catalogues de machines, assurez-vous de sélectionner **uniquement** les zones où des nœuds à locataire unique réservés sont disponibles. Consultez la section Activer la sélection de zone.

8. Sur la page **Comptes d'ordinateur**, sélectionnez un compte Active Directory, puis sélectionnez **Suivant**.

    - Si vous sélectionnez **Créer des nouveaux comptes Active Directory**, sélectionnez un domaine, puis entrez la séquence de caractères représentant le schéma de dénomination pour les comptes d'ordinateurs machine virtuelle provisionnés créés dans Active Directory. Le schéma d'attribution de nom de compte peut contenir entre 1 et 64 caractères et ne peut pas contenir d'espaces vides, ni de caractères non ASCII ou spéciaux.
    - Si vous sélectionnez **Utiliser des comptes Active Directory existants**, sélectionnez **Parcourir** pour accéder aux comptes d'ordinateur Active Directory existants pour les machines sélectionnées.

9. Sur la page **Informations d'identification du domaine**, sélectionnez **Entrer informations d'identification**, tapez le nom d'utilisateur et le mot de passe, sélectionnez **Enregistrer**, puis **Suivant**.

    - Les informations d'identification que vous tapez doivent disposer d'autorisations pour effectuer des opérations de compte Active Directory.

10. Sur la page **Résumé**, vérifiez les informations, spécifiez un nom pour le catalogue, puis sélectionnez **Terminer**.

    > **Remarque :**
    >
    > À partir de la version 2402, les noms de catalogues GCP doivent respecter les règles suivantes :
    >
    > - Commencer par une lettre minuscule.
    > - Inclure uniquement des lettres minuscules (a-z), des chiffres et des tirets.
    > - Se terminer par une lettre minuscule ou un chiffre.
    >
    > Lorsque vous tentez de renommer des catalogues GCP existants qui ne sont pas conformes à ces règles, des messages d'erreur apparaissent et vous indiquent de les renommer conformément aux règles mises à jour.

La création du catalogue de machines peut prendre du temps. Pour vérifier que les machines sont créées sur les groupes de nœuds cibles, accédez à la console Google Cloud.

Importer des machines Google Cloud créées manuellement

Vous pouvez *créer une connexion à Google Cloud*, puis *créer un catalogue contenant des machines Google Cloud*. Vous pouvez ensuite mettre sous tension les machines Google Cloud manuellement via Citrix Virtual Apps and Desktops. Avec cette fonctionnalité, vous pouvez :

- Importer des machines Google Cloud avec OS multi-session créées manuellement dans un catalogue de machines Citrix Virtual Apps and Desktops.
- Supprimer les machines Google Cloud avec OS multi-session créées manuellement d'un catalogue Citrix Virtual Apps and Desktops.
- Utiliser les fonctionnalités de gestion de l'alimentation Citrix Virtual Apps and Desktops existantes pour gérer l'alimentation des machines Google Cloud avec OS multi-session. Par exemple, définissez un programme de redémarrage pour ces machines.

Cette fonctionnalité ne nécessite aucune modification du workflow de provisioning Citrix Virtual Apps and Desktops existant, ni la suppression de toute fonctionnalité existante. Nous vous recommandons d'utiliser MCS pour provisionner des machines dans Web Studio au lieu d'importer des machines Google Cloud créées manuellement.

Cloud privé virtuel partagé

Les Virtual Private Cloud (VPC) partagés comprennent un projet hôte, à partir duquel les sous-réseaux partagés sont mis à disposition, et un ou plusieurs projets de service utilisant la ressource. Les VPC partagés sont des options souhaitables pour les installations de grande envergure, car ils fournissent un contrôle, une utilisation et une administration centralisés des ressources partagées de Google Cloud d'entreprise. Pour plus d'informations, consultez le site de la documentation Google.

Grâce à cette fonctionnalité, Machine Creation Services (MCS) prend en charge le provisioning et la gestion des catalogues de machines déployés sur des VPC partagés. Cette prise en charge, qui est fonctionnellement équivalente à celle actuellement fournie dans les VPC locaux, diffère par deux aspects :

1. Vous devez accorder des autorisations supplémentaires au compte de service utilisé pour créer la connexion hôte. Ce processus permet à MCS d'accéder aux ressources VPC partagées et de les utiliser.
2. Vous devez créer deux règles de pare-feu, une pour l'entrée et la sortie. Ces règles de pare-feu sont utilisées pendant le processus de mastering des images.

Nouvelles autorisations requises

Un compte de service Google Cloud avec des autorisations spécifiques est requis lors de la création de la connexion hôte. Ces autorisations supplémentaires doivent être accordées à tous les comptes

de service utilisés pour créer des connexions d'hôte basées sur un VPC partagé.

> **Conseil :**
>
> Ces autorisations supplémentaires ne sont pas nouvelles pour Citrix Virtual Apps and Desktops. Elles sont utilisées pour faciliter la mise en œuvre de VPC locaux. Avec les VPC partagés, ces autorisations supplémentaires permettent l'accès à d'autres ressources VPC partagées.

Un maximum de quatre autorisations supplémentaires doivent être accordées au compte de service associé à la connexion hôte pour prendre en charge un VPC partagé :

1. **compute.firewalls.list** - Cette autorisation est obligatoire. Elle permet à MCS de récupérer la liste des règles de pare-feu présentes sur le VPC partagé.
2. **compute.networks.list** - Cette autorisation est obligatoire. Elle permet à MCS d'identifier les réseaux VPC partagés disponibles pour le compte de service.
3. **compute.subnetworks.list** - Cette autorisation est facultative en fonction de la façon dont vous utilisez les VPC. Elle permet à MCS d'identifier les sous-réseaux dans les VPC partagés visibles. Cette autorisation est déjà requise lors de l'utilisation de VPC locaux, mais doit également être attribuée dans le projet Hôte VPC partagé.
4. **compute.subnetworks.use** - Cette autorisation est facultative en fonction de la façon dont vous utilisez les VPC. Elle est nécessaire pour utiliser des ressources de sous-réseau dans les catalogues de machines provisionnées. Cette autorisation est déjà requise pour utiliser des VPC locaux, mais doit également être attribuée dans le projet hôte VPC partagé.

Lorsque vous utilisez ces autorisations, gardez à l'esprit qu'il existe différentes approches basées sur le type d'autorisation utilisé pour créer le catalogue de machines :

- Autorisation au niveau du projet :
  - Permet l'accès à tous les VPC partagés au sein du projet hôte.
  - Nécessite que les autorisations #3 et #4 soient affectées au compte de service.
- Autorisation au niveau du sous-réseau :
  - Permet l'accès à des sous-réseaux spécifiques dans le VPC partagé.
  - Les autorisations #3 et #4 sont intrinsèques à l'affectation au niveau du sous-réseau et n'ont donc pas besoin d'être affectées directement au compte de service.

Sélectionnez l'approche qui correspond aux besoins et aux normes de sécurité de votre organisation.

> **Conseil :**
>
> Pour plus d'informations sur les différences entre les autorisations au niveau du projet et au niveau du sous-réseau, consultez la documentation Google Cloud.

Règles de pare-feu

Lors de la préparation d'un catalogue de machines, une image de machine est préparée pour servir de disque système d'image principale pour le catalogue. Lors de ce processus, le disque est temporairement attaché à une machine virtuelle. Cette machine virtuelle doit s'exécuter dans un environnement isolé qui empêche tout le trafic réseau entrant et sortant. Pour cela, une paire de règles de pare-feu deny-all est utilisée : une pour le trafic d'entrée et une pour le trafic de sortie. Lors de l'utilisation de VCP locaux Google Cloud, MCS crée ce pare-feu sur le réseau local et l'applique à la machine pour le mastering. Une fois le mastering terminé, la règle de pare-feu est supprimée de l'image.

Nous vous recommandons de limiter au minimum le nombre de nouvelles autorisations requises pour utiliser des VPC partagés. Les VPC partagés sont des ressources d'entreprise de plus haut niveau et ont généralement des protocoles de sécurité plus stricts. Pour cette raison, créez une paire de règles de pare-feu dans le projet hôte sur les ressources VPC partagées, une pour l'entrée et une pour la sortie. Attribuez-leur la priorité la plus élevée. Appliquez une nouvelle balise cible à chacune de ces règles, à l'aide de la valeur suivante :

```
citrix-provisioning-quarantine-firewall
```

Lorsque MCS crée ou met à jour un catalogue de machines, il recherche les règles de pare-feu contenant cette balise cible. Il examine ensuite les règles d'exactitude et les applique à la machine utilisée pour préparer l'image principale pour le catalogue. Si les règles de pare-feu sont introuvables ou si les règles sont trouvées mais que les règles ou leurs priorités sont incorrectes, un message similaire au suivant s'affiche :

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
 'deny all'firewall rules with the network tag 'citrix-provisioning-
quarantine-firewall'and proper priority.""Refer to Citrix Documentation
 for details."
```

Configuration du VPC partagé

Avant d'ajouter le VPC partagé en tant que connexion hôte dans Web Studio, procédez comme suit pour ajouter des comptes de service à partir du projet dans lequel vous avez l'intention de provisionner :

1. Créez un rôle IAM.
2. Ajoutez le compte de service utilisé pour créer une connexion hôte CVAD au rôle IAM du projet hôte VPC partagé.
3. Ajoutez le compte de service Cloud Build du projet dans lequel vous avez l'intention de provisionner au rôle IAM du projet hôte VPC partagé.
4. Créez des règles de pare-feu.

Créer un rôle IAM Déterminez le niveau d'accès du rôle : *accès au niveau du projet* ou modèle plus restreint avec *accès au niveau du sous-réseau*.

Accès au niveau du projet pour le rôle IAM. Pour le rôle IAM au niveau du projet, vous devez inclure les autorisations suivantes :

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Pour créer un rôle IAM au niveau du projet :

1. Dans la console Google Cloud, accédez à **IAM et administration > Rôles**.
2. Sur la page **Rôles**, sélectionnez **CRÉER UN RÔLE**.
3. Sur la page **Créer un rôle**, spécifiez le nom du rôle. Sélectionnez **AJOUTER DES AUTORISATIONS**.
    a) Sur la page **Ajouter des autorisations**, ajoutez des autorisations au rôle, individuellement. Pour ajouter une autorisation, tapez le nom de l'autorisation dans le champ **Filtrer le tableau**. Sélectionnez l'autorisation, puis sélectionnez **AJOUTER**.
    b) Sélectionnez **Créer**.

Rôle IAM au niveau du sous-réseau. Ce rôle omet l'ajout des autorisations `compute.subnetworks.list` et `compute.subnetworks.use` après avoir sélectionné **CRÉER UN ROLE**. Pour ce niveau d'accès IAM, les autorisations `compute.firewalls.list` et `compute.networks.list` doivent être appliquées au nouveau rôle.

Pour créer un rôle IAM au niveau du sous-réseau :

1. Dans la console Google Cloud, accédez à **Réseau VPC** > **VPC partagé**. La page **VPC partagé** apparaît et affiche les sous-réseaux des réseaux VPC partagés contenus dans le projet hôte.
2. Sur la page **VPC partagé**, sélectionnez le sous-réseau auquel vous souhaitez accéder.
3. Dans l'angle supérieur droit, sélectionnez **AJOUTER UN MEMBRE** pour ajouter un compte de service.
4. Sur la page **Add members**, procédez comme suit :
    a) Dans le champ **New members**, tapez le nom de votre compte de service, puis sélectionnez votre compte de service dans le menu.
    b) Sélectionnez le champ **Sélectionner un rôle**, puis **Utilisateur de réseau Compute**.
    c) Sélectionnez **Enregistrer**.
5. Dans la console Google Cloud, accédez à **IAM et administration** > **Rôles**.
6. Sur la page **Rôles**, sélectionnez **CRÉER UN RÔLE**.

7. Sur la page **Créer un rôle**, spécifiez le nom du rôle. Sélectionnez **AJOUTER DES AUTORISATIONS**.

    a) Sur la page **Ajouter des autorisations**, ajoutez des autorisations au rôle, individuellement. Pour ajouter une autorisation, tapez le nom de l'autorisation dans le champ **Filtrer le tableau**. Sélectionnez l'autorisation, puis sélectionnez **AJOUTER**.
    b) Sélectionnez **Créer**.

Ajouter un compte de service au rôle IAM du projet hôte Après avoir créé un rôle IAM, effectuez les étapes suivantes pour ajouter un compte de service pour le projet hôte :

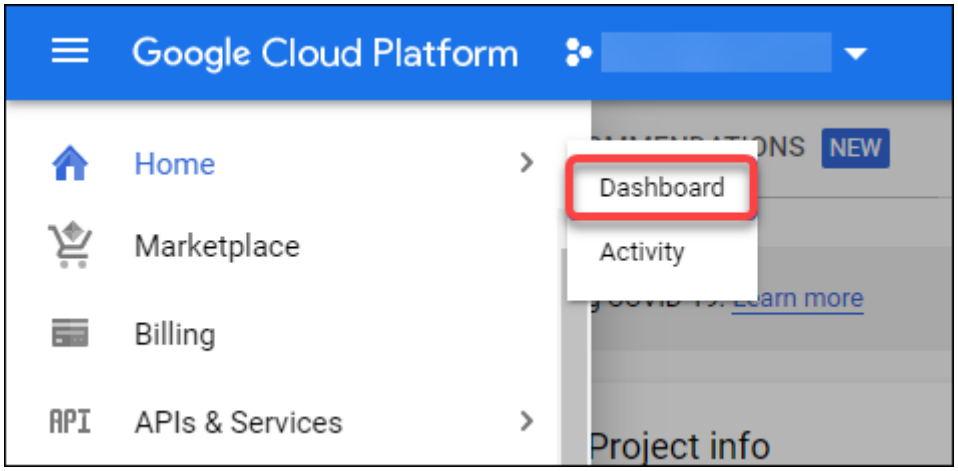
1. Dans la console Google Cloud, accédez au projet hôte, puis à **IAM et admin > IAM**.
2. Sur la page **IAM**, sélectionnez **AJOUTER** pour ajouter un compte de service.
3. Sur la page **Ajouter des membres** :

    a) Dans le champ **New members**, tapez le nom de votre compte de service, puis sélectionnez votre compte de service dans le menu.
    b) Sélectionnez un rôle, tapez le rôle IAM que vous avez créé, puis cliquez sur le rôle dans le menu.
    c) Sélectionnez **Enregistrer**.

Le compte de service est maintenant configuré pour le projet hôte.

Ajouter le compte de service Cloud Build au VPC partagé Chaque abonnement Google Cloud comporte un compte de service nommé d'après le numéro d'ID du projet, suivi de `cloudbuild.gserviceaccount`. Par exemple : `705794712345@cloudbuild.gserviceaccount`.

Vous pouvez déterminer le numéro d'ID de votre projet en sélectionnant **Accueil** et **Tableau de bord** dans la console Google Cloud :



Recherchez le **numéro de projet** sous la zone **Informations sur le projet** de l'écran.

Procédez comme suit pour ajouter le compte de service Cloud Build au VPC partagé :

1. Dans la console Google Cloud, accédez au projet hôte, puis à **IAM et admin** > **IAM**.
2. Sur la page **Autorisations**, sélectionnez **AJOUTER** pour ajouter un compte.
3. Sur la page **Add members**, procédez comme suit :

    a) Dans le champ **Nouveaux membres**, tapez le nom du compte de service Cloud Build, puis sélectionnez votre compte de service dans le menu.
    b) Sélectionnez le champ **Sélectionner un rôle**, tapez `Computer Network User`, puis sélectionnez le rôle dans le menu.
    c) Sélectionnez **Enregistrer**.

Créer des règles de pare-feu Dans le cadre du processus de création d'image principale, MCS copie l'image machine sélectionnée et l'utilise pour préparer le disque système d'image principale pour le catalogue. Pendant la création d'image principale, MCS attache le disque à une machine virtuelle temporaire, qui exécute ensuite des scripts de préparation. Cette machine virtuelle doit s'exécuter dans un environnement isolé qui interdit tout trafic réseau entrant et sortant. Pour créer un environnement isolé, MCS nécessite deux règles de pare-feu *deny all* (une règle d'entrée et une règle de sortie). Par conséquent, créez deux règles de pare-feu dans le *projet hôte* comme suit :

1. Dans la console Google Cloud, accédez au projet hôte, puis à **Réseau VPC > Pare-feu**.
2. Sur la page **Pare-feu**, sélectionnez **Créer une règle de pare-feu**.
3. Sur la page **Créer une règle de pare-feu**, procédez comme suit :

    - **Nom**. Tapez un nom pour la règle.
    - **Réseau**. Sélectionnez le réseau VPC partagé auquel la règle de pare-feu d'entrée s'applique.
    - **Priorité**. Plus la valeur est petite, plus la priorité de la règle est élevée. Nous recommandons une valeur peu élevée (par exemple, 10).
    - **Sens du trafic**. Sélectionnez **Entrée**.
    - **Action en cas de correspondance**. Sélectionnez **Refuser**.
    - **Cibles**. Utilisez **Tags cibles spécifiés** par défaut.
    - **Tags cibles**. Tapez `citrix-provisioning-quarantine-firewall`.
    - **Filtre source**. Utilisez **Plages d'adresses IP** par défaut.
    - **Plages d'adresses IP sources**. Tapez une plage qui correspond à tout le trafic. Tapez `0.0.0.0/0`.
    - **Protocoles et ports**. Sélectionnez **Tout refuser**.

4. Sélectionnez **CRÉER** pour créer la règle.
5. Répétez les étapes 1 à 4 pour créer une autre règle. Pour **Sens du trafic**, sélectionnez **Sortie**.

Ajouter une connexion Ajoutez une connexion aux environnements Google Cloud. Consultez la section Ajouter une connexion.

Activer la sélection de zone

Citrix Virtual Apps and Desktops prend en charge la sélection de zone. Avec la sélection de zone, vous spécifiez les zones dans lesquelles vous souhaitez créer des machines virtuelles. Avec la sélection de zone, les administrateurs peuvent placer des nœuds locataires uniques sur les zones de leur choix. Pour configurer la location unique, vous devez procéder comme suit sur Google Cloud :

- Réserver un nœud à locataire unique Google Cloud
- Créer l'image principale du VDA

Réservation d'un nœud à locataire unique Google Cloud

Pour réserver un nœud à locataire unique, reportez-vous à la documentation Google Cloud.

> **Important :**
>
> Un modèle de nœud est utilisé pour indiquer les caractéristiques de performance du système réservé dans le groupe de nœuds. Ces caractéristiques incluent le nombre de vGPU, la quantité de mémoire allouée au nœud et le type de machine utilisé pour les machines créées sur le nœud. Pour plus d'informations, consultez la documentation Google Cloud.

Création de l'image principale du VDA

Pour déployer des machines sur le nœud à locataire unique, vous devez prendre des mesures supplémentaires lors de la création d'une image de machine virtuelle principale. Les instances de machine sur Google Cloud ont une propriété appelée *libellés d'affinité de nœuds*. Les instances utilisées comme images principales pour les catalogues déployés sur le nœud à locataire unique nécessitent un *libellé d'affinité de nœuds* correspondant au nom du **groupe de nœuds cible**. Pour ce faire, gardez à l'esprit ce qui suit :

- Pour une nouvelle instance, définissez le libellé dans la console Google Cloud lors de la création d'une instance. Pour plus d'informations, consultez la section Définir un libellé d'affinité de nœuds lors de la création d'une instance.
- Pour une instance existante, définissez le libellé à l'aide de la ligne de commande **gcloud**. Pour plus de détails, voir Définir un libellé d'affinité de nœuds pour une instance existante.

> **Remarque :**
>
> Si vous avez l'intention d'utiliser la location unique avec un VPC partagé, reportez-vous à la section Cloud privé virtuel partagé.

Définir un libellé d'affinité de nœuds lors de la création d'une instance Pour définir le libellé d'affinité de nœuds :

1. Dans la console Google Cloud, accédez à **Compute Engine > Instances de machine virtuelle**.
2. Sur la page **Instances de machine virtuelle**, sélectionnez **Créer une instance**.
3. Sur la page **Création d'instance**, tapez ou configurez les informations requises, puis sélectionnez **Gestion, sécurité, disques, mise en réseau et location unique** pour ouvrir le panneau des paramètres.
4. Sous l'onglet **Location unique**, sélectionnez **Parcourir** pour afficher les groupes de nœuds disponibles dans le projet en cours. La page **Nœud à locataire unique** s'affiche avec une liste des groupes de nœuds disponibles.
5. Sur la page **Nœud à locataire unique**, sélectionnez le groupe de nœuds applicable dans la liste, puis sélectionnez **Sélectionner** pour revenir à l'onglet **Locataire unique**. Le champ de libellés d'affinité de nœuds renseigne les informations que vous avez sélectionnées. Ce paramètre garantit que les catalogues de machines créés à partir de l'instance seront déployés dans le groupe de nœuds sélectionné.
6. Sélectionnez **Créer** pour créer l'instance.

Définir un libellé d'affinité de nœuds pour une instance existante Pour définir le libellé d'affinité de nœuds :

1. Dans la fenêtre du terminal Google Cloud Shell, utilisez la commande *gcloud compute instances* pour définir un libellé d'affinité de nœuds. Vous devez inclure les informations suivantes dans la commande **gcloud** :

   - **Nom de la machine virtuelle**. Par exemple, utilisez une machine virtuelle existante nommée `s*2019-vda-base`.*
   - **Nom du groupe de nœuds**. Utilisez le nom du groupe de nœuds que vous avez créé précédemment. Par exemple, `mh-sole-tenant-node-group-1`.
   - **Zone dans laquelle réside l'instance**. Par exemple, la machine virtuelle réside dans `*us-east-1b* zone`.

   Par exemple, tapez la commande suivante dans la fenêtre du terminal :

- `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

Pour plus d'informations sur la commande *gcloud compute instances*, consultez la documentation Google Developer Tools sur https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling.

2. Accédez à la page **Détails de l'instance de machine virtuelle** et vérifiez que le champ **Affinités des nœuds** est rempli avec le libellé.

Créer un catalogue de machines Après avoir défini le libellé d'affinité des nœuds, configurez le catalogue de machines.

Clés de chiffrement gérées par le client (CMEK)

Vous pouvez utiliser des clés de chiffrement gérées par le client (CMEK) pour les catalogues MCS. Lorsque vous utilisez cette fonctionnalité, vous attribuez le rôle `CryptoKey Encrypter/Decrypter` de Google Cloud Key Management Service à l'agent de service Compute Engine. Le compte Citrix Virtual Apps and Desktops doit disposer des autorisations correctes dans le projet où la clé est stockée. Pour plus d'informations, reportez-vous à la section Contribuer à la protection des ressources en utilisant des clés Cloud KMS.

Votre agent de service Compute Engine se présente sous la forme suivante : `service-<Project_Number>@compute-system.iam.gserviceaccount.com`. Ce formulaire est différent du compte de service Compute Engine par défaut.

> **Remarque :**
>
> Ce compte de service Compute Engine peut ne pas apparaître dans l'écran **Autorisations IAM** de Google Console. Dans ce cas, utilisez la commande `gcloud` décrite dans la section Contribuer à la protection des ressources en utilisant des clés Cloud KMS.

Attribuer des autorisations au compte Citrix Virtual Apps and Desktops

Les autorisations Google Cloud KMS peuvent être configurées de différentes manières. Vous pouvez fournir des autorisations KMS *au niveau du projet* ou des autorisations KMS *au niveau des ressources*. Pour plus d'informations, consultez la section Autorisations et rôles.

Autorisations au niveau du projet L'une des options consiste à fournir au compte Citrix Virtual Apps and Desktops des autorisations au niveau du projet pour parcourir les ressources Cloud KMS. Pour ce faire, créez un rôle personnalisé et ajoutez les autorisations suivantes :

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Attribuez ce rôle personnalisé à votre compte Citrix Virtual Apps and Desktops. Cela vous permet de parcourir les clés régionales du projet concerné dans l'inventaire.

Permissions au niveau des ressources Pour l'autre option, les autorisations au niveau des ressources, dans la console Google Cloud, accédez à l'option `cryptoKey` que vous utilisez pour le provisioning MCS. Ajoutez le compte Citrix Virtual Apps and Desktops à un trousseau de clés ou à une clé que vous utilisez pour le provisioning du catalogue.

> **Conseil :**
>
> Avec cette option, vous ne pouvez pas parcourir les clés régionales de votre projet dans l'inventaire car le compte Citrix Virtual Apps and Desktops ne dispose pas d'autorisations de liste au niveau du projet sur les ressources Cloud KMS. Toutefois, vous pouvez toujours provisionner un catalogue à l'aide de CMEK en spécifiant le bon `cryptoKeyId` dans les propriétés `ProvScheme` personnalisées, décrites ci-dessous.

Provisioning avec CMEK à l'aide de propriétés personnalisées

Lorsque vous créez votre schéma de provisioning via PowerShell, spécifiez une propriété `CryptoKeyId` dans `ProvScheme CustomProperties`. Par exemple :

```
1 '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2     <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
        yourCryptoKeyId>" />
3 </CustomProperties>'
4 <!--NeedCopy-->
```

L'élément `cryptoKeyId` doit être au format suivant :

`projectId:location:keyRingName:cryptoKeyName`

Par exemple, si vous souhaitez utiliser la clé `my-example-key` du trousseau de clés `my-example-key-ring` dans la région `us-east1` et le projet avec ID `my-example-project-1`, vos paramètres `ProvScheme` personnalisés ressembleraient à :

```
1 '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
```



```
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
       example-project-1:us-east1:my-example-key-ring:my-example-key"
       />
</CustomProperties>'
<!--NeedCopy-->
```

Tous les disques et images provisionnés avec MCS associés à ce schéma de provisioning utilisent cette clé de chiffrement gérée par le client.

> **Conseil :**
>
> Si vous utilisez des clés globales, l'emplacement des propriétés du client doit indiquer `global` et non le nom de la **région**, qui dans l'exemple ci-dessus est **us-east1**. Par exemple : `<Property xsi:type="StringProperty"Name="CryptoKeyId"Value="my-example-project-1:global:my-example-key-ring:my-example-key"/>`.

Rotation des clés gérées par le client

Google Cloud ne prend pas en charge la rotation des clés sur des images ou des disques persistants existants. Une fois qu'une machine est provisionnée, elle est liée à la version clé utilisée au moment de sa création. Toutefois, une nouvelle version de la clé peut être créée et cette nouvelle clé est utilisée pour les machines ou les ressources nouvellement provisionnées créées lorsqu'un catalogue est mis à jour avec une nouvelle image principale.

Remarques importantes concernant les trousseaux de clés Les trousseaux de clés ne peuvent pas être renommés ou supprimés. En outre, vous risquez d'entraîner des frais imprévus lors de leur configuration. Lorsque vous supprimez ou retirez un trousseau de clés, Google Cloud affiche un message d'erreur :

```
Sorry, you can't delete or rename keys or key rings. We were concerned
   about the security implications of allowing multiple keys or key
   versions over time to have the same resource name, so we decided to
   make names immutable. (And you can't delete them, because we wouldn'
   t be able to do a true deletion--there would still have to be a
   tombstone tracking that this name had been used and couldn't be
   reused).
We're aware that this can make things untidy, but we have no immediate
   plans to change this.
If you want to avoid getting billed for a key or otherwise make it
   unavailable, you can do so by deleting all the key versions; neither
    keys nor key rings are billed for, just the active key versions
   within the keys.
<!--NeedCopy-->
```


> **Conseil :**
>
> Pour plus d'informations, consultez la section Modification ou suppression d'un trousseau de clés de la console.

Compatibilité de l'accès uniforme au niveau du bucket

Citrix Virtual Apps and Desktops est compatible avec la stratégie de contrôle Accès uniforme au niveau du bucket sur Google Cloud. Cette fonctionnalité augmente l'utilisation de la stratégie IAM qui accorde des autorisations à un compte de service pour permettre la manipulation des ressources, y compris des buckets de stockage. Avec le contrôle d'accès uniforme au niveau du bucket, Citrix Virtual Apps and Desktops vous permet d'utiliser une liste de contrôle d'accès (ACL) pour contrôler l'accès aux buckets de stockage ou aux objets qui y sont stockés. Consultez Accès uniforme au niveau du bucket pour obtenir des informations générales sur l'accès uniforme au niveau du bucket Google Cloud. Pour plus d'informations sur la configuration, voir Exiger un accès uniforme au niveau du bucket.

Créer un catalogue de machines à l'aide de PowerShell

Cette section explique comment créer des catalogues à l'aide de PowerShell :

- Créer un catalogue avec disque de cache en écriture persistant
- Améliorer les performances de démarrage avec MCSIO
- Créer un catalogue de machines à l'aide d'un profil de machine
- Créer un catalogue de machines avec un profil de machine en tant que modèle d'instance
- Utiliser PowerShell pour créer un catalogue avec machine virtuelle protégée
- Créer des machines virtuelles Windows 11 sur le nœud à locataire unique

Créer un catalogue avec disque de cache en écriture persistant

Pour configurer un catalogue avec un disque de cache en écriture différée persistant, utilisez le paramètre PowerShell `New-ProvScheme CustomProperties`.

> **Conseil :**
>
> Utilisez le paramètre PowerShell ici uniquement pour les connexions d'hébergement basées sur le cloud. Si vous souhaitez provisionner des machines à l'aide d'un disque de cache en écriture différée persistant pour une solution locale (par exemple, XenServer), PowerShell n'est pas nécessaire, car le disque persiste automatiquement.

Ce paramètre prend en charge une propriété supplémentaire, `PersistWBC`, utilisée pour déterminer la façon dont le disque de cache en réécriture persiste pour les machines provisionnées avec MCS. La propriété `PersistWBC` n'est utilisée que lorsque le paramètre `UseWriteBackCache` est spécifié et lorsque le paramètre `WriteBackCacheDiskSize` est défini pour indiquer qu'un disque est créé.

> **Remarque :**
>
> Ce comportement s'applique à Azure et GCP où le disque de cache en écriture MCSIO par défaut est supprimé et recréé lors du cycle d'alimentation. Vous pouvez choisir de persister le disque pour éviter la suppression et la recréation du disque de cache en réécriture MCSIO.

Lorsque la propriété `PersistWBC` est définie sur **`true`**, le disque de cache en réécriture n'est pas supprimé lorsque l'administrateur Citrix Virtual Apps and Desktops arrête la machine à l'aide de l'interface de gestion.

Lorsque la propriété `PersistWBC` est définie sur **`false`**, le disque de cache en réécriture est supprimé lorsque l'administrateur Citrix Virtual Apps and Desktops arrête la machine à l'aide de l'interface de gestion.

> **Remarque :**
>
> Si la propriété `PersistWBC` est omise, la propriété est **`false`** par défaut et le cache de réécriture est supprimé lors de l'arrêt de la machine à l'aide de l'interface de gestion.

Par exemple, utilisation du paramètre CustomProperties pour définir `PersistWBC` sur **`true`** :

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
     benvaldev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
6 </CustomProperties>
7 <!--NeedCopy-->
```

> **Remarque :**
>
> La propriété `PersistWBC` ne peut être définie qu'à l'aide de l'applet de commande PowerShell `New-ProvScheme`. La tentative de modification de `CustomProperties` pour un schéma de provisioning après la création n'a aucun impact sur le catalogue de machines et la persistance du disque de cache en réécriture lors de l'arrêt d'une machine.

Par exemple, définissez `New-ProvScheme` pour utiliser le cache en réécriture tout en définissant la propriété `PersistWBC` sur **`true`** :

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

Améliorer les performances de démarrage avec MCSIO

Vous pouvez améliorer les performances de démarrage des disques gérés par Azure et GCP lorsque MCSIO est activé. Utilisez la propriété personnalisée `PersistOSDisk` PowerShell dans la commande `New-ProvScheme` pour configurer cette fonctionnalité. Les options associées à `New-ProvScheme` incluent :

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="Resource <!--NeedCopy-->
``````<!--NeedCopy-->
<!--NeedCopy-->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
```

```
    />
</CustomProperties>
<!--NeedCopy-->
```

Pour activer cette fonctionnalité, définissez la propriété personnalisée `PersistOSDisk` sur **`true`**. Par exemple :

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

### Créer un catalogue de machines à l'aide d'un profil de machine

Lorsque vous créez un catalogue pour provisionner des machines à l'aide de Machine Creation Services (MCS), vous pouvez utiliser un profil de machine pour capturer les propriétés matérielles d'une machine virtuelle et les appliquer aux machines virtuelles nouvellement provisionnées dans le catalogue. Lorsque le paramètre `MachineProfile` n'est pas utilisé, les propriétés matérielles sont capturées à partir de la machine virtuelle ou de l'instantané de l'image principale.
Certaines propriétés que vous définissez explicitement, par exemple `StorageType`, `CatalogZones` et `CryptoKeyIs`, ne sont pas prises en compte dans le profil de machine.

- Pour créer un catalogue avec un profil de machine, utilisez la commande `New-ProvScheme`. Par exemple, `New-ProvScheme –MachineProfile "path to VM"`. Si vous ne spécifiez pas le paramètre `MachineProfile`, les propriétés matérielles sont capturées à partir de

la machine virtuelle de l'image principale.

- Pour mettre à jour un catalogue avec un nouveau profil de machine, utilisez la commande `Set-ProvScheme`. Par exemple, `Set-ProvScheme –MachineProfile "path to new VM"`. Cette commande ne modifie pas le profil de machine des machines virtuelles existantes dans le catalogue. Seules les machines virtuelles nouvellement créées ajoutées au catalogue ont le nouveau profil de machine.
- Vous pouvez également mettre à jour l'image principale, mais lorsque vous mettez à jour l'image principale, les propriétés matérielles ne sont pas mises à jour. Si vous souhaitez mettre à jour les propriétés matérielles, vous devez mettre à jour le profil de machine à l'aide de la commande `Set-ProvScheme`. Ces modifications ne s'appliqueront qu'aux nouvelles machines du catalogue. Pour mettre à jour les propriétés matérielles d'une machine existante, vous pouvez utiliser la commande `Set-ProvVMUpdateTimeWindow` avec les paramètres `-StartsNow` et `-DurationInMinutes -1`.

  > **Remarque :**
  >
  > - `StartsNow` indique que l'heure de démarrage planifiée est l'heure actuelle.
  > - `DurationInMinutes` avec un nombre négatif (par exemple, —1) indique qu'il n'y a pas de limite supérieure dans le créneau planifié.

### Créer un catalogue de machines avec un profil de machine en tant que modèle d'instance

Vous pouvez sélectionner un modèle d'instance GCP comme entrée pour le profil de la machine. Les modèles d'instance sont des ressources légères dans GCP et sont donc très rentables.

#### Créer un nouveau catalogue de machines avec un profil de machine en tant que modèle d'instance

1. Ouvrez une fenêtre PowerShell.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Recherchez un modèle d'instance dans votre projet GCP à l'aide de la commande suivante :

   ```
   cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
   <!--NeedCopy-->
   ```

4. Créez un nouveau catalogue de machines avec un profil de machine en tant que modèle d'instance à l'aide de la commande NewProvScheme :

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -
    HostingUnitName <HostingUnitName> -IdentityPoolName <identity
    pool name> -MasterImageVM
XDHyp:\HostingUnits<HostingUnitName> \Base.vm\Base.snapshot -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder\mytemplate.template
<!--NeedCopy-->
```

Pour plus d'informations sur la commande New-ProvScheme, consultez https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/.

5. Terminez la création du catalogue de machines à l'aide des commandes PowerShell. Pour plus d'informations sur la création d'un catalogue à l'aide du SDK Remote PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

#### Modifier le profil de machine d'un catalogue de machines existant afin qu'il devienne un modèle d'instance

Les étapes détaillées pour modifier le profil de machine d'un catalogue de machines existant afin qu'il devienne un modèle d'instance sont les suivantes :

1. Ouvrez une fenêtre PowerShell.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Exécutez la commande suivante :

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder<TemplateName>.template
<!--NeedCopy-->
```

Pour plus d'informations sur la commande Set-ProvScheme, consultez https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

### Utiliser PowerShell pour créer un catalogue avec machine virtuelle protégée

Vous pouvez créer un catalogue de machines MCS avec des propriétés de machine virtuelle protégée. Une machine virtuelle protégée est renforcée par un ensemble de contrôles de sécurité qui fournissent une intégrité vérifiable de vos instances Compute Engine, en utilisant des fonctionnalités avancées de sécurité de plate-forme telles que le démarrage sécurisé, un module de plate-forme virtuelle de confiance, un microprogramme UEFI et la surveillance de l'intégrité.

MCS prend en charge la création du catalogue à l'aide du workflow de profil de machine. Si vous utilisez un workflow de profil de machine, vous devez activer les propriétés de machine virtuelle pro-

tégée d'une instance de machine virtuelle. Vous pouvez ensuite utiliser cette instance de machine virtuelle comme entrée de profil de machine.

Pour créer un catalogue de machines MCS avec machine virtuelle protégée à l'aide du workflow de profil de machine :

1. Activez les options de machine virtuelle protégée d'une instance de machine virtuelle dans la console Google Cloud. Consultez Guide de démarrage rapide : activer les options de machine virtuelle protégée.
2. Créez un catalogue de machines MCS avec un workflow de profil de machine à l'aide de l'instance de machine virtuelle.
   a) Ouvrez une fenêtre PowerShell.
   b) Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
   c) Créez un pool d'identités s'il n'a pas déjà été créé.
   d) Exécutez la commande `New-ProvScheme`. Par exemple :

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>
-HostingUnitName gcp-hostint-unit
-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
   vda.vm
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
   machine.vm
<!--NeedCopy-->
```

3. Terminez la création du catalogue de machines.

Pour mettre à jour le catalogue de machines avec un nouveau profil de machine :

1. Exécutez la commande `Set-ProvScheme`. Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>
-MasterImageVM XDHyp:\HostingUnits<hostin-unit>\catalog-vda.vm
-MachineProfile "DHyp:\HostingUnits<hostin-unit>\catalog-machine.
   vm
<!--NeedCopy-->
```

Pour appliquer la modification effectuée dans `Set-ProvScheme` aux machines virtuelles existantes, exécutez la commande `Set-ProvVMUpdateTimeWindow`.

1. Exécutez la commande `Set-ProvVMUpdateTimeWindow`. Par exemple :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
   VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

2. Redémarrez les machines virtuelles.

### Créer des machines virtuelles Windows 11 sur le nœud à locataire unique

Vous pouvez créer des machines virtuelles Windows 11 dans GCP. Toutefois, si vous installez Windows 11 sur l'image principale, vous devez activer vTPM pendant le processus de création de l'image principale. Vous devez également activer vTPM sur la source du profil de la machine (machine virtuelle ou modèle d'instance).

Les principales étapes pour créer des machines virtuelles Windows 11 sur le nœud à locataire unique sont les suivantes :

1. Configurez les environnements de virtualisation Google Cloud. Pour plus d'informations, consultez la section Environnements Google Cloud.
2. Installez un VDA. Reportez-vous à la section Installer des VDA.
3. Créez une connexion à des environnements Google Cloud. Pour plus d'informations, consultez la section Connexion à des environnements Google Cloud.
4. Créez une image principale de Windows 11 BYOL (Bring Your Own License) et importez-la dans Google Cloud. Consultez la section Créer une image principale BYOL Windows 11.
5. Créez la source du profil de machine : provisionnez la machine virtuelle sur le nœud à locataire unique et activez le vTPM du profil de machine source. Consultez la section Provisionner une machine virtuelle sur un nœud à locataire unique.
6. Créez un catalogue de machines MCS à l'aide de la source de profil de machine Windows 11 avec vTPM activé. La source du profil de machine doit avoir le même type d'instance que celui décrit dans le nœud à locataire unique. Consultez la section Créer un catalogue de machines MCS à l'aide de la source de profil de machine Windows 11.

#### Créer une image principale BYOL Windows 11

Il existe deux options pour créer une image principale BYOL Windows 11 et l'importer dans Google Cloud :

- Utiliser les outils Cloud Build de Google Cloud
- Créer l'image principale sur n'importe quel autre hyperviseur

#### Utiliser les outils Cloud Build de Google Cloud

1. Téléchargez les fichiers d'installation ISO de Windows 11, du SDK GCP, de .NET Framework et de PowerShell dans le compartiment de stockage GCP.
2. Indiquez l'emplacement du fichier dans le fichier de création `.yaml` de Cloud Build en tant que paramètre.

3. Exécutez le Cloud Build suivant depuis la ligne de commandes pour créer l'image finale de Windows 11. GCP démarre et crée l'image principale dans le projet sélectionné à l'aide du workflow Daisy dans GCP, puis l'image principale est importée dans GCP.

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
<!--NeedCopy-->
```

> **Remarque :**
>
> Remplacez tout le texte en majuscules par les détails de la ressource.

Pour obtenir des informations complètes, consultez la page Créer des images sous licence BYOL Windows personnalisées.

#### Créer l'image principale sur n'importe quel autre hyperviseur

1. Créez l'image principale de Windows 11 à l'aide de n'importe quel autre hyperviseur.
2. Exportez l'image principale au format OVF vers la machine locale.
3. Téléchargez les fichiers OVF dans le compartiment de stockage GCP à l'aide de l'interface de ligne de commande gcloud locale.

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
<!--NeedCopy-->
```

4. Exécutez le Cloud Build suivant depuis la ligne de commandes pour créer l'image finale de Windows 11. GCP démarre et crée l'image principale dans le projet sélectionné à l'aide du workflow Daisy dans GCP, puis l'image principale est importée dans GCP.

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
<!--NeedCopy-->
```

> **Remarque :**
>
> Remplacez tout le texte en majuscules par les détails de la ressource.

#### Provisionner une machine virtuelle sur un nœud à locataire unique

Utilisez des nœuds à locataire unique pour séparer physiquement vos machines virtuelles des machines virtuelles d'autres projets, ou pour regrouper vos machines virtuelles sur le même matériel hôte. Pour plus d'informations sur le nœud à locataire unique, consultez le document GCP Présentation de la location unique.

Pour provisionner une machine virtuelle (source de profil de machine) sur le nœud à locataire unique, consultez le document GCP Provisionner des VM sur des nœuds à locataire unique.

> **Remarque :**
>
> - Sélectionnez le même type d'instance et la même région que le groupe de nœuds.
> - Activez vTPM dans la section VM protégée. Pour plus d'informations, consultez Guide de démarrage rapide : activer les options de VM protégée.
> - Désactivez le Bitlocker sur la machine virtuelle source.

#### Créer un catalogue de machines MCS à l'aide de la source de profil de machine Windows 11

Vous pouvez créer un catalogue de machines MCS pour créer des machines virtuelles Windows 11 à l'aide de Web Studio ou des commandes PowerShell.

> **Remarque :**
>
> - Pour l'image principale, sélectionnez l'instantané ou la machine virtuelle Windows 11.
> - Pour la source du profil de machine, sélectionnez la machine virtuelle Windows 11 comme profil de machine. La source du profil de machine doit avoir le même type d'instance que celui décrit dans le nœud à locataire unique.

Pour plus d'informations sur l'utilisation de Web Studio, consultez Créer un catalogue de machines à l'aide de Web Studio.

Pour plus d'informations sur les commandes PowerShell, consultez Créer un catalogue de machines à l'aide d'un profil de machine.

Après avoir créé le catalogue et mis sous tension les machines virtuelles, vous pouvez voir les machines virtuelles Windows 11 s'exécuter sur le nœud à locataire unique de la console Google Cloud.

### Google Cloud Marketplace

Vous pouvez parcourir et sélectionner les images proposées par Citrix sur **Google Cloud Marketplace** pour créer des catalogues de machines. Actuellement, MCS prend uniquement en charge le workflow de profil de machine pour cette fonctionnalité.

Pour rechercher un produit Citrix VDA machine virtuelle via Google Cloud Marketplace, accédez à https://console.cloud.google.com/marketplace.

Vous pouvez utiliser une image personnalisée ou une image Citrix Ready sur **Google Cloud Marketplace** pour mettre à jour l'image d'un catalogue de machines.

> **Remarque :**
>
> Si le profil de la machine ne contient pas d'informations sur le type de stockage, la valeur est dérivée de propriétés personnalisées.

Les images prises en charge par Google Cloud Marketplace sont les suivantes :

- Windows 2019 mono-session
- Windows 2019 multi-session
- Ubuntu

Exemple d'utilisation d'une image Citrix comme source pour créer un catalogue de machines :

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \
-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
   win2019-single-vda-v20220819.publicimage \
-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
<!--NeedCopy-->
```

### Autres ressources

- S'il s'agit du premier catalogue créé, Web Studio vous explique comment créer un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, consultez la section Installer et configurer.
- Pour gérer les catalogues, consultez Gérer les catalogues de machines et Gérer un catalogue Google Cloud Platform.

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à des environnements Google Cloud
- Créer des catalogues de machines

## Créer un catalogue de machines HPE Moonshot

June 27, 2024

La section Créer des catalogues de machines décrit les assistants qui permettent de créer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques à des environnements HPE Moonshot.

> **Remarque :**
>
> - Créer une connexion à HPE Moonshot
> - Assurez-vous qu'un ou plusieurs nœuds HPE Moonshot sont disponibles et installez des VDA sur ces nœuds.
> - Pour plus d'informations sur la création de l'image initiale de la cartouche HPE Moonshot, consultez le guide de l'utilisateur du déploiement du système d'exploitation sur Moonshot.

Vous pouvez créer un catalogue de machines HPE Moonshot en utilisant :

- Studio Web
- Commandes PowerShell

### Créer un catalogue de machines à l'aide de Web Studio

Dans l'assistant **Configuration du catalogue de machines** :

1. Sur la page **Système d'exploitation**, sélectionnez **OS multi-session** ou **OS mono-session**.
2. Sur la page **Gestion des machines**, sélectionnez **Machines dont l'alimentation est gérée** et **Autre service ou technologie**.
3. Sur la page **Machines virtuelles**, ajoutez des machines et leurs comptes de machines Active Directory. Vous pouvez effectuer l'une des opérations suivantes :
   - Cliquez sur **Ajouter des machines** pour ajouter des machines manuellement. La fenêtre **Sélectionner des machines virtuelles** apparaît. Développez la connexion au châssis HPE Moonshot que vous avez créée précédemment et sélectionnez les nœuds (machines virtuelles) que vous souhaitez ajouter. Ajoutez ensuite les noms de compte de machine associés.
   - Cliquez sur **Ajouter un fichier CSV** pour ajouter des machines en vrac. Pour plus d'informations sur l'utilisation de fichiers CSV pour ajouter des machines, voir Utiliser des fichiers CSV pour ajouter des machines en vrac à un catalogue.

Les pages **Étendues** et **Résumé** ne contiennent pas d'informations spécifiques à HPE Moonshot.

### Créer un catalogue de machines à l'aide de commandes PowerShell

Exécutez les commandes PowerShell `New-BrokerCatalog` et `New-BrokerMachine` pour créer un catalogue de brokers et importer des machines dans le catalogue de brokers.

Par exemple :

```
New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
    "103.14.252.249" -AllocationType "Random" -IsRemotePC $False -
    MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
    BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
    Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
    -4578-bc07-bcf2a82d1463"
New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
    "103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1" -
    HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
    -1-5-21-2589939477-3963209805-1860259709-1121"
<!--NeedCopy-->
```

### Autres ressources

- S'il s'agit du premier catalogue créé, Web Studio vous explique comment créer un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, consultez la section Installer et configurer.
- Pour gérer les catalogues, consultez Gérer les catalogues de machines et Gérer un catalogue HPE Moonshot

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à HPE Moonshot
- Créer des catalogues de machines

## Créer un catalogue Microsoft Azure

June 28, 2024

> **Remarque :**
>
> Depuis juillet 2023, Microsoft a renommé Azure Active Directory (Azure AD) Microsoft Entra ID. Dans ce document, toute occurrence de l'appellation Azure Active Directory, Azure AD ou de l'acronyme AAD fait désormais référence à Microsoft Entra ID.

La section Créer des catalogues de machines décrit les assistants qui permettent de créer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements de cloud Microsoft Azure Resource Manager.

> **Remarque :**
>
> Avant de créer un catalogue Microsoft Azure, vous devez terminer la création d'une connexion à Microsoft Azure. Voir Connexion à Microsoft Azure.

### Créer un catalogue de machines

Vous pouvez créer un catalogue de machines de deux manières :

- Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans Web Studio
- Créer un catalogue de machines à l'aide de PowerShell

#### Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans Web Studio

Une image peut être un disque, un instantané ou une version d'image d'une définition d'image dans Azure Compute Gallery utilisé pour créer les machines virtuelles dans un catalogue de machines. Avant de créer le catalogue de machines, créez une image dans Azure Resource Manager. Pour obtenir des informations générales sur les images, consultez la rubrique Créer des catalogues de machines.

> **Remarque :**
>
> La prise en charge de l'utilisation d'une image principale provenant d'une région différente de celle configurée dans la connexion hôte est obsolète. Utilisez Azure Compute Gallery pour répliquer l'image principale dans la région souhaitée.

Lors de la préparation de l'image, une machine virtuelle (machine virtuelle) de préparation est créée sur la base de la machine virtuelle d'origine. Cette machine virtuelle de préparation est déconnectée du réseau. Pour déconnecter le réseau de la machine virtuelle de préparation, un groupe de sécurité réseau est créé pour refuser tout trafic entrant et sortant. Le groupe de sécurité réseau est créé automatiquement une fois par catalogue. Le nom du groupe de sécurité réseau est `Citrix-Deny-All-a3pgu-GUID` où le GUID est généré de manière aléatoire. Par exemple, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

Dans l'assistant de création de catalogue de machines :

- Les pages **Type de machine** et **Gestion des machines** ne contiennent aucune information spécifique à Azure. Suivez les instructions de l'article Créer des catalogues de machines.
- Sur la page **Image**, choisissez l'image que vous souhaitez utiliser comme modèle pour créer des machines dans ce catalogue.

  Si vous sélectionnez **Image principale** comme type d'image à utiliser, cliquez sur **Sélectionner une image** et procédez comme suit pour sélectionner une image principale si nécessaire :

1. (Applicable uniquement aux connexions configurées avec des images partagées au sein des locataires ou entre eux) Sélectionnez un abonnement dans lequel se trouve l'image.
2. Sélectionnez un groupe de ressources.
3. Accédez au disque dur virtuel Azure, à Azure Compute Gallery ou à la version Azure de l'image. Ajoutez une note pour l'image sélectionnée si nécessaire.

Lorsque vous sélectionnez une image, tenez compte des points suivants :

- Vérifiez qu'un Citrix VDA est installé sur l'image.
- Si vous sélectionnez un VHD attaché à une machine virtuelle, vous devez arrêter la machine virtuelle avant de passer à l'étape suivante.

> **Remarque :**
>
> - L'abonnement correspondant à la connexion (hôte) qui a créé les machines du catalogue est indiqué par un point vert. Les autres abonnements sont ceux pour lesquels une galerie Azure Compute Gallery est partagée avec cet abonnement. Dans ces abonnements, seules les galeries partagées sont affichées. Pour plus d'informations sur la configuration des abonnements partagés, reportez-vous aux sections Partager des images au sein d'un locataire (entre abonnements) et Partager des images entre locataires.
> - L'utilisation d'un profil de machine avec lancement fiable comme **Type de sécurité** est obligatoire lorsque vous sélectionnez une image ou un instantané pour lequel le lancement fiable est activé. Vous pouvez ensuite activer ou désactiver SecureBoot et vTPM en spécifiant leurs valeurs dans le profil de la machine. Le lancement fiable n'est pas pris en charge pour Shared Image Gallery. Pour plus d'informations sur le lancement fiable Azure, consultez https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
> - Vous pouvez créer un schéma de provisioning à l'aide d'un disque d'OS éphémère sous Windows avec lancement fiable. Lorsque vous sélectionnez une image avec lancement fiable, vous devez sélectionner un profil de machine avec lancement fiable qui est activé avec vTPM. Pour créer des catalogues de machines à l'aide d'un disque d'OS éphémère, consultez Comment créer des machines à l'aide de disques d'OS éphémères.
> - Lorsque la réplication de l'image est en cours, vous pouvez continuer et sélectionner l'image comme image principale et terminer la configuration. Toutefois, la création du catalogue peut prendre plus de temps pendant la réplication de l'image. MCS requiert que la réplication soit terminée dans un délai d'une heure à compter de la création du catalogue. Si le délai de réplication est dépassé, la création du catalogue échoue. Vous pouvez vérifier l'état de la réplication dans Azure. Réessayez si la réplication est toujours en attente ou une fois la réplication terminée.

> - Lorsque vous sélectionnez une image principale pour les catalogues de machines dans Azure, MCS identifie le type de système d'exploitation en fonction de l'image principale et du profil de machine que vous sélectionnez. Si MCS ne parvient pas à l'identifier, sélectionnez le type de système d'exploitation correspondant à l'image principale.
> - Vous pouvez provisionner un catalogue de machines virtuelles Gen2 en utilisant une image Gen2 pour améliorer les performances de démarrage. Toutefois, la création d'un catalogue de machines Gen2 à l'aide d'une image Gen1 n'est pas prise en charge. De même, la création d'un catalogue de machines Gen1 à l'aide d'une image Gen2 n'est pas non plus prise en charge. Par ailleurs, toute image plus ancienne qui ne possède pas d'informations de génération est une image Gen1.

Si vous sélectionnez **Image préparée** comme type d'image à utiliser, cliquez sur **Sélectionner une image** et sélectionnez une image préparée si nécessaire.

Pour garantir la réussite de la création de la machine virtuelle, vérifiez que Citrix VDA 2311 ou version ultérieure est installé sur l'image et que MCSIO est présent sur le VDA.

Une fois que vous avez sélectionné une image, la case **Utiliser un profil de machine (obligatoire pour Azure Active Directory)** est automatiquement cochée. Cliquez sur **Sélectionner un profil de machine** pour accéder à une spécification de modèle ARM ou machine virtuelle à partir d'une liste de groupes de ressources. Les machines virtuelles du catalogue peuvent hériter des configurations du profil de machine sélectionné.

Validez la spécification du modèle ARM pour vous assurer qu'elle peut être utilisée comme profil de machine pour créer un catalogue de machines. Il existe deux manières de valider la spécification du modèle ARM :

- Après avoir sélectionné la spécification du modèle ARM dans la liste des groupes de ressources, cliquez sur **Suivant**. Des messages d'erreur s'affichent si la spécification du modèle ARM contient des erreurs.
- Exécutez une des commandes PowerShell suivantes :
  * `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  * `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

Voici quelques exemples de configurations dont les machines virtuelles peuvent hériter d'un profil de machine :

- Réseaux accélérés
- Diagnostic de démarrage
- Mise en cache du disque hôte (relative aux disques OS et MCSIO)

- Taille de la machine (sauf indication contraire)
- Balises placées sur la machine virtuelle

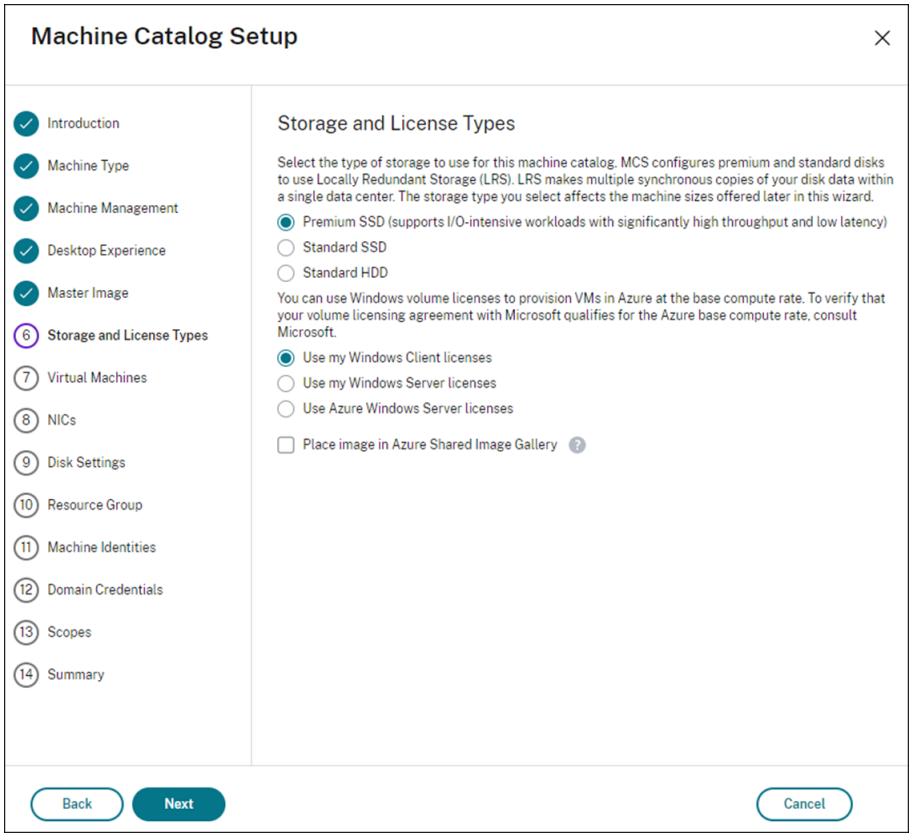
Après avoir créé le catalogue, vous pouvez afficher les configurations du profil de machine dont l'image hérite. Dans le nœud **Catalogues de machines**, sélectionnez le catalogue pour afficher ses détails dans le volet inférieur. Cliquez ensuite sur l'onglet **Propriétés du modèle** pour afficher les propriétés du profil de machine. La section **Balises** affiche jusqu'à trois balises. Pour afficher toutes les balises placées sur la machine virtuelle, cliquez sur **Afficher tout**.

Si vous souhaitez que MCS provisionne des machines virtuelles sur un hôte dédié Azure, cochez la case **Utiliser un groupe d'hôtes dédié**, puis sélectionnez un groupe d'hôtes dans la liste. Un groupe d'hôtes est une ressource qui représente un ensemble d'hôtes dédiés. Un hôte dédié est un service qui fournit des serveurs physiques qui hébergent une ou plusieurs machines virtuelles. Votre serveur est dédié à votre abonnement Azure et n'est pas partagé avec d'autres abonnés. Lorsque vous utilisez un hôte dédié, Azure s'assure que vos machines virtuelles sont les seules machines exécutées sur cet hôte. Cette fonctionnalité convient aux scénarios dans lesquels vous devez répondre à des exigences réglementaires ou de sécurité internes. Pour en savoir plus sur les groupes d'hôtes et les considérations relatives à leur utilisation, consultez la rubrique Hôtes dédiés Azure.

> **Important :**
>
> - Seuls les groupes d'hôtes pour lesquels le placement automatique Azure est activé sont affichés.
> - L'utilisation d'un groupe d'hôtes modifie la page **Machines virtuelles** proposée plus loin dans l'assistant. Seules les tailles de machine contenues dans le groupe d'hôtes sélectionné sont affichées sur cette page. De plus, les zones de disponibilité sont sélectionnées automatiquement et ne sont pas proposées à la sélection.

- La page **Types de stockage et de licence** s'affiche uniquement lors de l'utilisation de l'image Azure Resource Manager.




Les types de stockage suivants peuvent être utilisés pour le catalogue de machines :

- **SSD premium**. Offre une option de stockage sur disque hautes performances et à faible latence adaptée aux machines virtuelles avec des charges d'E/S intensives.
- **SSD standard**. Offre une option de stockage économique qui convient aux charges de travail nécessitant des performances constantes à des niveaux d'E/S par seconde inférieurs.
- **HDD standard**. Offre une option de stockage sur disque fiable et économique adaptée aux machines virtuelles qui exécutent des charges de travail insensibles à la latence.
- **Disque d'OS éphémère Azure**. Offre une option de stockage économique qui réutilise le disque local des machines virtuelles pour héberger le disque du système d'exploitation. Vous pouvez également utiliser PowerShell pour créer des machines qui utilisent des disques d'OS éphémères. Pour plus d'informations, consultez Disques éphémères Azure. Lorsque vous utilisez un disque d'OS éphémère, prenez en compte les points suivants :
  - Le disque d'OS éphémère Azure et les E/S de MCS ne peuvent pas être activés en même temps.
  - Pour mettre à jour les machines qui utilisent des disques d'OS éphémères, vous devez sélectionner une image dont la taille n'excède pas la taille du disque cache ou du disque temporaire de la machine virtuelle.
  - Vous ne pouvez pas utiliser l'option **Conserver la machine virtuelle et le disque système pendant les cycles d'alimentation** proposée ultérieurement dans l'Assistant.

> **Remarque :**
>
> Le disque d'identité est toujours créé à l'aide d'un SSD standard, quel que soit le type de stockage que vous choisissez.

Le type de stockage détermine les tailles de machine qui sont disponibles sur la page **Machines virtuelles** de l'assistant. MCS configure les disques standard et premium pour utiliser le stockage localement redondant (LRS). LRS effectue de multiples copies synchrones de vos données dans un seul data center. Les disques d'OS éphémères Azure utilisent le disque local des machines virtuelles pour stocker le système d'exploitation. Pour de plus amples informations sur les types de stockage et la réplication de stockage Azure, consultez les rubriques suivantes :

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/

Indiquez si vous souhaitez utiliser des licences Windows ou Linux existantes.

- Licences Windows : l'utilisation de licences Windows avec des images Windows (images de support de plate-forme Azure ou images personnalisées) vous permet d'exécuter des machines virtuelles Windows dans Azure à un coût réduit. Il existe deux types de licences :
  - **Licence Windows Server**. Vous permet d'utiliser vos licences Windows Server ou Azure Windows Server, ce qui vous permet d'utiliser Azure Hybrid Benefits. Pour plus de détails, consultez https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. Azure Hybrid Benefit réduit les coûts d'exécution de machine virtuelle dans Azure au taux de calcul de base, les licences Windows Server supplémentaires de la galerie Azure sont donc gratuites.
  - **Licence client Windows**. Vous permet de transférer vos licences Windows 10 et Windows 11 vers Azure, ce qui vous permet d'exécuter des machines virtuelles Windows 10 et Windows 11 dans Azure sans avoir besoin de licences supplémentaires. Pour plus de détails, consultez la section Licences d'accès client et licences de gestion.

Vous pouvez vérifier que la machine virtuelle provisionnée utilise bien une de ces licences en exécutant la commande PowerShell suivante : `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Pour le type de licence Windows Server, vérifiez que le type de licence est **Windows_Server**. Des instructions supplémentaires sont disponibles sur https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.
- Pour le type de licence Client Windows, vérifiez que le type de licence est **Windows_Client**. Des instructions supplémentaires sont disponibles sur https://docs.microsoft.com/en-

us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

Vous pouvez également utiliser le SDK PowerShell `Get-Provscheme` pour effectuer la vérification. Par exemple : `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Pour plus d'informations sur cette applet de commande, voir https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Licences Linux : avec les licences Linux BYOS (Bring-Your-Own-Subscription), vous n'avez pas à payer le logiciel. Les frais BYOS incluent uniquement les frais liés au matériel informatique. Il existe deux types de licences :
  - **RHEL_BYOS** : pour utiliser le type RHEL_BYOS, activez Red Hat Cloud Access sur votre abonnement Azure.
  - **SLES_BYOS** : les versions BYOS de SLES incluent la prise en charge de SUSE.

  Vous pouvez définir la valeur LicenseType sur les options Linux dans les champs `New-ProvScheme` et `Set-ProvScheme`.

  Exemple de définition de LicenseType sur RHEL_BYOS dans le champ `New-ProvScheme` :

```
1 New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "
      azureCatalog" -RunAsynchronously -Scope @() -SecurityGroup
      @() -CustomProperties '<CustomProperties xmlns="http://
      schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http
      ://www.w3.org/2001/XMLSchema-instance"><Property xsi:type="
      StringProperty" Name="UseManagedDisks" Value="true" /><
      Property xsi:type="StringProperty" Name="StorageAccountType
      " Value="StandardSSD_LRS" /><Property xsi:type="
      StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
      /><Property xsi:type="StringProperty" Name="OsType" Value="
      Linux" /><Property xsi:type="StringProperty" Name="
      LicenseType" Value="RHEL_BYOS" /></CustomProperties>'
2 <!--NeedCopy-->
```

  Exemple de définition de LicenseType sur SLES_BYOS dans le champ `Set-ProvScheme` :

```
1 Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
      CustomProperties '<CustomProperties xmlns="http://schemas.
      citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
      w3.org/2001/XMLSchema-instance"><Property xsi:type="
      StringProperty" Name="UseManagedDisks" Value="true" /><
      Property xsi:type="StringProperty" Name="StorageAccountType
      " Value="StandardSSD_LRS" /><Property xsi:type="
      StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
      /><Property xsi:type="StringProperty" Name="OsType" Value="
```

```
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="SLES_BYOS" /></CustomProperties>'
<!--NeedCopy-->
```

> **Remarque :**
>
> Si la valeur `LicenseType` est vide, les valeurs par défaut sont Azure Windows Server License ou Azure Linux License, selon la valeur OsType.

Exemple de définition de LicenseType sur une valeur vide :

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.
    w3.org/2001/XMLSchema-instance"><Property xsi:type="
    StringProperty" Name="UseManagedDisks" Value="true" /><
    Property xsi:type="StringProperty" Name="StorageAccountType
    " Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /></CustomProperties>'
<!--NeedCopy-->
```

Consultez les documents suivants pour comprendre les types de licence et leurs avantages :

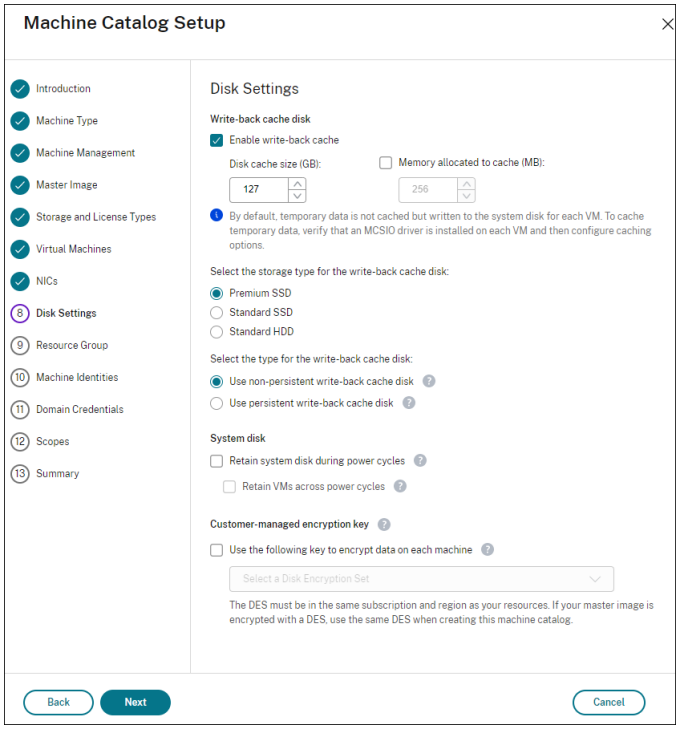
- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery (anciennement Azure Shared Image Gallery) est un référentiel permettant de gérer et de partager des images. Il vous permet de mettre vos images à disposition de l'ensemble de votre organisation. Nous vous recommandons de stocker une image dans SIG lors de la création de catalogues de machines non persistants volumineux, car cela permet de réinitialiser plus rapidement les disques du système d'exploitation VDA. Après avoir sélectionné **Placer l'image préparée dans Azure Compute Gallery**, la section **Paramètres d'Azure Compute Gallery** apparaît, vous permettant de spécifier des paramètres Azure Compute Gallery supplémentaires :

- **Ratio réplicas d'images/machines virtuelles**. Permet de spécifier le ratio entre les machines virtuelles et les réplicas d'images que vous souhaitez conserver dans Azure. Par défaut, Azure conserve un réplica d'image unique pour 40 machines non persistantes. Pour les machines persistantes, ce nombre est 1 000 par défaut.
- **Nombre maximal de réplicas**. Vous permet de spécifier le nombre maximal de réplicas d'images que vous souhaitez qu'Azure conserve. La valeur par défaut est 10.

- Sur la page **Machines virtuelles**, indiquez le nombre de machines virtuelles à créer. Vous devez en spécifier au moins une et sélectionner une taille de machine. Après la création du catalogue, vous pouvez modifier la taille de machine en modifiant le catalogue.
- La page **Cartes d'interface réseau** ne contient pas d'informations spécifiques à Azure. Suivez les instructions de l'article Créer des catalogues de machines.
- Sur la page **Paramètres du disque**, indiquez si vous souhaitez activer le cache en écriture différée. Lorsque la fonctionnalité d'optimisation du stockage MCS est activée, vous pouvez configurer les paramètres suivants lors de la création d'un catalogue. Ces paramètres s'appliquent aux environnements Azure et GCP.




Après avoir activé le cache en écriture différée, vous pouvez effectuer les opérations suivantes :

- Configurez la taille du disque et de la RAM utilisés pour la mise en cache des données temporaires. Pour plus d'informations, consultez Configurer un cache pour les données temporaires.
- Sélectionnez le type de stockage pour le disque de cache en écriture différée. Les options de stockage suivantes peuvent être utilisées pour le disque de cache en écriture différée :
  - SSD premium
  - SSD standard
  - HDD standard
- Choisissez si vous souhaitez que le disque de cache en écriture différée persiste pour les machines virtuelles provisionnées. Sélectionnez **Activer le cache en écriture différée**

pour voir les options disponibles. Par défaut, l'option **Utiliser disque de cache en écriture différée non persistant** est sélectionnée.

- Sélectionnez le type de disque de cache en écriture différée.
  - **Utilisez disque de cache en écriture différée non persistant**. Si cette option est sélectionnée, le disque de cache en écriture différée est supprimé pendant les cycles d'alimentation. Toutes les données qui y sont redirigées seront perdues. Si le disque temporaire de la machine virtuelle dispose de suffisamment d'espace, il est utilisé pour héberger le disque de cache en écriture différée afin de réduire vos coûts. Après la création du catalogue, vous pouvez vérifier si les machines provisionnées utilisent le disque temporaire. Pour ce faire, cliquez sur le catalogue et vérifiez les informations de l'onglet **Propriétés du modèle**. Si le disque temporaire est utilisé, l'option **Disque de cache en écriture différée non persistant** est affichée et sa valeur est **Oui (à l'aide du disque temporaire de la machine virtuelle)**. Si ce n'est pas le cas, l'option **Disque de cache en écriture différée non persistant** est affichée et sa valeur est **Non (sans le disque temporaire de la machine virtuelle)**.
  - **Utiliser disque de cache en écriture différée persistant**. Si cette option est sélectionnée, le disque de cache en écriture différée persiste pour les machines virtuelles provisionnées. L'activation de cette option augmente vos coûts de stockage.
- Indiquez si vous souhaitez conserver les machines virtuelles et les disques système pour les VDA pendant les cycles d'alimentation.

  **Conservation des machines virtuelles et des disques système pendant les cycles d'alimentation**. Disponible lorsque vous avez sélectionné **Activer le cache en écriture différée**. Par défaut, les machines virtuelles et les disques système sont supprimés à l'arrêt et recréés au démarrage. Si vous souhaitez réduire les temps de redémarrage des machines virtuelles, sélectionnez cette option. N'oubliez pas que l'activation de cette option augmente également les coûts de stockage.
- Choisissez si vous souhaitez activer les **Économies sur les coûts de stockage**. Si cette option est activée, réduisez les coûts de stockage en rétrogradant le disque de stockage vers un disque dur standard lorsque la machine virtuelle s'arrête. La machine virtuelle revient à ses paramètres d'origine au redémarrage. L'option s'applique à la fois aux disques de stockage et aux disques de cache à écriture différée. Vous pouvez également utiliser PowerShell. Voir Changer le type de stockage vers un niveau inférieur lorsqu'une machine virtuelle est arrêtée.

  > **Remarque :**
  >
  > Microsoft impose des restrictions sur la modification du type de stockage lors de l'arrêt de la machine virtuelle. Il est également possible que Microsoft bloque les changements de type de stockage à l'avenir. Pour plus d'informations, consultez cet article

> Microsoft.

- Indiquez si vous souhaitez chiffrer les données sur les machines provisionnées dans le catalogue. Le chiffrement côté serveur à l'aide d'une clé de chiffrement gérée par le client vous permet de gérer le chiffrement au niveau du disque géré et de protéger les données sur les machines du catalogue. Pour plus d'informations, consultez Chiffrement Azure côté serveur.

- Sur la page **Groupe de ressources**, choisissez si vous souhaitez créer des groupes de ressources ou utiliser des groupes existants.

  - Si vous choisissez de créer des groupes de ressources, sélectionnez **Suivant**.
  - Si vous choisissez d'utiliser des groupes de ressources existants, sélectionnez les groupes dans la liste **Groupes de ressources de provisioning disponibles**. **Rappel** : sélectionnez un nombre suffisant de groupes pour prendre en charge les machines que vous créez dans le catalogue. Un message s'affiche si vous n'en choisissez pas assez. Vous pouvez sélectionner un nombre supérieur au minimum requis si vous envisagez d'ajouter d'autres machine virtuelle au catalogue ultérieurement. Vous ne pouvez pas ajouter d'autres groupes de ressources à un catalogue après que le catalogue a été créé.

  Pour plus d'informations, consultez la rubrique Groupes de ressources Azure.

- Sur la page **Identités des machines**, choisissez un type d'identité et configurez les identités des machines de ce catalogue. Si vous sélectionnez **Joint à Azure Active Directory** pour les machines virtuelles, vous pouvez les ajouter à un groupe de sécurité Azure AD. Les étapes détaillées sont les suivantes :

  1. Dans le champ **Type d'identité**, sélectionnez **Joint à Azure Active Directory**. L'option **Groupe de sécurité Azure AD (facultatif)** s'affiche.
  2. Cliquez sur **Groupe de sécurité Azure AD : Créer un nouveau**.
  3. Entrez un nom de groupe, puis cliquez sur **Créer**.
  4. Suivez les instructions qui s'affichent à l'écran pour vous connecter à Azure.
     Si le nom du groupe n'existe pas dans Azure, une icône verte apparaît. Dans le cas contraire, un message d'erreur s'affiche vous demandant de saisir un nouveau nom.
  5. Entrez le schéma de dénomination des comptes de machines virtuelles.

  Après la création du catalogue, Citrix Virtual Apps and Desktops accède à Azure en votre nom et crée le groupe de sécurité ainsi qu'une règle d'appartenance dynamique pour le groupe. Selon cette règle, les machines virtuelles dont le schéma de dénomination est spécifié dans ce catalogue sont automatiquement ajoutées au groupe de sécurité.

  Pour ajouter des machines virtuelles avec un schéma de dénomination différent à ce catalogue, vous devez vous connecter à Azure. Citrix Virtual Apps and Desktops peut ensuite accéder à

Azure et créer une règle d'appartenance dynamique basée sur le nouveau schéma de dénomination.

Lorsque vous supprimez ce catalogue, la suppression du groupe de sécurité d'Azure nécessite également de vous connecter à Azure.

- Les pages **Informations d'identification du domaine** et **Résumé** ne contiennent pas d'informations spécifiques à Azure. Suivez les instructions de l'article Créer des catalogues de machines.

Suivez les instructions de l'assistant.

### Conditions pour que le disque temporaire Azure puisse être utilisé comme disque de cache en écriture différée

Vous pouvez utiliser le disque temporaire Azure en tant que disque de cache en écriture différée uniquement si toutes les conditions suivantes sont remplies :

- Le disque de cache en écriture différée ne doit pas persister car le disque temporaire Azure n'est pas approprié pour les données persistantes.
- La taille de machine virtuelle Azure choisie doit inclure un disque temporaire.
- Il n'est pas nécessaire d'activer le disque d'OS éphémère.
- Acceptez de placer le fichier de cache en écriture différée sur le disque temporaire Azure.
- La taille du disque temporaire Azure doit être supérieure à la taille totale de (taille du disque du cache en écriture différée + espace réservé pour le fichier d'échange + 1 Go d'espace tampon).

### Scénarios de disque de cache en écriture différée non persistant

Le tableau suivant décrit trois scénarios différents dans lesquels un disque temporaire est utilisé pour le cache en écriture différée lors de la création d'un catalogue de machines.

| Scénario | Résultat |
| --- | --- |
| Toutes les conditions pour utiliser un disque temporaire pour le cache en écriture différée sont remplies. | Le fichier WBC `mcsdif.vhdx` est placé sur le disque temporaire. |
| Le disque temporaire ne dispose pas d'espace suffisant pour l'utilisation du cache en écriture différée. | Un disque VHD `MCSWCDisk` est créé et un fichier WBC `mcsdif.vhdx` est placé sur ce disque. |

| Scénario | Résultat |
| --- | --- |
| Le disque temporaire dispose de suffisamment d'espace pour l'utilisation du cache en écriture différée, mais `UseTempDiskForWBC` est défini sur **false**. | Un disque VHD `MCSWCDisk` est créé et un fichier WBC `mcsdif.vhdx` est placé sur ce disque. |

### Créer une spécification de modèle Azure

Vous pouvez créer une spécification de modèle Azure dans le portail Azure et l'utiliser dans Web Studio ou exécuter des commandes PowerShell pour créer ou mettre à jour un catalogue de machines MCS.

Pour créer une spécification de modèle Azure pour une machine virtuelle existante :

1. Accédez au portail Azure. Sélectionnez un groupe de ressources, puis sélectionnez la machine virtuelle et l'interface réseau. Dans le menu **...** en haut de la page, cliquez sur **Exporter le modèle**.
2. Décochez la case **Inclure les paramètres** si vous souhaitez créer une spécification de modèle pour le provisioning du catalogue.
3. Cliquez sur **Ajouter à la bibliothèque** pour modifier ultérieurement la spécification de modèle.
4. Sur la page **Importation du modèle**, entrez les informations requises telles que le **nom**, l'**abonnement**, le **groupe de ressources**, l'**emplacement** et **la version**. Cliquez sur **Suivant : Modifier le modèle**.
5. Vous avez également besoin d'une interface réseau en tant que ressource indépendante si vous souhaitez provisionner des catalogues. Par conséquent, vous devez supprimer tout `dependsOn` spécifié dans la spécification de modèle. Par exemple :

   ```
   "dependsOn": [
   "[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
   ],
   <!--NeedCopy-->
   ```

6. Créez **Examiner et créer** et créez la spécification de modèle.
7. Sur la page **Specs de modèle**, vérifiez la spécification de modèle que vous venez de créer. Cliquez sur la spécification de modèle. Dans le panneau de gauche, cliquez sur **Versions**.
8. Vous pouvez créer une nouvelle version en cliquant sur **Créer version**. Spécifiez un nouveau numéro de version, modifiez la spécification de modèle actuelle, puis cliquez sur **Examiner et créer** pour créer la nouvelle version de la spécification de modèle.

Vous pouvez obtenir des informations sur la spécification de modèle et la version du modèle à l'aide des commandes PowerShell suivantes :

- Pour obtenir des informations sur la spécification de modèle, exécutez :

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec
<!--NeedCopy-->
```

- Pour obtenir des informations sur la version de la spécification de modèle, exécutez :

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
    templatespecversion
<!--NeedCopy-->
```

### Utiliser une spécification de modèle pour créer ou mettre à jour un catalogue

Vous pouvez créer ou mettre à jour un catalogue de machines MCS à l'aide d'une spécification de modèle comme entrée de profil de machine. Pour ce faire, vous pouvez utiliser les commandes Web Studio ou PowerShell.

- Pour Web Studio, voir Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans Web Studio.
- Pour PowerShell, voir Utiliser une spécification de modèle lors de la création ou de la mise à jour d'un catalogue à l'aide de PowerShell.

### Chiffrement Azure côté serveur

Citrix Virtual Apps and Desktops prend en charge les clés de cryptage gérées par le client pour les disques gérés Azure via Azure Key Vault. Cette prise en charge vous permet de gérer vos exigences en matière d'organisation et de conformité en chiffrant les disques gérés de votre catalogue de machines à l'aide de vos propres clés de chiffrement. Pour plus d'informations, consultez Chiffrement côté serveur de stockage sur disque Azure.

Lors de l'utilisation de cette fonctionnalité pour les disques gérés :

- Pour modifier la clé avec laquelle le disque est chiffré, modifiez la clé actuelle dans `DiskEncryptionSet`. Toutes les ressources associées à la modification de `DiskEncryptionSet` doivent être chiffrées avec la nouvelle clé.
- Lorsque vous désactivez ou supprimez votre clé, toutes les machines virtuelles avec des disques utilisant cette clé s'arrêtent automatiquement. Après l'arrêt, les machines virtuelles ne sont pas utilisables, sauf si la clé est réactivée ou si vous attribuez une nouvelle clé. Tout catalogue utilisant la clé ne peut pas être mis sous tension et vous ne pouvez pas y ajouter de machines virtuelles.

#### Considérations importantes lors de l'utilisation de clés de chiffrement gérées par le client

Tenez compte de ce qui suit lors de l'utilisation de cette fonctionnalité :

- Toutes les ressources associées aux clés gérées par le client (instances Azure Key Vaults, jeux de cryptage de disque, machines virtuelles, disques et instantanés) doivent résider dans le même abonnement et la même région.
- Une fois que vous avez activé la clé de chiffrement gérée par le client, vous ne pouvez pas la désactiver ultérieurement. Si vous souhaitez désactiver ou supprimer la clé de chiffrement gérée par le client, copiez toutes les données sur un autre disque géré qui n'utilise pas la clé de chiffrement gérée par le client.
- Les disques créés à partir d'images personnalisées chiffrées à l'aide du chiffrement côté serveur et des clés gérées par le client doivent être chiffrés à l'aide des mêmes clés gérées par le client. Ces disques doivent résider dans le même abonnement.
- Les instantanés créés à partir de disques chiffrés à l'aide du chiffrement côté serveur et des clés gérées par le client doivent être chiffrés à l'aide des mêmes clés gérées par le client.
- Les disques, instantanés et images chiffrés à l'aide de clés gérées par le client ne peuvent pas être transférés vers un autre groupe de ressources et un autre abonnement.
- Les disques gérés, actuellement ou préalablement chiffrés à l'aide d'Azure Disk Encryption, ne peuvent pas être chiffrés à l'aide de clés gérées par le client.
- Consultez le site Microsoft pour connaître les limitations des jeux de cryptage de disque par région.

> **Remarque :**
>
> Consultez Démarrage rapide : créer un coffre de clés avec le portail Azure pour plus d'informations sur la configuration du cryptage Azure côté serveur.

### Clé de cryptage gérée par le client Azure

Lors de la création d'un catalogue de machines, vous pouvez choisir de chiffrer les données sur les machines provisionnées dans le catalogue. Le chiffrement côté serveur à l'aide d'une clé de chiffrement gérée par le client vous permet de gérer le chiffrement au niveau du disque géré et de protéger les données sur les machines du catalogue. Un jeu de chiffrement de disque (Disk Encryption Set ou DES) représente une clé gérée par le client. Pour utiliser cette fonctionnalité, vous devez d'abord créer votre DES dans Azure. Un DES est dans le format suivant :

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption`

Sélectionnez un DES dans la liste. Le DES sélectionné doit se trouver dans le même abonnement et la même région que vos ressources. Si votre image est chiffrée avec un DES, utilisez le même DES lors de la création du catalogue de machines. Vous ne pouvez pas modifier le DES après avoir créé le catalogue.

Si vous créez un catalogue avec une clé de cryptage et que vous désactivez ultérieurement le DES correspondant dans Azure, vous ne pouvez plus mettre les machines du catalogue sous tension ou y ajouter des machines.

Consultez la section Créer un catalogue de machines à l'aide d'une clé gérée par le client.

### Cryptage de disque sur l'hôte Azure

Vous pouvez créer un catalogue de machines MCS avec fonctionnalité de cryptage sur l'hôte. Actuellement, MCS prend uniquement en charge le workflow de profil de machine pour cette fonctionnalité. Vous pouvez utiliser une machine virtuelle ou une spécification de modèle comme entrée pour un profil de machine.

Cette méthode de chiffrement ne chiffre pas les données via le stockage Azure. Le serveur hébergeant la machine virtuelle chiffre les données, puis les données chiffrées circulent via le serveur de stockage Azure. Par conséquent, cette méthode de chiffrement chiffre les données de bout en bout.

**Restrictions :**

Limites du chiffrement de disque Azure sur l'hôte :

- Non pris en charge pour toutes les tailles de machines Azure
- Incompatible avec le chiffrement de disque Azure

Pour créer un catalogue de machines avec fonctionnalité de chiffrement sur l'hôte, procédez comme suit :

1. Vérifiez si la fonctionnalité de chiffrement sur l'hôte est activée ou non dans l'abonnement. Pour ce faire, voir https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Si elle n'est pas activée, vous devez activer la fonctionnalité pour l'abonnement. Pour plus d'informations sur l'activation de cette fonctionnalité pour votre abonnement, consultez https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Vérifiez si une taille de machine virtuelle Azure particulière prend en charge le chiffrement sur l'hôte ou non. Pour ce faire, dans une fenêtre PowerShell, exécutez l'une des opérations suivantes :

```
1 PS XDHyp:\Connections<your connection>\east us.region\
     serviceoffering.folder>
2 <!--NeedCopy-->
```

```
PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
<!--NeedCopy-->
```

3. Créez une machine virtuelle ou une spécification de modèle, en tant qu'entrée pour le profil de la machine, dans le portail Azure avec le chiffrement sur l'hôte activé.

   - Si vous souhaitez créer une machine virtuelle, sélectionnez une taille de machine virtuelle qui prend en charge le chiffrement sur l'hôte. Une fois la machine virtuelle créée, la propriété de la machine virtuelle **Chiffrement sur l'hôte** est activée.
   - Si vous souhaitez utiliser une spécification de modèle, attribuez au paramètre `Encryption at Host` la valeur **true** dans `securityProfile`.

4. Créez un catalogue de machines MCS avec un workflow de profil de machine en sélectionnant une machine virtuelle ou une spécification de modèle.

   - Disque d'OS/disque de données : chiffré via une clé gérée par le client et une clé gérée par la plate-forme
   - Disque d'OS éphémère : chiffré uniquement via une clé gérée par la plate-forme
   - Disque cache : chiffré via une clé gérée par le client et une clé gérée par la plate-forme

   Vous pouvez créer le catalogue de machines à l'aide de Web Studio ou en exécutant des commandes PowerShell.

#### Récupérer les informations de chiffrement sur l'hôte à partir d'un profil de machine

Vous pouvez récupérer les informations de chiffrement sur l'hôte à partir d'un profil de machine lorsque vous exécutez la commande PowerShell avec le paramètre `AdditionalData`. Si le paramètre `EncryptionAtHost` est **True**, cela indique que le chiffrement sur l'hôte est activé pour le profil de machine.

Par exemple : lorsque l'entrée du profil de machine est une machine virtuelle, exécutez la commande suivante :

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def.vm).AdditionalData
<!--NeedCopy-->
```

Par exemple : lorsque l'entrée du profil de la machine est une spécification de modèle, exécutez la commande suivante :

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
   templatespecversion).AdditionalData
<!--NeedCopy-->
```

### Chiffrement double sur disque géré

Vous pouvez créer un catalogue de machines avec chiffrement double. Tous les catalogues créés à l'aide de cette fonctionnalité sont chiffrés côté serveur à l'aide de clés gérées par la plate-forme et par le client. Vous possédez et gérez Azure Key Vault, la clé de chiffrement et les jeux de chiffrement de disque (DES).

Le chiffrement double est un chiffrement côté plate-forme (par défaut) et un chiffrement géré par le client (CMEK). Par conséquent, si vous êtes un client gérant des données sensibles en termes de sécurité et que vous êtes préoccupé par le risque associé à un algorithme de cryptage, à une mise en œuvre ou à une clé compromise, vous pouvez opter pour ce cryptage double. Les disques du système d'exploitation et de données persistants, ainsi que les instantanés et les images sont chiffrés au repos à l'aide du chiffrement double.

> **Remarque :**
>
> - Vous pouvez créer et mettre à jour un catalogue de machines utilisant un chiffrement double à l'aide de Web Studio et de commandes PowerShell. Reportez-vous à la section Créer un catalogue de machines avec chiffrement double pour les commandes PowerShell.
> - Vous pouvez utiliser un workflow non basé sur un profil de machine ou un workflow basé sur un profil de machine pour créer ou mettre à jour un catalogue de machines utilisant un cryptage double.
> - Si vous créez un catalogue de machines à l'aide d'un workflow non basé sur un profil de machine, vous pouvez réutiliser l'ID `DiskEncryptionSetId` stocké.
> - Si vous utilisez un profil de machine, vous pouvez utiliser une machine virtuelle ou une spécification de modèle comme entrée de profil de machine.

**Limitations :**

- Le chiffrement double n'est pas pris en charge pour les disques Ultra Disks ou Premium SSD v2.
- Le chiffrement double n'est pas pris en charge sur les disques non gérés.
- Si vous désactivez une clé DiskEncryptionSet associée à un catalogue, les machines virtuelles du catalogue sont désactivées.
- Toutes les ressources associées à vos clés gérées par le client (Azure Key Vault, jeux de chiffrement de disque, machines virtuelles, disques et instantanés) doivent résider dans le même abonnement et la même région.
- Vous ne pouvez créer qu'un maximum de 50 jeux de cryptage de disque par région et par abonnement.
- Vous ne pouvez pas mettre à jour un catalogue de machines qui possède déjà un élément `DiskEncryptionSetId` avec un autre élément `DiskEncryptionSetId`.

## Groupes de ressources Azure

Les groupes de ressources de provisioning d'Azure permettent de provisionner les machine virtuelle qui fournissent des applications et bureaux aux utilisateurs. Vous pouvez ajouter des groupes de ressources Azure vides existants lorsque vous créez un catalogue de machines MCS, ou ils peuvent être créés pour vous. Pour plus d'informations sur les groupes de ressources Azure, consultez la documentation Microsoft.

### Utilisation du groupe de ressources Azure

Le nombre de machines virtuelles, de disques gérés, d'instantanés et d'images par groupe de ressources Azure n'est pas limité. (La limitation de 240 machines virtuelles/800 disques gérés par groupe de ressources Azure a été supprimée.)

- Lorsque vous utilisez le principal de service à étendue complète pour créer un catalogue de machines, MCS crée uniquement un groupe de ressources Azure et utilise ce groupe pour le catalogue.
- Lorsque vous utilisez le principal de service à étendue limitée pour créer un catalogue de machines, vous devez fournir un groupe de ressources Azure précréé vide pour le catalogue.

## Disques éphémères Azure

Un disque éphémère Azure vous permet de réutiliser le disque cache ou le disque temporaire pour stocker le disque d'OS d'une machine virtuelle compatible Azure. Cette fonctionnalité est utile pour les environnements Azure qui nécessitent un disque SSD plus performant sur un disque dur standard. Pour plus d'informations sur la création d'un catalogue avec un disque éphémère Azure, voir Créer un catalogue avec un disque éphémère Azure.

> **Remarque :**
>
> Les catalogues persistants ne prennent pas en charge les disques d'OS éphémères.

Les disques d'OS éphémères nécessitent que votre schéma de provisioning utilise des disques gérés et une galerie d'images partagées.

### Stockage d'un disque temporaire d'OS éphémère

Vous avez la possibilité de stocker un disque d'OS éphémère sur le disque temporaire de la machine virtuelle ou sur un disque de ressources. Cette fonctionnalité vous permet d'utiliser un disque d'OS éphémère avec une machine virtuelle qui ne possède pas de cache ou dont le cache est insuffisant.

Ces machines virtuelles disposent d'un disque temporaire ou de ressources pour stocker un disque d'OS éphémère, tel que `Ddv4`.

Tenez compte des considérations suivantes :

- Un disque éphémère est stocké soit sur le disque cache de la machine virtuelle, soit sur le disque temporaire (ressource) de la machine virtuelle. Le disque de cache est préféré au disque temporaire, sauf si le disque de cache n'est pas suffisamment grand pour le contenu du disque d'OS.
- Pour les mises à jour, une nouvelle image plus grande que le disque cache mais plus petite que le disque temporaire entraîne le remplacement du disque d'OS éphémère par le disque temporaire de la machine virtuelle.

### Optimisation du stockage MCS (Machine Creation Services) (E/S de MCS) et du disque d'OS éphémère

Le disque d'OS éphémère Azure et les E/S de MCS ne peuvent pas être activés en même temps.

Remarques importantes :

- Vous ne pouvez pas créer un catalogue de machines avec le disque d'OS éphémère et les E/S de MCS activés en même temps.
- Les paramètres PowerShell (`UseWriteBackCache` et `UseEphemeralOsDisk`) échouent avec des messages d'erreur appropriés si vous les définissez sur **true** dans `New-ProvScheme` ou `Set-ProvScheme`.
- Pour les catalogues de machines existants créés avec les deux fonctionnalités activées, vous pouvez toujours :
  - mettre un catalogue de machines à jour
  - ajouter ou supprimer des machines virtuelles
  - supprimer un catalogue de machines

### Azure Compute Gallery

Utilisez Azure Compute Gallery (anciennement Azure Shared Image Gallery) en tant que référentiel d'images publiées pour les machines provisionnées avec MCS dans Azure. Vous pouvez stocker une image publiée dans la galerie pour accélérer la création et l'hydratation des disques du système d'exploitation, ce qui améliore les temps de démarrage et de lancement des applications pour les machines virtuelles non persistantes. Shared Image Gallery contient les trois éléments suivants :

- *Galerie* : les images sont stockées ici. MCS crée une galerie pour chaque catalogue de machines.

- *Définition de l'image de la galerie* : cette définition inclut des informations (type et état du système d'exploitation, région Azure) sur l'image publiée. MCS crée une définition d'image pour chaque image créée pour le catalogue.
- *Version d'image de la galerie*: chaque image de Shared Image Gallery peut avoir plusieurs versions, et chaque version peut avoir plusieurs réplicas dans différentes régions. Chaque réplica est une copie complète de l'image publiée.

> **Remarque :**
>
> La fonctionnalité Shared Image Gallery est uniquement compatible avec les disques gérés. Elle n'est pas disponible pour les anciens catalogues de machines.

Pour plus d'informations, consultez la rubrique Vue d'ensemble d'Azure Compute Gallery.

Pour plus d'informations sur la création ou la mise à jour d'un catalogue de machines à l'aide d'une image Azure Compute Gallery avec PowerShell, voir Créer ou mettre à jour un catalogue de machines à l'aide d'une image Azure Compute Gallery.

### Machines virtuelles confidentielles Azure

Les machines virtuelles informatiques confidentielles Azure garantissent que votre bureau virtuel est chiffré en mémoire et protégé lors de son utilisation.

Vous pouvez utiliser MCS pour créer un catalogue avec des machines virtuelles confidentielles Azure. Vous devez utiliser le workflow du profil de machine pour créer un tel catalogue. Vous pouvez utiliser les spécifications de modèle VM et ARM comme entrée de profil de machine.

#### Considérations importantes concernant les machines virtuelles confidentielles

Considérations importantes concernant les tailles de machines virtuelles prises en charge et la création d'un catalogue de machines avec des machines virtuelles confidentielles :

- Tailles de machines virtuelles prises en charge : les machines virtuelles confidentielles prennent en charge les tailles de machines virtuelles suivantes :
  - Série DCasv5
  - Série DCadsv5
  - Série ECasv5
  - Série ECadsv5
- Créez un catalogue de machines avec des machines virtuelles confidentielles.
  - Vous pouvez créer un catalogue de machines virtuelles confidentielles Azure à l'aide des commandes Web Studio et PowerShell.

- Vous devez utiliser un workflow basé sur le profil de machine pour créer un catalogue de machines avec des machines virtuelles confidentielles Azure. Vous pouvez utiliser une machine virtuelle ou une spécification de modèle comme entrée de profil de machine.
- L'image principale et l'entrée du profil de la machine doivent toutes deux être activées avec le même type de sécurité confidentiel. Ces types de sécurité sont les suivants :
  * **VMGuestStateOnly** : machine virtuelle confidentielle avec cryptage de l'état invité seulement de la machine virtuelle
  * **DiskWithVMGuestState** : machine virtuelle confidentielle avec cryptage du disque du système d'exploitation et de l'état invité de la machine virtuelle à l'aide d'une clé gérée par la plate-forme ou d'une clé gérée par le client. Les disques du système d'exploitation normal et éphémère peuvent être chiffrés.
- Le paramètre AdditionalData vous permet d'obtenir des informations de machine virtuelle confidentielle sur différents types de ressources, tels qu'un disque géré, un instantané, une image Azure Compute Gallery, une machine virtuelle et une spécification de modèle ARM. Par exemple :

  ```
  PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
     \image.folder\username-dev-testing-rg.resourcegroup\
     username-dev-tsvda.vm).AdditionalData
  <!--NeedCopy-->
  ```

  Les champs de données supplémentaires sont les suivants :
  * DiskSecurityType
  * ConfidentialVMDiskEncryptionSetId
  * DiskSecurityProfiles

  Pour obtenir la propriété informatique confidentielle d'une taille de machine, exécutez la commande suivante : `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  Le champ de données supplémentaire est `ConfidentialComputingType`.
- Vous ne pouvez pas modifier l'image principale ou le profil de la machine d'un type de sécurité confidentiel vers un type de sécurité non confidentiel, ou d'un type de sécurité non confidentiel vers un type de sécurité confidentiel.
- Vous obtenez des messages d'erreur appropriés pour toute configuration incorrecte.

#### Préparer des images principales et des profils de machines

Avant de créer un ensemble de machines virtuelles confidentielles, préparez leur image principale et leur profil de machine en procédant comme suit :

1. Dans le portail Azure, créez une machine virtuelle confidentielle avec des paramètres spécifiques, tels que :

   - **Type de sécurité** : machines virtuelles confidentielles
   - **Cryptage des disques confidentiels du système d'exploitation** : activé.
   - **Gestion des clés** : cryptage des disques confidentiels à l'aide d'une clé gérée par la plateforme

     Pour plus d'informations sur la création de machines virtuelles confidentielles, consultez cet article de Microsoft.

2. Préparez l'image principale sur la machine virtuelle créée. Installez les applications et le VDA nécessaires sur la machine virtuelle créée.

   > **Remarque :**
   >
   > La création de machines virtuelles confidentielles à l'aide d'un disque dur virtuel n'est pas prise en charge. Pour cela, utilisez plutôt Azure Compute Gallery, des disques gérés ou des instantanés.

3. Créez le profil de machine en appliquant l'une des méthodes suivantes :

   - Utilisez la machine virtuelle existante créée à l'étape 1 si elle possède les propriétés de machine nécessaires.
   - Si vous optez pour une spécification de modèle ARM comme profil de machine, créez la spécification de modèle selon vos besoins. Plus spécifiquement, vous devez configurer les paramètres qui répondent à la configuration requise de votre machine virtuelle confidentielle, tels que *SecurityEncryptionType* et *diskEncryptionSet* (pour les clés gérées par le client). Pour plus d'informations, consultez Créer une spécification de modèle Azure.

     > **Remarque :**
     >
     > - Assurez-vous que l'image principale et le profil de la machine ont le même type de clé de sécurité.
     > - Pour créer des machines virtuelles confidentielles nécessitant un cryptage des disques confidentiels du système d'exploitation à l'aide d'une clé gérée par le client, assurez-vous que les ID du jeu de cryptage de disque sont identiques dans l'image principale et dans le profil de la machine.

#### Créer des machines virtuelles confidentielles à l'aide des commandes Web Studio ou PowerShell

Pour créer un ensemble de machines virtuelles confidentielles, créez un catalogue de machines à l'aide d'une image principale et d'un profil de machine dérivé de la machine virtuelle confidentielle souhaitée.

Pour créer le catalogue à l'aide de Web Studio, suivez les étapes décrites dans l'article Créer des catalogues de machines. Gardez à l'esprit les considérations suivantes :

- Sur la page **Image**, sélectionnez l'image principale et le profil de machine que vous avez préparés en vue de la création d'une machine virtuelle confidentielle. La sélection d'un profil de machine est obligatoire et seuls les profils correspondant au même type de cryptage de sécurité que celui de l'image principale sélectionnée sont disponibles.
- Sur la page **Machines virtuelles**, seules les tailles de machine compatibles avec les machines virtuelles confidentielles s'affichent pour la sélection.
- Sur la page **Paramètres de disque**, vous ne pouvez pas spécifier le jeu de cryptage de disque, car il est hérité du profil de machine sélectionné.

### Azure Marketplace

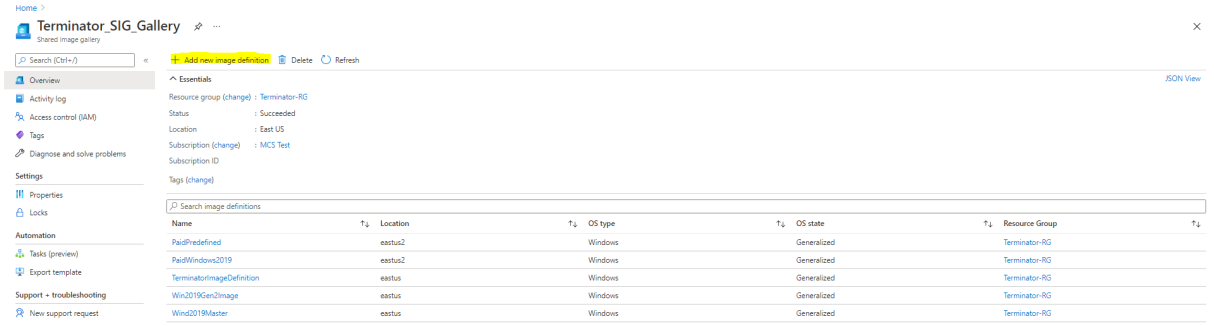
Citrix Virtual Apps and Desktops prend en charge l'utilisation d'une image principale sur Azure qui contient des informations de plan pour créer un catalogue de machines. Pour plus d'informations, consultez Microsoft Azure Marketplace.

> **Conseil :**
>
> Certaines images disponibles sur Azure Marketplace, telles que l'image Windows Server standard, n'ajoutent pas d'informations de plan. La fonctionnalité Citrix Virtual Apps and Desktops est destinée aux images payantes.

#### S'assurer que l'image créée dans Shared Image Gallery contient des informations de plan Azure

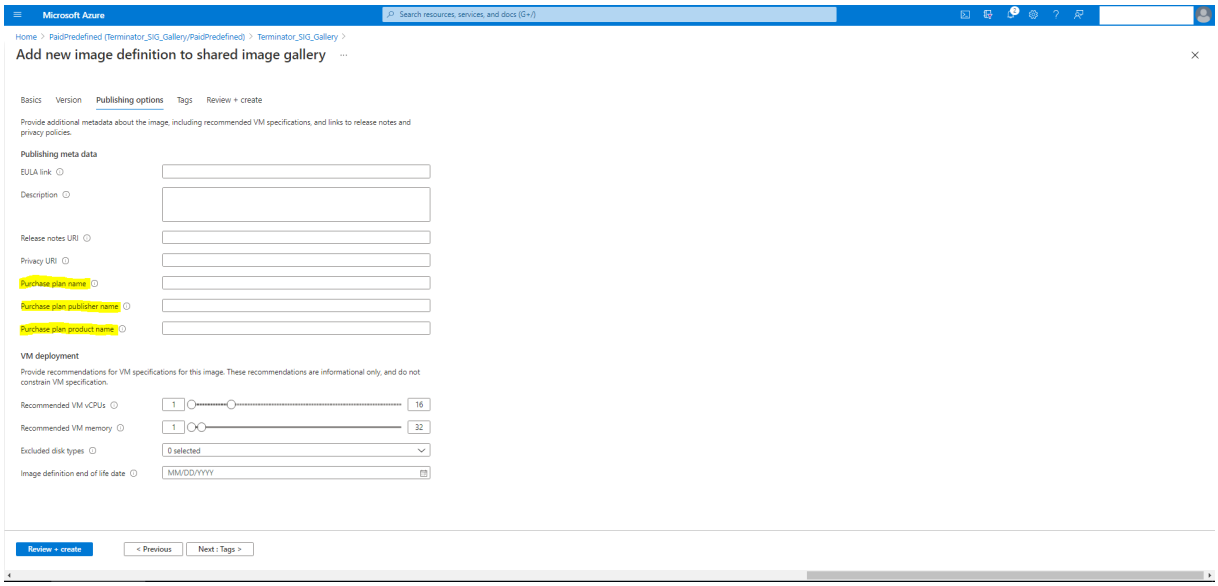
Suivez la procédure décrite dans cette section pour afficher les images de Shared Image Gallery dans Web Studio. Ces images peuvent éventuellement être utilisées pour une image principale. Pour placer l'image dans Shared Image Gallery, créez une définition d'image dans une galerie.



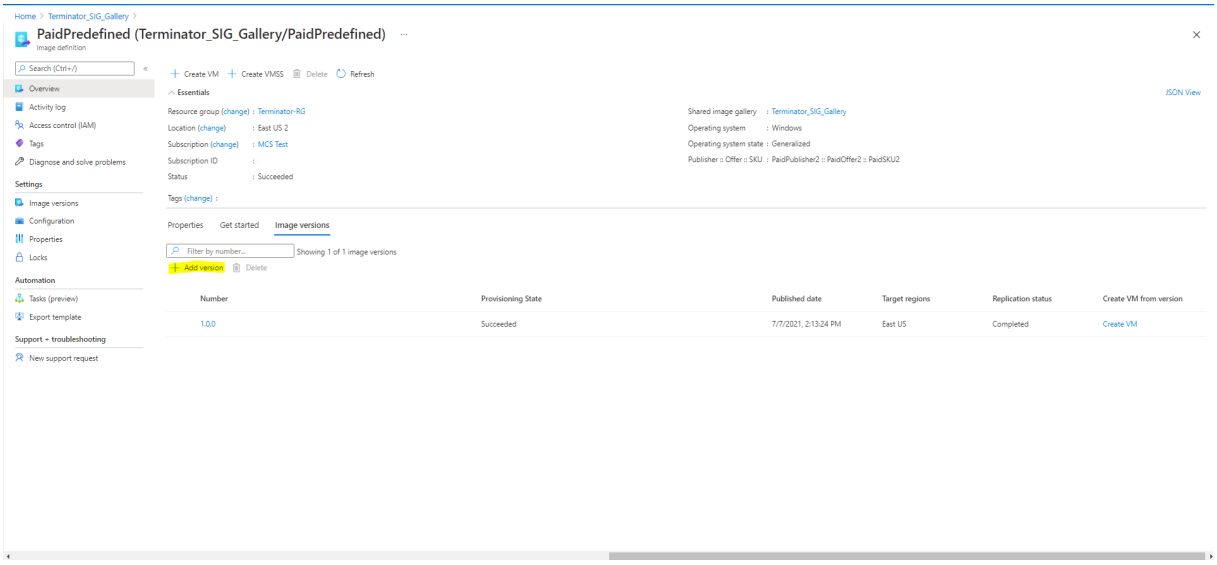

Sur la page **Options de publication**, vérifiez les informations du plan d'achat.

Les champs d'informations sur le plan d'achat sont initialement vides. Renseignez ces champs avec les informations de plan d'achat utilisées pour l'image. Ne pas renseigner les informations du plan d'achat peut entraîner l'échec du processus de catalogue de machines.

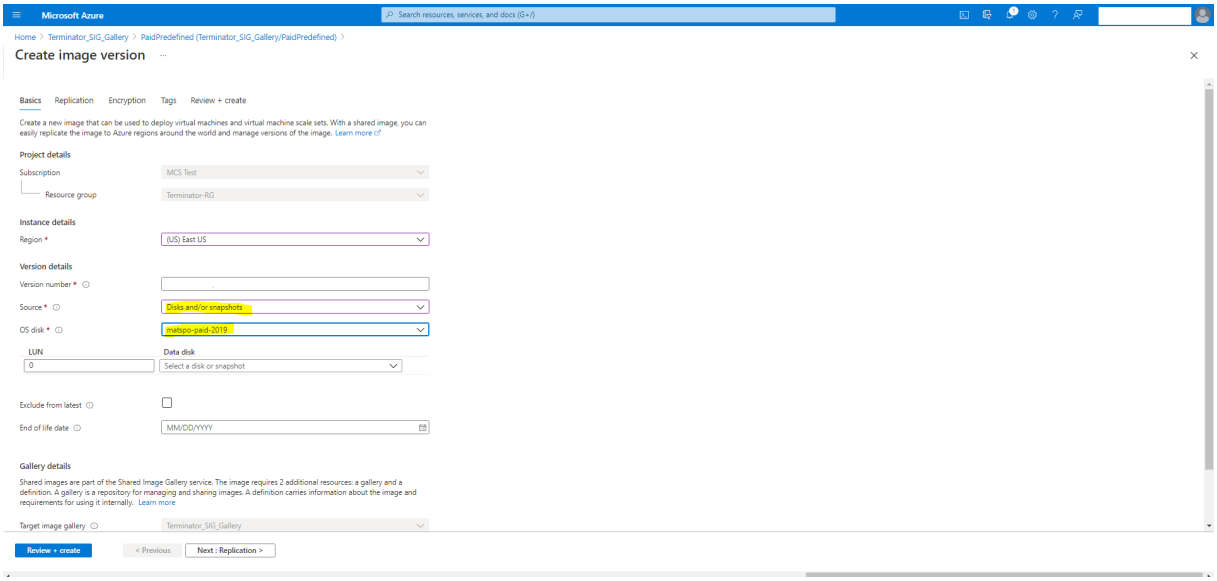



Après avoir vérifié les informations du plan d'achat, créez une version d'image dans la définition. Elle est utilisée comme image principale. Cliquez sur **Ajouter une version** :




Dans la section **Détails de la version**, sélectionnez l'instantané d'image ou le disque géré comme source :




## Créer un catalogue de machines à l'aide de PowerShell

Cette section explique comment créer des catalogues à l'aide de PowerShell :

- Créer un catalogue avec disque de cache en écriture non persistant
- Créer un catalogue avec disque de cache en écriture persistant
- Améliorer les performances de démarrage avec MCSIO
- Utiliser une spécification de modèle lors de la création ou de la mise à jour d'un catalogue à l'aide de PowerShell
- Catalogues de machines avec lancement fiable

- Utiliser les valeurs des propriétés du profil machine
- Créer un catalogue de machines avec une clé de chiffrement gérée par le client
- Créer un catalogue de machines avec cryptage double
- Créer un catalogue avec des disques éphémères Azure
- Hôtes dédiés Azure
- Créer ou mettre à jour un catalogue de machines à l'aide d'une image Azure Compute Gallery
- Configurer Azure Shared Image Gallery
- Provisionner des machines dans des zones de disponibilité spécifiées
- Types de stockage
- Emplacement du fichier d'échange
- Mettre à jour les paramètres du fichier d'échange
- Créer un catalogue à l'aide des machines virtuelles Azure Spot
- Configurer les tailles des machines virtuelles de sauvegarde
- Copier les balises sur toutes les ressources
- Provisionner des machines virtuelles de catalogue avec l'agent Azure Monitor installé

### Créer un catalogue avec disque de cache en écriture non persistant

Pour configurer un catalogue avec un disque de cache en écriture différée non persistant, utilisez le paramètre PowerShell `New-ProvScheme CustomProperties`. La propriété personnalisée `UseTempDiskForWBC` indique si vous acceptez d'utiliser le stockage temporaire Azure pour stocker le fichier de cache en écriture différée. Elle doit être configurée sur true lors de l'exécution de `New-ProvScheme` si vous souhaitez utiliser le disque temporaire comme disque de cache en écriture différée. Si cette propriété n'est pas spécifiée, le paramètre est défini sur **False** par défaut.

Exemple d'utilisation du paramètre `CustomProperties` pour définir la valeur `UseTempDiskForWBC` sur **true** :

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
   XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
   "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client"/> `
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="
   true"/> `
</CustomProperties>'
<!--NeedCopy-->
```

> **Remarque :**
>
> Une fois que vous avez validé le catalogue de machines pour utiliser le stockage temporaire local Azure pour le fichier de cache en écriture différée, il ne peut pas être modifié pour utiliser le disque dur virtuel ultérieurement.

### Créer un catalogue avec disque de cache en écriture persistant

Pour configurer un catalogue avec un disque de cache en écriture différée persistant, utilisez le paramètre PowerShell `New-ProvScheme CustomProperties`. Ce paramètre prend en charge une propriété supplémentaire, `PersistWBC`, utilisée pour déterminer la façon dont le disque de cache en réécriture persiste pour les machines provisionnées avec MCS. La propriété `PersistWBC` n'est utilisée que lorsque le paramètre `UseWriteBackCache` est spécifié et lorsque le paramètre `WriteBackCacheDiskSize` est défini pour indiquer qu'un disque est créé.

Voici des exemples de propriétés du paramètre `CustomProperties` avant la prise en charge de `PersistWBC` :

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

Lorsque vous utilisez ces propriétés, notez qu'elles contiennent des valeurs par défaut si elles sont omises du paramètre `CustomProperties`. La propriété `PersistWBC` a deux valeurs possibles : **true** ou **false**.

Lorsque la propriété `PersistWBC` est définie sur **true**, le disque de cache en réécriture n'est pas supprimé lorsque l'administrateur Citrix Virtual Apps and Desktops arrête la machine à l'aide de Web Studio.

Lorsque la propriété `PersistWBC` est définie sur **false**, le disque de cache en réécriture est supprimé lorsque l'administrateur Citrix Virtual Apps and Desktops arrête la machine à l'aide de Web Studio.

> **Remarque :**
>
> Si la propriété `PersistWBC` est omise, la propriété est **false** par défaut et le cache de réécriture est supprimé lors de l'arrêt de la machine à l'aide de Web Studio.

Par exemple, utilisation du paramètre `CustomProperties` pour définir la valeur `PersistWBC` sur true :

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> **Important :**
>
> La propriété `PersistWBC` ne peut être définie qu'à l'aide de l'applet de commande PowerShell `New-ProvScheme`. La tentative de modification de `CustomProperties` pour un schéma de provisioning après la création n'a aucun impact sur le catalogue de machines et la persistance du disque de cache en réécriture lors de l'arrêt d'une machine.

Par exemple, définissez `New-ProvScheme`pour utiliser le cache en réécriture tout en définissant la propriété `PersistWBC` sur true :

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`" /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSIO-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualprivatecloud\adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
```

```
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

### Améliorer les performances de démarrage avec MCSIO

Vous pouvez améliorer les performances de démarrage des disques gérés par Azure et GCP lorsque MCSIO est activé. Utilisez la propriété personnalisée `PersistOSDisk` PowerShell dans la commande `New-ProvScheme` pour configurer cette fonctionnalité. Les options associées à `New-ProvScheme` incluent :

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="Resource <!--NeedCopy-->
``````<!--NeedCopy-->
<!--NeedCopy-->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>
<!--NeedCopy-->
```

Pour activer cette fonctionnalité, définissez la propriété personnalisée `PersistOSDisk` sur **`true`**. Par exemple :

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
```

```
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

### Utiliser une spécification de modèle lors de la création ou de la mise à jour d'un catalogue à l'aide de PowerShell

Vous pouvez créer ou mettre à jour un catalogue de machines MCS à l'aide d'une spécification de modèle comme entrée de profil de machine. Pour ce faire, vous pouvez utiliser les commandes Web Studio ou PowerShell.

Pour Web Studio, voir Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans Web Studio.

Utilisation des commandes PowerShell :

1. Ouvrez la fenêtre **PowerShell**.
2. Exécutez `asnp citrix*`.
3. Créez ou mettez à jour un catalogue.

   - Pour créer un catalogue :

     a) Utilisez la commande `New-ProvScheme` avec une spécification de modèle comme entrée de profil de machine. Par exemple :

     ```
     New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
         image.folder/fgthj.resourcegroup/nab-ws-
         vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
         folder/fgthj.resourcegroup/test.templatespec/V1.
         templatespecversion"
     -ProvisioningSchemeName <String>
     -HostingUnitName <String>
     -IdentityPoolName <String>
     [-ServiceOffering <String>][-CustomProperties <String>
     [-LoggingId <Guid>]
     [-BearerToken <String>][-AdminAddress <String>]
     [<CommonParameters>]
     <!--NeedCopy-->
     ```

     b) Terminez la création du catalogue.

   - Pour mettre à jour un catalogue, utilisez la commande `Set-ProvScheme` avec une spécification de modèle comme entrée de profil de machine. Par exemple :

     ```
     Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
         Us.region/vm.folder/MasterDisk.vm'
     ```

```
MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/testing.templatespec/V1.
    templatespecversion'
[-ProvisioningSchemeName] <String>
[-CustomProperties <String>][-ServiceOffering <String>] [-
    PassThru]
[-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <
    String>] [<CommonParameters>]
<!--NeedCopy-->
```

### Catalogues de machines avec lancement fiable

Pour créer un catalogue de machines avec le lancement fiable, utilisez :

- Un profil de machine avec lancement fiable
- Une taille de machine virtuelle qui prend en charge le lancement fiable
- Une version de machine virtuelle Windows qui prend en charge le lancement fiable. Actuellement, Windows 10, Windows 11, Windows Server 2016, 2019 et 2022 prennent en charge le lancement fiable.

> **Important :**
>
> MCS prend en charge la création d'un catalogue avec des machines virtuelles compatibles avec le lancement fiable. Cependant, pour mettre à jour un catalogue persistant existant et des machines virtuelles existantes, vous devez utiliser le portail Azure. Vous ne pouvez pas mettre à jour le lancement fiable d'un catalogue non persistant. Pour plus d'informations, consultez le document Microsoft Activez le lancement fiable sur une machine virtuelle existante.

Pour afficher les éléments d'inventaire Citrix Virtual Apps and Desktops et pour déterminer si la taille de machine virtuelle prend en charge le lancement fiable, exécutez la commande suivante :

1. Ouvrez une fenêtre PowerShell.
2. Exécutez **asnp citrix*** pour charger des modules PowerShell spécifiques à Citrix.
3. Exécutez la commande suivante :

```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
    .folder"<VM size>.serviceoffering)
<!--NeedCopy-->
```

4. Exécutez `$s | select -ExpandProperty Additionaldata`.
5. Vérifiez la valeur de l'attribut `SupportsTrustedLaunch`.
   - Si la valeur de `SupportsTrustedLaunch` est **True**, la taille de machine virtuelle prend en charge le lancement fiable.

- Si la valeur de `SupportsTrustedLaunch` est **False**, la taille de machine virtuelle ne prend pas en charge le lancement fiable.

Avec Azure PowerShell, vous pouvez utiliser la commande suivante pour déterminer les tailles de machine virtuelle qui prennent en charge le lancement fiable :

```
(Get-AzComputeResourceSku | where {
 $_.Locations.Contains($region) -and ($_.Name -eq "<VM size>")  }
 )[0].Capabilities
<!--NeedCopy-->
```

Vous trouverez ci-dessous des exemples qui indiquent si la taille de machine virtuelle prend en charge le lancement fiable après avoir exécuté la commande Azure PowerShell.

- *Exemple 1* : si la machine virtuelle Azure prend uniquement en charge la génération 1, elle ne prend pas en charge le lancement fiable. Par conséquent, la fonctionnalité `TrustedLaunchDisabled` n'est pas affichée après l'exécution de la commande Azure PowerShell.
- *Exemple 2* : si la machine virtuelle Azure prend uniquement en charge la génération 2 et que la fonctionnalité `TrustedLaunchDisabled` est **True**, la taille de machine virtuelle de génération 2 ne prend pas en charge le lancement fiable.
- *Exemple 3* : si la machine virtuelle Azure prend uniquement en charge la génération 2 et que la fonctionnalité `TrustedLaunchDisabled` n'est pas affichée après l'exécution de la commande PowerShell, la taille de machine virtuelle de génération 2 prend en charge le lancement fiable.

Pour plus d'informations sur le lancement fiable pour les machines virtuelles Azure, consultez le document Microsoft Lancement fiable pour les machines virtuelles Azure.

#### Créer un catalogue de machines avec lancement fiable

1. Créez une image principale compatible avec le lancement fiable. Consultez la documentation Microsoft Images de machine virtuelle de lancement fiable.
2. Créez une machine virtuelle ou une spécification de modèle avec le type de sécurité **machines virtuelles de lancement fiable**. Pour plus d'informations sur la création d'une machine virtuelle ou d'une spécification de modèle, consultez le document Microsoft Déployer une machine virtuelle de lancement fiable.
3. Créez un catalogue de machines à l'aide de Web Studio ou des commandes PowerShell.
    - Si vous souhaitez utiliser Web Studio, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans Web Studio.

- Si vous souhaitez utiliser des commandes PowerShell, utilisez la commande New-ProvScheme avec la machine virtuelle ou la spécification de modèle comme entrée de profil de machine. Pour obtenir la liste complète des commandes permettant de créer un catalogue, consultez la section Création d'un catalogue.

  Exemple de commande New-ProvScheme avec une machine virtuelle comme entrée de profil de machine :

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.
    folder<def.resourcegroup><machine profile vm.vm>"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
<!--NeedCopy-->
```

  Exemple de commande New-ProvScheme avec une spécification de modèle comme entrée de profil de machine :

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
    resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/test.templatespec/V1.
    templatespecversion"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
<!--NeedCopy-->
```

#### Erreurs lors de la création de catalogues de machines avec le lancement fiable

Vous obtenez les erreurs appropriées dans les scénarios suivants lors de la création d'un catalogue de machines avec le lancement fiable :

| Scénario | Erreur |
| --- | --- |
| Si vous sélectionnez un profil de machine lors de la création d'un catalogue non géré | MachineProfileNotSupportedForUnmanagedCata |

| Scénario | Erreur |
| --- | --- |
| Si vous sélectionnez un profil de machine prenant en charge le lancement fiable lors de la création d'un catalogue avec un disque non géré comme image principale | `SecurityTypeNotSupportedForUnmanagedDisk` |
| Si vous ne sélectionnez pas de profil de machine lors de la création d'un catalogue géré avec une source d'image principale avec le lancement fiable comme type de sécurité | `MachineProfileNotFoundForTrustedLaunchMaste` |
| Si vous sélectionnez un profil de machine avec un type de sécurité différent du type de sécurité de l'image principale | `SecurityTypeConflictBetweenMasterImageAndMa` |
| Si vous sélectionnez une taille de machine virtuelle qui ne prend pas en charge le lancement fiable mais que vous utilisez une image principale qui prend en charge le lancement fiable lors de la création d'un catalogue | `MachineSizeNotSupportTrustedLaunch` |

### Utiliser les valeurs des propriétés du profil machine

Le catalogue de machines utilise les propriétés suivantes qui sont définies dans les propriétés personnalisées :

- Zone de disponibilité
- ID de groupe d'hôtes dédié
- ID de jeu de chiffrement de disque
- Type d'OS
- Type de licence
- Type de stockage

Si ces propriétés personnalisées ne sont pas définies explicitement, les valeurs de propriété sont définies à partir de la spécification du modèle ARM ou de la machine virtuelle, selon celle qui est utilisée comme profil de machine. De plus, si `ServiceOffering` n'est pas spécifié, il est défini à partir du profil de la machine.

> **Remarque :**
>
> Si certaines propriétés sont absentes du profil de la machine et ne sont pas définies dans les pro-

> priétés personnalisées, les valeurs par défaut de ces propriétés sont appliquées le cas échéant.

La section suivante décrit certains scénarios `New-ProvScheme` et `Set-ProvScheme` lorsque toutes les propriétés sont définies pour `CustomProperties` ou que les valeurs sont dérivées de MachineProfile.

- Scénarios New-ProvScheme
  - MachineProfile a toutes les propriétés et les propriétés CustomProperties ne sont pas définies. Exemple :

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    ```
    1  Get-ProvScheme | select CustomProperties
    2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
           machinecreation" xmlns:xsi="http://www.w3.org/2001/
           XMLSchema-instance">
    3  <Property xsi:type="StringProperty" Name="StorageAccountType"
            Value="<mpA-value>"/>
    4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
           -value>"/>
    5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
           "<mpA-value>"/>
    6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
           " Value="<mpA-value>"/>
    7  <Property xsi:type="StringProperty" Name="
           DedicatedHostGroupId" Value="<mpA-value>"/>
    8  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
           value>"/>
    9  </CustomProperties>
    10 <!--NeedCopy-->
    ```

  - MachineProfile a certaines propriétés et les propriétés CustomProperties ne sont pas définies. Exemple : MachineProfile a uniquement LicenseType et OSType.

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    ```
    1  Get-ProvScheme | select CustomProperties
    2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
           machinecreation" xmlns:xsi="http://www.w3.org/2001/
           XMLSchema-instance">
    3  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
           -value>"/>
    ```

```
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<mpA-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- MachineProfile et CustomProperties définissent toutes les propriétés. Exemple :

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
 $CustomPropertiesA
```

Les propriétés personnalisées sont prioritaires. Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
    CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId
    " Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="
    DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<
    CustomPropertiesA-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Certaines propriétés sont définies dans MachineProfile et certaines sont définies dans CustomProperties. Exemple :
  - CustomProperties définit LicenseType et StorageAccountType
  - MachineProfile définit LicenseType, OSType et Zones

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
 $CustomPropertiesA
```

Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
     Value="<CustomPropertiesA-value>"/>
```

```
4   <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
       -value>"/>
5   <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<CustomPropertiesA-value>"/>
6   <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
       value>"/>
7   </CustomProperties>
8   <!--NeedCopy-->
```

- Certaines propriétés sont définies dans MachineProfile et certaines sont définies dans CustomProperties. ServiceOffering n'est pas défini. Exemple :
  - CustomProperties définit StorageType
  - MachineProfile définit LicenseType

```
1   New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
       \machineprofile.folder\azure.resourcegroup\mp.vm"
2   -ServiceOffering "XDHyp:\HostingUnits\azureunit\
       serviceoffering.folder<explicit-machine-size>.
       serviceoffering"
3   <!--NeedCopy-->
```

Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

```
1   Get-ProvScheme | select ServiceOffering
2   serviceoffering.folder<explicit-machine-size>.serviceoffering
3
4   Get-ProvScheme | select CustomProperties
5   <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
6   <Property xsi:type="StringProperty" Name="StorageAccountType"
        Value="explicit-storage-type"/>
7   <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "value-from-machineprofile"/>
8   </CustomProperties>
9   <!--NeedCopy-->
```

- Si OSType ne figure ni dans CustomProperties ni dans MachineProfile, alors :
  - La valeur est lue à partir de l'image principale.
  - Si l'image principale est un disque non géré, OSType est défini sur Windows. Exemple :

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
 "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

La valeur de l'image principale est écrite dans les propriétés personnalisées, dans ce cas Linux.

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance">
<Property xsi:type="StringProperty" Name="OSType" Value="
    Linux"/>
</CustomProperties>
<!--NeedCopy-->
```

- Scénarios Set-ProvScheme
  - Un catalogue existant avec :
    - CustomProperties pour `StorageAccountType` et OSType
    - MachineProfile `mpA.vm` qui définit les zones
  - Mises à jour :
    - MachineProfile mpB.machine virtuelle qui définit StorageAccountType
    - Un nouveau jeu de propriétés personnalisées $CustomPropertiesB qui définit License-Type et OSType

    ```
    Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
     $CustomPropertiesB
    ```

    Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    ```
    Get-ProvScheme | select CustomProperties
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation" xmlns:xsi="http://www.w3.org/2001/
        XMLSchema-instance">
    <Property xsi:type="StringProperty" Name="StorageAccountType"
         Value="<mpB-value>"/>
    <Property xsi:type="StringProperty" Name="OSType" Value="<
        CustomPropertiesB-value>"/>
    <Property xsi:type="StringProperty" Name="LicenseType" Value=
        "<CustomPropertiesB-value>"/>
         </CustomProperties>
    <!--NeedCopy-->
    ```

  - Un catalogue existant avec :
    - CustomProperties pour `StorageAccountType` et OSType
    - MachineProfile `mpA.vm` qui définit StorageAccountType et LicenseType
  - Mises à jour :
    - Un nouveau jeu de propriétés personnalisées $CustomPropertiesB qui définit StorageAccountType et OSType

```
Set-ProvScheme -CustomProperties $CustomPropertiesB
```

Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   CustomPropertiesB-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<mp-A-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Un catalogue existant avec :
  - CustomProperties pour `StorageAccountType` et OSType
  - MachineProfile `mpA.vm` qui définit les zones
- Mises à jour :
  - MachineProfile mpB.machine virtuelle qui définit StorageAccountType et LicenseType
  - `ServiceOffering` n'est pas spécifié

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"
```

Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<value-from-machineprofile>.
   serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   prior-CustomProperties-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<mpB-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

### Provisionner des machines virtuelles de catalogue avec l'agent Azure Monitor installé

Le service de surveillance Azure vous permet de collecter, d'analyser et d'exploiter des données de télémétrie provenant de vos environnements Azure et locaux.

L'agent Azure Monitor Agent (AMA) collecte les données de surveillance à partir de ressources de calcul telles que des machines virtuelles et les transmet à Azure Monitor. Il prend actuellement en charge la collecte des journaux d'événements, du syslog et des métriques de performance et les envoie aux sources de données Azure Monitor Metrics et Azure Monitor Logs.

Pour surveiller en identifiant de manière unique les machines virtuelles dans les données de surveillance, vous pouvez provisionner les machines virtuelles d'un catalogue de machines MCS avec l'agent AMA installé en tant qu'extension.

#### Exigences

- Autorisations : assurez-vous de disposer des autorisations Azure minimales spécifiées dans la section Autorisations Azure requises et des autorisations suivantes pour utiliser Azure Monitor :
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- Règle de collecte de données : configurez une règle de collecte de données dans le portail Azure. Pour plus d'informations sur la configuration d'une règle de collecte de données, consultez la section Créer une règle de collecte de données. Une règle de collecte de données est spécifique à une plate-forme (Windows ou Linux). Assurez-vous de créer une règle pour la plate-forme requise.
  L'agent AMA utilise des règles de collecte de données (DCR) pour gérer le mappage entre les ressources, telles que les machines virtuelles, et les sources de données, telles qu'Azure Monitor Metrics et Azure Monitor Logs.
- Espace de travail par défaut : créez un espace de travail dans le portail Azure. Pour plus d'informations sur la création d'un espace de travail, voir Créer un espace de travail Log Analytics. Lorsque vous collectez des journaux et des données, les informations sont stockées dans un espace de travail. Un espace de travail possède un identifiant d'espace de travail et un identifiant de ressource uniques. Le nom de l'espace de travail doit être unique pour un groupe de ressources donné. Après avoir créé un espace de travail, configurez les sources de données et les solutions pour stocker leurs données dans l'espace de travail.

- Extension Monitor ajoutée à la liste blanche : les extensions `AzureMonitorWindowsAgent` et `AzureMonitorLinuxAgent` sont des extensions sur liste blanche définies par Citrix. Pour afficher la liste des extensions figurant sur la liste blanche, utilisez la commande PoSH, `Get-ProvMetadataConfiguration`.
- Image principale : Microsoft recommande de supprimer les extensions d'une machine existante avant d'en créer une nouvelle à partir de celle-ci. Si les extensions ne sont pas supprimées, des fichiers peuvent rester et un comportement inattendu peut se produire. Pour plus d'informations, consultez Si la machine virtuelle est recréée à partir d'une machine virtuelle existante.

Pour provisionner des machines virtuelles de catalogue avec l'agent AMA activé :

1. Configurez un modèle de profil de machine.
   - Si vous souhaitez utiliser une machine virtuelle comme modèle de profil de machine :
     a) Créez une machine virtuelle dans le portail Azure.
     b) Allumez la machine virtuelle.
     c) Ajoutez la machine virtuelle à la règle de collecte de données sous **Ressources**. Cela appelle l'installation de l'agent sur la machine virtuelle modèle.

     > **Remarque :**
     >
     > Si vous devez créer un catalogue Linux, configurez une machine Linux.

   - Si vous souhaitez utiliser une spécification de modèle comme modèle de profil de machine :
     a) Configurez une spécification de modèle.
     b) Ajoutez l'association d'extension et de règle de collecte de données suivantes à la spécification de modèle générée :

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {

    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
 }
```

```
18
19  }
20  ,
21  {
22
23     "type": "Microsoft.Insights/
          dataCollectionRuleAssociations",
24     "apiVersion": "2021-11-01",
25     "name": "<associatio-name>",
26     "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
27     "dependsOn": [
28      "Microsoft.Compute/virtualMachines/<vm-name>",
29     "Microsoft.Compute/virtualMachines/<vm-name>/extensions
          /AzureMonitorWindowsAgent"
30     ],
31     "properties": {
32
33        "description": "Association of data collection rule.
              Deleting this association will break the data
             collection for this Arc server.",
34      "dataCollectionRuleId": "/subscriptions/<azure-
           subscription>/resourcegroups/<azure-resource-group
           >/providers/microsoft.insights/datacollectionrules
           /<azure-data-collection-rule>"
35       }
36
37      }
38
39 <!--NeedCopy-->
```

2. Créez ou mettez à jour un catalogue de machines MCS existant.

   - Pour créer un nouveau catalogue MCS :

     a) Sélectionnez cette machine virtuelle ou une spécification de modèle en tant que profil de machine dans Web Studio.
     b) Procédez aux étapes suivantes pour créer le catalogue.

   - Pour mettre à jour un catalogue MCS existant, utilisez les commandes PoSH suivantes :

     - Pour que les nouvelles machines virtuelles obtiennent le modèle de profil de machine mis à jour, exécutez la commande suivante :

       ```
       1  Set-ProvScheme -ProvisioningSchemeName "name"
       2  -MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
             folder\abc.resourcegroup\ab-machine-profile.vm"
       3  <!--NeedCopy-->
       ```

     - Pour mettre à jour les machines virtuelles existantes avec le modèle de profil de machine mis à jour :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-
    catalog -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

3. Allumez les machines virtuelles du catalogue.
4. Accédez au portail Azure et vérifiez si l'extension Monitor est installée sur la machine virtuelle et si la machine virtuelle apparaît sous les ressources de DCR. Après quelques minutes, les données de surveillance s'affichent sur Azure Monitor.

#### Dépannage

Pour des conseils de dépannage pour Azure Monitor Agent, consultez :

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

### Créer un catalogue de machines avec une clé de chiffrement gérée par le client

Les étapes détaillées pour créer un catalogue de machines avec une clé de chiffrement gérée par le client sont les suivantes :

1. Ouvrez une fenêtre PowerShell.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Entrez `cd xdhyp:/.`
4. Entrez `cd .\HostingUnits\(your hosting unit).`
5. Entrez `cd diskencryptionset.folder.`
6. Entrez `dir` pour obtenir la liste des jeux de chiffrement de disque.
7. Copiez l'ID d'un jeu de chiffrement de disque.
8. Créez une chaîne de propriétés personnalisée pour inclure l'ID du jeu de chiffrement de disque. Par exemple :

```
$customProperties = "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.
    org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
    Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"persistWBC`" Value=`"
    False`" />
```

```
<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value
   =`"false`" />
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
   Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
    Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/
   resourceGroups/abc/providers/Microsoft.Compute/
   diskEncryptionSets/abc-des`"/>
</CustomProperties>
<!--NeedCopy-->
```

9. Créez un pool d'identités s'il n'a pas déjà été créé. Par exemple :

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
   Domain def.local -NamingSchemeType Numeric
<!--NeedCopy-->
```

10. Exécutez la commande New-ProvScheme. Par exemple :

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
   IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
   resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
    def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
    " }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
   folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.folder<
   def.resourcegroup><machine profile vm.vm>"
-CustomProperties $customProperties
<!--NeedCopy-->
```

11. Terminez la création du catalogue de machines.

### Créer un catalogue de machines avec cryptage double

Vous pouvez créer et mettre à jour un catalogue de machines utilisant un chiffrement double à l'aide de Web Studio et de commandes PowerShell.

Les étapes détaillées pour créer un catalogue de machines avec chiffrement double sont les suivantes :

1. Créez une instance Azure Key Vault et un jeu de chiffrement de disque avec des clés gérées par la plate-forme et gérées par le client. Pour plus d'informations sur la création d'une instance Azure Key Vault et d'un jeu de chiffrement de disque (DES), consultez la section Utiliser le portail Azure pour activer le chiffrement double au repos pour les disques gérés.

2. Pour parcourir les jeux de chiffrement de disque disponibles dans votre connexion d'hébergement, procédez comme suit :

   a) Ouvrez une fenêtre **PowerShell**.
   b) Exécutez les commandes PowerShell suivantes :

      i. `asnp citrix*`
      ii. `cd xdhyp:`
      iii. `cd HostingUnits`
      iv. `cd YourHostingUnitName` (par exemple, azure-east)
      v. `cd diskencryptionset.folder`
      vi. `dir`

   Vous pouvez utiliser un identifiant de `DiskEncryptionSet` pour créer ou mettre à jour un catalogue à l'aide de propriétés personnalisées.

3. Si vous souhaitez utiliser le workflow du profil de machine, créez une machine virtuelle ou une spécification de modèle en tant qu'entrée de profil de machine.

   - Si vous souhaitez utiliser une machine virtuelle comme entrée de profil de machine :
     a) Créez une machine virtuelle dans le portail Azure.
     b) Accédez à **Disques > Gestion des clés** pour chiffrer la machine virtuelle directement avec n'importe quel `DiskEncryptionSetID`.
   - Si vous souhaitez utiliser une spécification de modèle comme entrée de profil de machine :
     a) Dans le modèle, sous `properties>storageProfile>osDisk>managedDisk`, ajoutez un paramètre `diskEncryptionSet` et ajoutez l'identifiant du jeu de chiffrement de disque utilisant le chiffrement double.

4. Créez le catalogue de machines.

   - Si vous utilisez Web Studio, effectuez l'une des opérations suivantes en plus des étapes décrites dans la section Créer des catalogues de machines.
     - Si vous n'utilisez pas de workflow basé sur le profil de la machine, sur la page **Paramètres du disque**, sélectionnez **Utilisez la clé suivante pour chiffrer les données sur chaque machine**. Sélectionnez ensuite le chiffrement de disque utilisant le chiffrement double dans la liste déroulante. Continuez à créer le catalogue.
     - Si vous utilisez le workflow basé sur le profil de la machine, sur la page **Image**, sélectionnez une image principale et un profil de machine. Assurez-vous que le profil de la machine est associé à un identifiant de jeu de chiffrement de disque dans ses propriétés.

     Le chiffrement double est appliqué à toutes les machines créées dans le catalogue via la clé associée au jeu de chiffrement de disque que vous avez sélectionné.

- Si vous utilisez les commandes PowerShell, effectuez l'une des opérations suivantes :
  - Si vous n'utilisez pas de workflow basé sur le profil de la machine, ajoutez la propriété personnalisée `DiskEncryptionSetId` dans la commande `New-ProvScheme`. Par exemple :

```
New-ProvScheme -CleanOnBoot -CustomProperties '<
   CustomProperties xmlns="http://schemas.citrix.com/2014/
   xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks"
    Value="true" />
<Property xsi:type="StringProperty" Name="
   StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="
   DiskEncryptionSetId" Value="/subscriptions/12345678-
   xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
   providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
</CustomProperties>'
-HostingUnitName "Redacted"
-IdentityPoolName "Redacted"
-InitialBatchSizeHint 1
-MasterImageVM "Redacted"
-NetworkMapping @{
"0"="Redacted" }

-ProvisioningSchemeName "Redacted"
-ServiceOffering "Redacted"
<!--NeedCopy-->
```

  - Si vous utilisez un workflow basé sur le profil de la machine, utilisez une entrée de profil de machine dans la commande `New-ProvScheme`. Par exemple :

```
New-ProvScheme -CleanOnBoot
-HostingUnitName azure-east
-IdentityPoolName aio-ip
-InitialBatchSizeHint 1
-MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
   \abc.resourcegroup\fgb-vda-snapshot.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
   folder\apa-resourceGroup.resourcegroup\apa-
   resourceGroup-vnet.virtualprivatecloud\default.network"
    }

-ProvisioningSchemeName aio-test
-MachineProfile XDHyp:\HostingUnits\azure-east\
   machineprofile.folder\abc.resourcegroup\abx-mp.
   templatespec\1.0.0.templatespecversion
<!--NeedCopy-->
```

5. Terminez la création du catalogue à l'aide de Remote PowerShell SDK. Pour plus d'informations sur la création d'un catalogue à l'aide du SDK Remote PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Le chiffrement double est appliqué à toutes les machines créées dans le catalogue via la clé associée au jeu de chiffrement de disque que vous avez sélectionné.

#### Convertir un catalogue non crypté en catalogue avec cryptage double

Vous pouvez mettre à jour le type de chiffrement d'un catalogue de machines (à l'aide de propriétés personnalisées ou d'un profil de machine) uniquement si le catalogue a déjà été déchiffré.

- Si vous n'utilisez pas de workflow basé sur le profil de la machine, ajoutez la propriété personnalisée DiskEncryptionSetId dans la commande `Set-ProvScheme`. Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix
   .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
   /2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
   Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
   resourceGroups/Sample-RG/providers/Microsoft.Compute/
   diskEncryptionSets/SampleEncryptionSet" />
</CustomProperties>'
<!--NeedCopy-->
```

- Si vous utilisez un workflow basé sur le profil de la machine, utilisez une entrée de profil de machine dans la commande `Set-ProvScheme`. Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
    XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
   resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
<!--NeedCopy-->
```

Si l'opération réussit, le chiffrement double est appliqué à toutes les nouvelles machines virtuelles que vous ajoutez à votre catalogue via la clé associée au jeu de chiffrement de disque que vous avez sélectionné.

#### Vérifier que le cryptage double est appliqué au catalogue

- Dans Web Studio :
  1. Accédez à **Catalogues de machines**.
  2. Sélectionnez le catalogue que vous souhaitez vérifier. Cliquez sur l'onglet **Propriétés du modèle** situé en bas de l'écran.

3. Dans **Détails Azure**, vérifiez l'ID du jeu de chiffrement de disque dans **Jeu de chiffrement de disque**. Si l'ID du jeu de chiffrement de disque associé au catalogue est vide, le catalogue n'est pas chiffré.
4. Dans le portail Azure, vérifiez que le type de cryptage du jeu de cryptage de disque associé à l'ID DES est une clé gérée par la plate-forme et une clé gérée par le client.

- À l'aide de la commande PowerShell :

1. Ouvrez la fenêtre **PowerShell**.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Utilisez `Get-ProvScheme` pour obtenir les informations de votre catalogue de machines. Par exemple :

```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
<!--NeedCopy-->
```

4. Récupérez la propriété personnalisée de l'ID du jeu de chiffrement de disque associé au catalogue de machines. Par exemple :

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions
   /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
   -RG/providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
<!--NeedCopy-->
```

5. Dans le portail Azure, vérifiez que le type de cryptage du jeu de cryptage de disque associé à l'ID DES est une clé gérée par la plate-forme et une clé gérée par le client.

### Créer un catalogue avec des disques éphémères Azure

Pour utiliser des disques éphémères, vous devez définir la propriété personnalisée `UseEphemeralOsDisk` sur **true** lors de l'exécution de `New-ProvScheme`.

> **Remarque :**
>
> Si la propriété personnalisée `UseEphemeralOsDisk` est définie sur **false** ou si une valeur n'est pas spécifiée, tous les VDA provisionnés continuent d'utiliser un disque d'OS provisionné.

Voici un exemple d'ensemble de propriétés personnalisées à utiliser dans le schéma de provisioning :

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
```

```
                    "Value": "true"
                }
    ,
                {

                    "Name": "StorageType",
                    "Value": "Standard_LRS"
                }
    ,
                {

                    "Name": "UseSharedImageGallery",
                    "Value": "true"
                }
    ,
                {

                    "Name": "SharedImageGalleryReplicaRatio",
                    "Value": "40"
                }
    ,
                {

                    "Name": "SharedImageGalleryReplicaMaximum",
                    "Value": "10"
                }
    ,
                {

                    "Name": "LicenseType",
                    "Value": "Windows_Server"
                }
    ,
                {

                    "Name": "UseEphemeralOsDisk",
                    "Value": "true"
                }

            ],
    <!--NeedCopy-->
```

**Configurer un disque éphémère pour un catalogue**

Pour configurer un disque d'OS éphémère Azure pour un catalogue, utilisez le paramètre `UseEphemeralOsDisk` dans `Set-ProvScheme`. Définissez la valeur du paramètre `UseEphemeralOsDisk` sur **true**.

> **Remarque :**
>
> Pour utiliser cette fonctionnalité, vous devez également activer les paramètres `UseManagedDisks` et `UseSharedImageGallery`.

Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties <
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
    "true" />
<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
    true" />
</CustomProperties>'
<!--NeedCopy-->
```

#### Remarques importantes sur les disques éphémères

Pour provisionner des disques d'OS éphémères en utilisant `New-ProvScheme`, tenez compte des contraintes suivantes :

- La taille de machine virtuelle utilisée pour le catalogue doit prendre en charge les disques d'OS éphémères.
- La taille du cache ou du disque temporaire associé à la taille de la machine virtuelle doit être supérieure ou égale à la taille du disque d'OS.
- La taille du disque temporaire doit être supérieure à la taille du disque de cache.

Tenez également compte de ces points lors des opérations suivantes :

- Création du schéma de provisioning.
- Modification du schéma de provisioning.
- Mise à jour de l'image.

### Hôtes dédiés Azure

Vous pouvez utiliser MCS pour provisionner des machines virtuelles sur des hôtes dédiés Azure. Avant de provisionner des machines virtuelles sur des hôtes dédiés Azure :

- Créez un groupe d'hôtes.
- Créez des hôtes dans ce groupe d'hôtes.

- Assurez-vous que la capacité des hôtes est suffisante pour la création de catalogues et de machines virtuelles.

Vous pouvez créer un catalogue de machines avec la location d'hôte définie à l'aide du script PowerShell suivant :

```
New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
   xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
   ="http://www.w3.org/2001/XMLSchema-instance">
 <Property xsi:type="StringProperty" Name="HostGroupId" Value="
    myResourceGroup/myHostGroup" />
 ...other Custom Properties...
 </CustomProperties>
<!--NeedCopy-->
```

Lorsque vous utilisez MCS pour provisionner des machines virtuelles sur des hôtes dédiés Azure, tenez compte des éléments suivants :

- Un *hôte dédié* est une propriété de catalogue et ne peut pas être modifié une fois le catalogue créé. La location dédiée n'est actuellement pas prise en charge sur Azure.
- Un groupe d'hôtes Azure préconfiguré, dans la région de l'unité d'hébergement, est requis lors de l'utilisation du paramètre `HostGroupId`.
- Le placement automatique Azure est requis. Cette fonctionnalité effectue une demande d'intégration à l'abonnement associé au groupe d'hôtes. Pour plus d'informations, consultez Échelle MV définie sur les hôtes dédiés Azure - Version préliminaire publique. Si le placement automatique n'est pas activé, MCS génère une erreur lors de la création du catalogue.

### Créer ou mettre à jour un catalogue de machines à l'aide d'une image Azure Compute Gallery

Lorsque vous sélectionnez une image à utiliser pour créer un catalogue de machines, vous pouvez sélectionner les images que vous avez créées dans Azure Compute Gallery.

Pour que ces images apparaissent, vous devez :

1. Configurer un site Citrix Virtual Apps and Desktops.
2. Connectez-vous à Azure Resource Manager.
3. Dans le portail Azure, créez un groupe de ressources. Pour plus d'informations, consultez Créer une instance Azure Compute Gallery à l'aide du portail.
4. Dans le groupe de ressources, créez une instance Azure Compute Gallery.
5. Dans Azure Compute Gallery, créez une définition d'image.
6. Dans la définition de l'image, créez une version d'image.

Utilisez les commandes PowerShell suivantes pour créer ou mettre à jour un catalogue de machines à l'aide d'une image provenant d'Azure Compute Gallery :

1. Ouvrez une fenêtre PowerShell.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Sélectionnez un groupe de ressources, puis répertoriez toutes les galeries de ce groupe de ressources.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup")
<!--NeedCopy-->
```

4. Sélectionnez une galerie, puis répertoriez toutes les définitions d'images de cette galerie.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery")
<!--NeedCopy-->
```

5. Sélectionnez une définition d'image, puis répertoriez toutes les versions d'image de cette définition d'image.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery\sigtestimage.
    imagedefinition")
<!--NeedCopy-->
```

6. Créez et mettez à jour un catalogue MCS à l'aide des éléments suivants :

   - Groupe de ressources
   - Galerie
   - Définition de l'image de la galerie
   - Version d'image de la galerie

   Pour plus d'informations sur la création d'un catalogue à l'aide du SDK Remote PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

### Configurer Azure Shared Image Gallery

Utilisez la commande `New-ProvScheme` pour créer un schéma de provisioning avec la prise en charge de Shared Image Gallery. Utilisez la commande `Set-ProvScheme` pour activer ou désactiver cette fonctionnalité pour un schéma de provisioning et pour modifier le ratio de réplica et les valeurs maximales de réplicas.

Trois propriétés personnalisées ont été ajoutées aux schémas de provisioning pour prendre en charge la fonctionnalité Shared Image Gallery :

`UseSharedImageGallery`

- Indique si vous souhaitez utiliser Shared Image Gallery pour stocker les images publiées. Si cette propriété est définie sur **True**, l'image est stockée en tant qu'image Shared Image Gallery, sinon l'image est stockée sous la forme d'un instantané.
- Les valeurs valides sont **True** et **False**.
- Si la propriété n'est pas définie, la valeur par défaut est **False**.

`SharedImageGalleryReplicaRatio`

- Définit le ratio entre les machines et les réplicas de version d'image de la galerie.
- Les valeurs valides sont des nombres entiers supérieurs à 0.
- Si la propriété n'est pas définie, les valeurs par défaut sont utilisées. La valeur par défaut pour les disques du système d'exploitation persistants est de 1 000 ; la valeur par défaut pour les disques du système d'exploitation non persistants est de 40.

`SharedImageGalleryReplicaMaximum`

- Définit le nombre maximal de réplicas pour chaque version d'image de la galerie.
- Les valeurs valides sont des nombres entiers supérieurs à 0.
- Si la propriété n'est pas définie, la valeur par défaut est 10.
- Azure prend actuellement en charge jusqu'à 10 réplicas pour une version unique d'image de la galerie. Si la propriété est définie sur une valeur supérieure à celle prise en charge par Azure, MCS tente d'utiliser la valeur spécifiée. Azure génère une erreur, que MCS consigne, puis laisse le nombre de réplicas actuel inchangé.

> **Conseil :**
>
> Lors de l'utilisation de Shared Image Gallery pour stocker une image publiée pour les catalogues provisionnés avec MCS, MCS définit le nombre de réplicas de version d'image de galerie en fonction du nombre de machines dans le catalogue, du ratio de réplica et du maximum de réplicas. Le nombre de réplicas est calculé en divisant le nombre de machines du catalogue par le ratio de réplica (arrondi à la valeur entière la plus proche), puis en plafonnant la valeur au nombre maximal de réplicas. Par exemple, avec un ratio de réplica de 20 et un maximum de 5, 0 à 20 machines ont un réplica, 21—40 ont 2 réplicas, 41—60 ont 3 réplicas, 61 à 80 ont 4 réplicas, 81+ 5 réplicas.

#### Cas d'utilisation : mise à jour du ratio de réplica Shared Image Gallery et du maximum de réplicas

Le catalogue de machines existant utilise Shared Image Gallery. Utilisez la commande `Set-ProvScheme` pour mettre à jour les propriétés personnalisées de toutes les machines existantes du catalogue et de toutes les futures machines :

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

**Cas d'utilisation : conversion d'un catalogue d'instantanés en catalogue Shared Image Gallery**

Pour ce cas d'utilisation :

1. Exécutez `Set-ProvScheme` avec l'indicateur `UseSharedImageGallery` défini sur **True**. Vous pouvez également inclure les propriétés `SharedImageGalleryReplicaRatio` et `SharedImageGalleryReplicaMaximum`.
2. Mettez le catalogue à jour.
3. Effectuez un cycle d'alimentation sur les machines pour forcer une mise à jour.

Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

> **Conseil :**
>
> Les paramètres `SharedImageGalleryReplicaRatio` et `SharedImageGalleryReplicaMaximum` ne sont pas obligatoires. Une fois la commande `Set-ProvScheme` terminée, l'image Shared Image Gallery n'a pas encore été créée. Une fois que le catalogue est configuré pour utiliser la galerie, l'opération suivante de mise à jour du catalogue stocke l'image publiée dans la galerie. La commande de mise à jour du catalogue crée la galerie, l'image de la galerie et la version de l'image. Le cycle d'alimentation des machines les met à jour, et le nombre de réplicas est mis à jour, le cas échéant. À partir de ce moment, toutes les machines non persistantes existantes sont réinitialisées à l'aide de l'image Shared Image Gallery et toutes les machines

> nouvellement provisionnées sont créées à l'aide de l'image. L'ancien instantané est nettoyé automatiquement en quelques heures.

#### Cas d'utilisation : conversion d'un catalogue Shared Image Gallery en catalogue d'instantanés

Pour ce cas d'utilisation :

1. Exécutez `Set-ProvScheme` avec l'indicateur `UseSharedImageGallery` défini sur **False** ou non défini.
2. Mettez le catalogue à jour.
3. Effectuez un cycle d'alimentation sur les machines pour forcer une mise à jour.

Par exemple :

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance"> <Property xsi:type="StringProperty" Name="StorageType"
     Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
     UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
     Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
2 <!--NeedCopy-->
```

> **Conseil :**
>
> Contrairement à la mise à jour d'un instantané vers un catalogue Shared Image Gallery, les données personnalisées de chaque machine ne sont pas encore mises à jour pour refléter les nouvelles propriétés personnalisées. Exécutez la commande suivante pour afficher les propriétés personnalisées Shared Image Gallery d'origine : `Get-ProvVm -ProvisioningSchemeName catalog-name`. Une fois la commande `Set-ProvScheme` terminée, l'instantané de l'image n'a pas encore été créé. Une fois que le catalogue est configuré pour ne pas utiliser la galerie, la prochaine opération de mise à jour du catalogue stocke l'image publiée sous forme d'instantané. À partir de ce moment, toutes les machines non persistantes existantes sont réinitialisées à l'aide de l'instantané et toutes les machines nouvellement provisionnées sont créées à partir de l'instantané. Le cycle d'alimentation des machines les met à jour, et les données de machine personnalisées sont mises à jour pour refléter que `UseSharedImageGallery` est défini sur **False**. Les anciennes ressources Shared Image Gallery (galerie, image et version) sont automatiquement nettoyées en quelques heures.

### Provisionner des machines dans des zones de disponibilité spécifiées

Vous pouvez provisionner des machines dans une zone de disponibilité spécifique dans les environnements Azure. Vous pouvez pour cela utiliser PowerShell.

> **Remarque :**
>
> Si aucune zone n'est spécifiée, MCS laisse Azure placer les machines dans la région. Si plusieurs zones sont spécifiées, MCS distribue les machines de manière aléatoire dans ces zones.

#### Configurer des zones de disponibilité via PowerShell

À l'aide de PowerShell, vous pouvez afficher les éléments d'inventaire de l'offre en utilisant `Get-Item`. Par exemple, pour consulter l'offre de services de la *région États-Unis de l'Est* `Standard_B1ls` :

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
    name\East US.region\serviceoffering.folder\Standard_B1ls.
    serviceoffering"
<!--NeedCopy-->
```

Pour afficher les zones, utilisez le paramètre `AdditionalData` de l'élément :

```
$serviceOffering.AdditionalData
```

Si les zones de disponibilité ne sont pas spécifiées, les machines sont provisionnées de la même façon.

Pour configurer les zones de disponibilité via PowerShell, utilisez la propriété personnalisée **Zones** disponible avec l'opération `New-ProvScheme`. La propriété **Zones** définit une liste de zones de disponibilité dans lesquelles provisionner les machines. Ces zones peuvent inclure une ou plusieurs zones de disponibilité. Par exemple, `<Property xsi:type="StringProperty"Name="Zones"Value="1, 3"/>` pour les zones 1 et 3.

Utilisez la commande `Set-ProvScheme` pour mettre à jour les zones d'un schéma de provisioning.

Si une zone non valide est fournie, le schéma de provisioning n'est pas mis à jour et un message d'erreur apparaît indiquant comment corriger la commande non valide.

> **Conseil :**
>
> Si vous spécifiez une propriété personnalisée non valide, le schéma de provisioning n'est pas mis à jour et un message d'erreur correspondant s'affiche.

### Types de stockage

Sélectionnez différents types de stockage pour les machines virtuelles dans des environnements Azure utilisant MCS. Pour les machines virtuelles cibles, MCS prend en charge :

- Disque d'OS : SSD premium, SSD ou HDD

- Disque de cache en écriture différée : SSD premium, SSD ou HDD

Lorsque vous utilisez ces types de stockage, tenez compte des points suivants :

- Assurez-vous que votre machine virtuelle prend en charge le type de stockage sélectionné.
- Si votre configuration utilise un disque éphémère Azure, vous ne voyez pas l'option pour le paramètre de disque de cache en écriture différée.

> **Conseil :**
>
> `StorageType` est configuré pour un type d'OS et un compte de stockage. `WBCDiskStorageType` est configuré pour le type de stockage Cache en écriture différée. Pour un catalogue normal, `StorageType` est requis. Si `WBCDiskStorageType` n'est pas configuré, `StorageType` est utilisé par défaut pour `WBCDiskStorageType`.

Si WBCDiskStorageType n'est pas configuré, StorageType est utilisé par défaut pour WBCDiskStorageType.

#### Configurer des types de stockage

Pour configurer les types de stockage pour machine virtuelle, utilisez le paramètre `StorageType` dans `New-ProvScheme`. Définissez la valeur du paramètre `StorageType` sur l'un des types de stockage pris en charge.

Voici un exemple du paramètre `CustomProperties` dans un schéma de provisioning :

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="LicenseType" Value="
     Windows_Client" />
5 </CustomProperties>'
6 <!--NeedCopy-->
```

#### Activer le stockage redondant interzone

Vous pouvez sélectionner le stockage redondant interzone (ZRS) lors de la création de catalogue. Il réplique de manière synchrone votre disque géré par Azure sur plusieurs zones de disponibilité, ce qui vous permet de récupérer d'une panne dans une zone en utilisant la redondance dans d'autres.

Vous pouvez spécifier **Premium_ZRS** et **StandardSSD_ZRS** dans les propriétés personnalisées du type de stockage. Le stockage ZRS peut être défini à l'aide de propriétés personnalisées existantes ou via le modèle **MachineProfile**. Le stockage ZRS est également compatible avec la commande `Set-ProvVMUpdateTimeWindow` et les paramètres `-StartsNow` et `-DurationInMinutes -1`. Vous pouvez changer une machine existante d'un stockage LRS vers un stockage ZRS.

**Limitations :**

- Pris en charge uniquement pour les disques gérés
- Compatible uniquement avec les disques SSD (SSD) haut de gamme et standard
- Non compatible avec `StorageTypeAtShutdown`
- Disponible uniquement dans certaines régions.
- Les performances d'Azure diminuent lors de la création de disques ZRS à grande échelle. Par conséquent, lors de la première mise sous tension, allumez les machines par lots plus petits (moins de 300 machines à la fois)

**Définir le stockage redondant interzone comme type de stockage sur disque** Vous pouvez sélectionner le stockage redondant interzone lors de la création initiale du catalogue, ou vous pouvez mettre à jour votre type de stockage dans un catalogue existant.

**Sélectionner le stockage redondant interzone à l'aide des commandes PowerShell** Lorsque vous créez un catalogue dans Azure à l'aide de la commande PowerShell `New-ProvScheme`, utilisez `Standard_ZRS` comme valeur dans `StorageAccountType`.
Par exemple :

```
1 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     StandardSSD_ZRS" />
2 <!--NeedCopy-->
```

Lorsque vous définissez cette valeur, elle est validée par une API dynamique qui détermine si elle peut être utilisée correctement. Les exceptions suivantes peuvent se produire si l'utilisation de ZRS n'est pas valide pour votre catalogue :

- **StorageTypeAtShutdownNotSupportedForZrsDisks** : la propriété personnalisée StorageTypeatShutdown ne peut pas être utilisée avec le stockage ZRS.
- **StorageAccountTypeNotSupportedInRegion** : cette exception se produit si vous essayez d'utiliser le stockage ZRS dans une région Azure qui ne prend pas en charge ZRS
- **ZrsRequiresManagedDisks** : vous ne pouvez utiliser le stockage redondant interzone qu'avec des disques gérés.

Vous pouvez définir le type de stockage de disque à l'aide des propriétés personnalisées suivantes :

- `StorageType`

- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Remarque :**
>
> Lors de la création du catalogue, le disque d'OS du profil de machine `StorageType` est utilisé si les propriétés personnalisées ne sont pas définies.

## Capturez les paramètres de diagnostic sur les machine virtuelle et les cartes d'interface réseau à partir d'un profil de machine

Vous pouvez capturer les paramètres de diagnostic des machine virtuelle et des cartes d'interface réseau à partir d'un profil de machine au moment de créer un catalogue de machines, de mettre à jour un catalogue de machines existant et de mettre à jour des machine virtuelle existantes.

Vous pouvez créer une spécification de machine virtuelle ou de modèle en tant que source de profil de machine.

### Étapes clés

1. Configurez les identifiants requis dans Azure. Vous devez fournir ces identifiants dans la spécification du modèle.
    - Compte de stockage
    - Espace de travail Log Analytics
    - Espace de noms Event Hub avec tarification standard
2. Créez une source de profil de machine.
3. Créez un nouveau catalogue de machines, mettez à jour un catalogue existant ou mettez à jour des machine virtuelle existantes.

### Configurer les identifiants requis dans Azure

Configurez l'une des options suivantes dans Azure :

- Compte de stockage
- Espace de travail Log Analytics
- Espace de noms Event Hub avec tarification standard

**Configurer un compte de stockage** Créez un compte de stockage standard dans Azure. Dans la spécification du modèle, indiquez `storageAccountId` comme ResourceID complet du compte de stockage.

Une fois que les machine virtuelle sont configurées pour enregistrer les données sur le compte de stockage, les données se trouvent sous le conteneur `insights-metrics-pt1m`.

**Configurer un espace de travail Log Analytics** Créez un espace de travail Log Analytics. Dans la spécification du modèle, indiquez le ResourceID complet de l'espace de travail Log Analytics tel que le WorkspaceID.

Une fois que les machine virtuelle sont configurées pour enregistrer les données dans l'espace de travail, les données peuvent être interrogées dans Logs in Azure. Vous pouvez exécuter la commande suivante dans Azure, sous Logs, pour afficher le décompte de toutes les mesures enregistrées par une ressource :

'AzureMetrics
| summarize Count=count() by ResourceId# Créer un catalogue Microsoft Azure

> **Remarque :**
>
> Depuis juillet 2023, Microsoft a renommé Azure Active Directory (Azure AD) Microsoft Entra ID. Dans ce document, toute occurrence de l'appellation Azure Active Directory, Azure AD ou de l'acronyme AAD fait désormais référence à Microsoft Entra ID.

La section Créer des catalogues de machines décrit les assistants qui permettent de créer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements de cloud Microsoft Azure Resource Manager.

> **Remarque :**
>
> Avant de créer un catalogue Microsoft Azure, vous devez terminer la création d'une connexion à Microsoft Azure. Voir Connexion à Microsoft Azure.

## Créer un catalogue de machines

Vous pouvez créer un catalogue de machines de deux manières :

- Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans Web Studio
- Créer un catalogue de machines à l'aide de PowerShell

### Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans Web Studio

Une image peut être un disque, un instantané ou une version d'image d'une définition d'image dans Azure Compute Gallery utilisé pour créer les machines virtuelles dans un catalogue de machines.

Avant de créer le catalogue de machines, créez une image dans Azure Resource Manager. Pour obtenir des informations générales sur les images, consultez la rubrique Créer des catalogues de machines.

> **Remarque :**
>
> La prise en charge de l'utilisation d'une image principale provenant d'une région différente de celle configurée dans la connexion hôte est obsolète. Utilisez Azure Compute Gallery pour répliquer l'image principale dans la région souhaitée.

Lors de la préparation de l'image, une machine virtuelle (machine virtuelle) de préparation est créée sur la base de la machine virtuelle d'origine. Cette machine virtuelle de préparation est déconnectée du réseau. Pour déconnecter le réseau de la machine virtuelle de préparation, un groupe de sécurité réseau est créé pour refuser tout trafic entrant et sortant. Le groupe de sécurité réseau est créé automatiquement une fois par catalogue. Le nom du groupe de sécurité réseau est <!JEKYLL@5300@0> où le GUID est généré de manière aléatoire. Par exemple, <!JEKYLL@5300@1>.

Dans l'assistant de création de catalogue de machines :

- Les pages **Type de machine** et **Gestion des machines** ne contiennent aucune information spécifique à Azure. Suivez les instructions de l'article Créer des catalogues de machines.
- Sur la page **Image**, choisissez l'image que vous souhaitez utiliser comme modèle pour créer des machines dans ce catalogue.

  Si vous sélectionnez **Image principale** comme type d'image à utiliser, cliquez sur **Sélectionner une image** et procédez comme suit pour sélectionner une image principale si nécessaire :

  1. (Applicable uniquement aux connexions configurées avec des images partagées au sein des locataires ou entre eux) Sélectionnez un abonnement dans lequel se trouve l'image.
  2. Sélectionnez un groupe de ressources.
  3. Accédez au disque dur virtuel Azure, à Azure Compute Gallery ou à la version Azure de l'image. Ajoutez une note pour l'image sélectionnée si nécessaire.

  Lorsque vous sélectionnez une image, tenez compte des points suivants :

  - Vérifiez qu'un Citrix VDA est installé sur l'image.
  - Si vous sélectionnez un VHD attaché à une machine virtuelle, vous devez arrêter la machine virtuelle avant de passer à l'étape suivante.

  > **Remarque :**
  >
  > - L'abonnement correspondant à la connexion (hôte) qui a créé les machines du catalogue est indiqué par un point vert. Les autres abonnements sont ceux pour lesquels une galerie Azure Compute Gallery est partagée avec cet abonnement. Dans ces abonnements, seules les galeries partagées sont affichées. Pour plus d'informations sur

la configuration des abonnements partagés, reportez-vous aux sections Partager des images au sein d'un locataire (entre abonnements) et Partager des images entre locataires.

- L'utilisation d'un profil de machine avec lancement fiable comme **Type de sécurité** est obligatoire lorsque vous sélectionnez une image ou un instantané pour lequel le lancement fiable est activé. Vous pouvez ensuite activer ou désactiver SecureBoot et vTPM en spécifiant leurs valeurs dans le profil de la machine. Le lancement fiable n'est pas pris en charge pour Shared Image Gallery. Pour plus d'informations sur le lancement fiable Azure, consultez https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
- Vous pouvez créer un schéma de provisioning à l'aide d'un disque d'OS éphémère sous Windows avec lancement fiable. Lorsque vous sélectionnez une image avec lancement fiable, vous devez sélectionner un profil de machine avec lancement fiable qui est activé avec vTPM. Pour créer des catalogues de machines à l'aide d'un disque d'OS éphémère, consultez Comment créer des machines à l'aide de disques d'OS éphémères.
- Lorsque la réplication de l'image est en cours, vous pouvez continuer et sélectionner l'image comme image principale et terminer la configuration. Toutefois, la création du catalogue peut prendre plus de temps pendant la réplication de l'image. MCS requiert que la réplication soit terminée dans un délai d'une heure à compter de la création du catalogue. Si le délai de réplication est dépassé, la création du catalogue échoue. Vous pouvez vérifier l'état de la réplication dans Azure. Réessayez si la réplication est toujours en attente ou une fois la réplication terminée.
- Lorsque vous sélectionnez une image principale pour les catalogues de machines dans Azure, MCS identifie le type de système d'exploitation en fonction de l'image principale et du profil de machine que vous sélectionnez. Si MCS ne parvient pas à l'identifier, sélectionnez le type de système d'exploitation correspondant à l'image principale.
- Vous pouvez provisionner un catalogue de machines virtuelles Gen2 en utilisant une image Gen2 pour améliorer les performances de démarrage. Toutefois, la création d'un catalogue de machines Gen2 à l'aide d'une image Gen1 n'est pas prise en charge. De même, la création d'un catalogue de machines Gen1 à l'aide d'une image Gen2 n'est pas non plus prise en charge. Par ailleurs, toute image plus ancienne qui ne possède pas d'informations de génération est une image Gen1.

Si vous sélectionnez **Image préparée** comme type d'image à utiliser, cliquez sur **Sélectionner une image** et sélectionnez une image préparée si nécessaire.

Pour garantir la réussite de la création de la machine virtuelle, vérifiez que Citrix VDA 2311 ou version ultérieure est installé sur l'image et que MCSIO est présent sur le VDA.

Une fois que vous avez sélectionné une image, la case **Utiliser un profil de machine (obligatoire pour Azure Active Directory)** est automatiquement cochée. Cliquez sur **Sélectionner un profil de machine** pour accéder à une spécification de modèle ARM ou machine virtuelle à partir d'une liste de groupes de ressources. Les machines virtuelles du catalogue peuvent hériter des configurations du profil de machine sélectionné.

Validez la spécification du modèle ARM pour vous assurer qu'elle peut être utilisée comme profil de machine pour créer un catalogue de machines. Il existe deux manières de valider la spécification du modèle ARM :

- Après avoir sélectionné la spécification du modèle ARM dans la liste des groupes de ressources, cliquez sur **Suivant**. Des messages d'erreur s'affichent si la spécification du modèle ARM contient des erreurs.
- Exécutez une des commandes PowerShell suivantes :
  * <!JEKYLL@5300@2>
  * <!JEKYLL@5300@3>

Voici quelques exemples de configurations dont les machines virtuelles peuvent hériter d'un profil de machine :

- Réseaux accélérés
- Diagnostic de démarrage
- Mise en cache du disque hôte (relative aux disques OS et MCSIO)
- Taille de la machine (sauf indication contraire)
- Balises placées sur la machine virtuelle

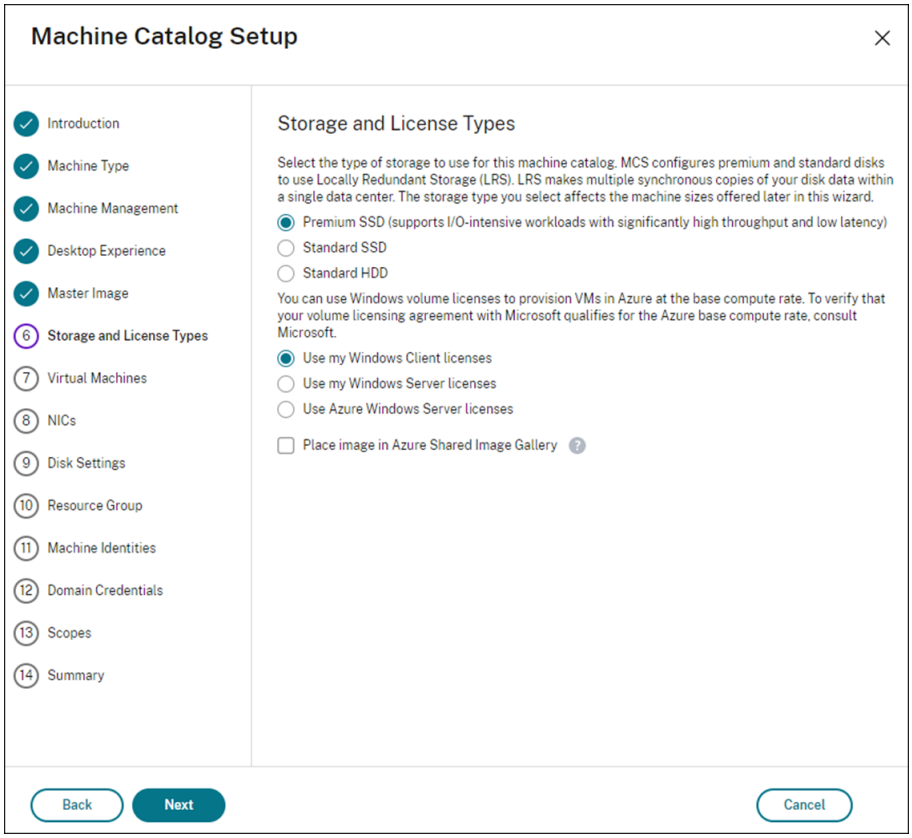
Après avoir créé le catalogue, vous pouvez afficher les configurations du profil de machine dont l'image hérite. Dans le nœud **Catalogues de machines**, sélectionnez le catalogue pour afficher ses détails dans le volet inférieur. Cliquez ensuite sur l'onglet **Propriétés du modèle** pour afficher les propriétés du profil de machine. La section **Balises** affiche jusqu'à trois balises. Pour afficher toutes les balises placées sur la machine virtuelle, cliquez sur **Afficher tout**.

Si vous souhaitez que MCS provisionne des machines virtuelles sur un hôte dédié Azure, cochez la case **Utiliser un groupe d'hôtes dédié**, puis sélectionnez un groupe d'hôtes dans la liste. Un groupe d'hôtes est une ressource qui représente un ensemble d'hôtes dédiés. Un hôte dédié est un service qui fournit des serveurs physiques qui hébergent une ou plusieurs machines virtuelles. Votre serveur est dédié à votre abonnement Azure et n'est pas partagé avec d'autres abonnés. Lorsque vous utilisez un hôte dédié, Azure s'assure que vos machines virtuelles sont les seules machines exécutées sur cet hôte. Cette fonctionnalité convient aux scénarios dans lesquels vous devez répondre à des exigences réglementaires ou de sécurité internes. Pour en savoir plus sur les groupes d'hôtes et les considérations relatives à leur utilisation, consultez la rubrique Hôtes dédiés Azure.

> **Important :**
>
> – Seuls les groupes d'hôtes pour lesquels le placement automatique Azure est activé sont affichés.
> – L'utilisation d'un groupe d'hôtes modifie la page **Machines virtuelles** proposée plus loin dans l'assistant. Seules les tailles de machine contenues dans le groupe d'hôtes sélectionné sont affichées sur cette page. De plus, les zones de disponibilité sont sélectionnées automatiquement et ne sont pas proposées à la sélection.

- La page **Types de stockage et de licence** s'affiche uniquement lors de l'utilisation de l'image Azure Resource Manager.




Les types de stockage suivants peuvent être utilisés pour le catalogue de machines :

– **SSD premium**. Offre une option de stockage sur disque hautes performances et à faible latence adaptée aux machines virtuelles avec des charges d'E/S intensives.
– **SSD standard**. Offre une option de stockage économique qui convient aux charges de travail nécessitant des performances constantes à des niveaux d'E/S par seconde inférieurs.
– **HDD standard**. Offre une option de stockage sur disque fiable et économique adaptée aux machines virtuelles qui exécutent des charges de travail insensibles à la latence.
– **Disque d'OS éphémère Azure**. Offre une option de stockage économique qui réutilise le disque local des machines virtuelles pour héberger le disque du système d'exploita-

tion. Vous pouvez également utiliser PowerShell pour créer des machines qui utilisent des disques d'OS éphémères. Pour plus d'informations, consultez Disques éphémères Azure. Lorsque vous utilisez un disque d'OS éphémère, prenez en compte les points suivants :

* Le disque d'OS éphémère Azure et les E/S de MCS ne peuvent pas être activés en même temps.
* Pour mettre à jour les machines qui utilisent des disques d'OS éphémères, vous devez sélectionner une image dont la taille n'excède pas la taille du disque cache ou du disque temporaire de la machine virtuelle.
* Vous ne pouvez pas utiliser l'option **Conserver la machine virtuelle et le disque système pendant les cycles d'alimentation** proposée ultérieurement dans l'Assistant.

> **Remarque :**
>
> Le disque d'identité est toujours créé à l'aide d'un SSD standard, quel que soit le type de stockage que vous choisissez.

Le type de stockage détermine les tailles de machine qui sont disponibles sur la page **Machines virtuelles** de l'assistant. MCS configure les disques standard et premium pour utiliser le stockage localement redondant (LRS). LRS effectue de multiples copies synchrones de vos données dans un seul data center. Les disques d'OS éphémères Azure utilisent le disque local des machines virtuelles pour stocker le système d'exploitation. Pour de plus amples informations sur les types de stockage et la réplication de stockage Azure, consultez les rubriques suivantes :

- https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction/
- https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance/
- https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy/

Indiquez si vous souhaitez utiliser des licences Windows ou Linux existantes.

- Licences Windows : l'utilisation de licences Windows avec des images Windows (images de support de plate-forme Azure ou images personnalisées) vous permet d'exécuter des machines virtuelles Windows dans Azure à un coût réduit. Il existe deux types de licences :

  * **Licence Windows Server**. Vous permet d'utiliser vos licences Windows Server ou Azure Windows Server, ce qui vous permet d'utiliser Azure Hybrid Benefits. Pour plus de détails, consultez https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. Azure Hybrid Benefit réduit les coûts d'exécution de machine virtuelle dans Azure au taux de calcul de base, les licences Windows Server supplémentaires de la galerie Azure sont donc gratuites.

  * **Licence client Windows**. Vous permet de transférer vos licences Windows 10 et Windows 11 vers Azure, ce qui vous permet d'exécuter des machines virtuelles Windows

10 et Windows 11 dans Azure sans avoir besoin de licences supplémentaires. Pour plus de détails, consultez la section Licences d'accès client et licences de gestion.

Vous pouvez vérifier que la machine virtuelle provisionnée utilise bien une de ces licences en exécutant la commande PowerShell suivante : <!JEKYLL@5300@4>.

- Pour le type de licence Windows Server, vérifiez que le type de licence est **Windows_Server**. Des instructions supplémentaires sont disponibles sur https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.
- Pour le type de licence Client Windows, vérifiez que le type de licence est **Windows_Client**. Des instructions supplémentaires sont disponibles sur https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

Vous pouvez également utiliser le SDK PowerShell <!JEKYLL@5300@5> pour effectuer la vérification. Par exemple : <!JEKYLL@5300@6>. Pour plus d'informations sur cette applet de commande, voir https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Licences Linux : avec les licences Linux BYOS (Bring-Your-Own-Subscription), vous n'avez pas à payer le logiciel. Les frais BYOS incluent uniquement les frais liés au matériel informatique. Il existe deux types de licences :
  - **RHEL_BYOS** : pour utiliser le type RHEL_BYOS, activez Red Hat Cloud Access sur votre abonnement Azure.
  - **SLES_BYOS** : les versions BYOS de SLES incluent la prise en charge de SUSE.

  Vous pouvez définir la valeur LicenseType sur les options Linux dans les champs <!JEKYLL@5300@7> et <!JEKYLL@5300@8>.

  Exemple de définition de LicenseType sur RHEL_BYOS dans le champ <!JEKYLL@5300@9> :

  <!JEKYLL@5300@10>

  Exemple de définition de LicenseType sur SLES_BYOS dans le champ <!JEKYLL@5300@11> :

  <!JEKYLL@5300@12>

  > **Remarque :**
  >
  > Si la valeur <!JEKYLL@5300@13> est vide, les valeurs par défaut sont Azure Windows Server License ou Azure Linux License, selon la valeur OsType.

  Exemple de définition de LicenseType sur une valeur vide :

  <!JEKYLL@5300@14>

Consultez les documents suivants pour comprendre les types de licence et leurs avantages :

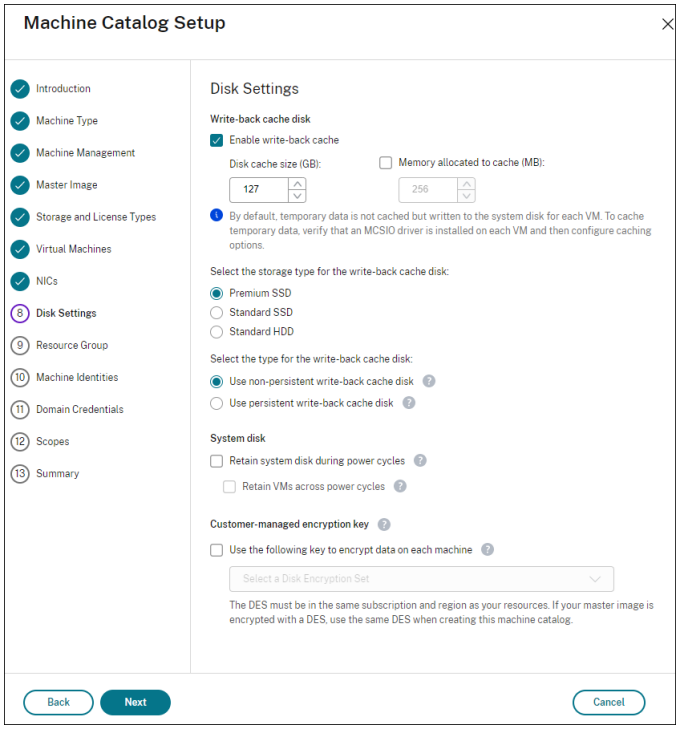
- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery (anciennement Azure Shared Image Gallery) est un référentiel permettant de gérer et de partager des images. Il vous permet de mettre vos images à disposition de l'ensemble de votre organisation. Nous vous recommandons de stocker une image dans SIG lors de la création de catalogues de machines non persistants volumineux, car cela permet de réinitialiser plus rapidement les disques du système d'exploitation VDA. Après avoir sélectionné **Placer l'image préparée dans Azure Compute Gallery**, la section **Paramètres d'Azure Compute Gallery** apparaît, vous permettant de spécifier des paramètres Azure Compute Gallery supplémentaires :

- **Ratio réplicas d'images/machines virtuelles**. Permet de spécifier le ratio entre les machines virtuelles et les réplicas d'images que vous souhaitez conserver dans Azure. Par défaut, Azure conserve un réplica d'image unique pour 40 machines non persistantes. Pour les machines persistantes, ce nombre est 1 000 par défaut.
- **Nombre maximal de réplicas**. Vous permet de spécifier le nombre maximal de réplicas d'images que vous souhaitez qu'Azure conserve. La valeur par défaut est 10.

- Sur la page **Machines virtuelles**, indiquez le nombre de machines virtuelles à créer. Vous devez en spécifier au moins une et sélectionner une taille de machine. Après la création du catalogue, vous pouvez modifier la taille de machine en modifiant le catalogue.
- La page **Cartes d'interface réseau** ne contient pas d'informations spécifiques à Azure. Suivez les instructions de l'article Créer des catalogues de machines.
- Sur la page **Paramètres du disque**, indiquez si vous souhaitez activer le cache en écriture différée. Lorsque la fonctionnalité d'optimisation du stockage MCS est activée, vous pouvez configurer les paramètres suivants lors de la création d'un catalogue. Ces paramètres s'appliquent aux environnements Azure et GCP.




Après avoir activé le cache en écriture différée, vous pouvez effectuer les opérations suivantes :

- Configurez la taille du disque et de la RAM utilisés pour la mise en cache des données temporaires. Pour plus d'informations, consultez Configurer un cache pour les données temporaires.
- Sélectionnez le type de stockage pour le disque de cache en écriture différée. Les options de stockage suivantes peuvent être utilisées pour le disque de cache en écriture différée :
  * SSD premium
  * SSD standard
  * HDD standard
- Choisissez si vous souhaitez que le disque de cache en écriture différée persiste pour les machines virtuelles provisionnées. Sélectionnez **Activer le cache en écriture différée** pour voir les options disponibles. Par défaut, l'option **Utiliser disque de cache en écriture différée non persistant** est sélectionnée.
- Sélectionnez le type de disque de cache en écriture différée.
  * **Utilisez disque de cache en écriture différée non persistant**. Si cette option est sélectionnée, le disque de cache en écriture différée est supprimé pendant les cycles d'alimentation. Toutes les données qui y sont redirigées seront perdues. Si le disque temporaire de la machine virtuelle dispose de suffisamment d'espace, il est utilisé pour héberger le disque de cache en écriture différée afin de réduire vos coûts. Après la création du catalogue, vous pouvez vérifier si les machines provisionnées utilisent

le disque temporaire. Pour ce faire, cliquez sur le catalogue et vérifiez les informations de l'onglet **Propriétés du modèle**. Si le disque temporaire est utilisé, l'option **Disque de cache en écriture différée non persistant** est affichée et sa valeur est **Oui (à l'aide du disque temporaire de la machine virtuelle)**. Si ce n'est pas le cas, l'option **Disque de cache en écriture différée non persistant** est affichée et sa valeur est **Non (sans le disque temporaire de la machine virtuelle)**.

  * **Utiliser disque de cache en écriture différée persistant**. Si cette option est sélectionnée, le disque de cache en écriture différée persiste pour les machines virtuelles provisionnées. L'activation de cette option augmente vos coûts de stockage.

- Indiquez si vous souhaitez conserver les machines virtuelles et les disques système pour les VDA pendant les cycles d'alimentation.

  **Conservation des machines virtuelles et des disques système pendant les cycles d'alimentation**. Disponible lorsque vous avez sélectionné **Activer le cache en écriture différée**. Par défaut, les machines virtuelles et les disques système sont supprimés à l'arrêt et recréés au démarrage. Si vous souhaitez réduire les temps de redémarrage des machines virtuelles, sélectionnez cette option. N'oubliez pas que l'activation de cette option augmente également les coûts de stockage.

- Choisissez si vous souhaitez activer les **Économies sur les coûts de stockage**. Si cette option est activée, réduisez les coûts de stockage en rétrogradant le disque de stockage vers un disque dur standard lorsque la machine virtuelle s'arrête. La machine virtuelle revient à ses paramètres d'origine au redémarrage. L'option s'applique à la fois aux disques de stockage et aux disques de cache à écriture différée. Vous pouvez également utiliser PowerShell. Voir Changer le type de stockage vers un niveau inférieur lorsqu'une machine virtuelle est arrêtée.

  > **Remarque :**
  >
  > Microsoft impose des restrictions sur la modification du type de stockage lors de l'arrêt de la machine virtuelle. Il est également possible que Microsoft bloque les changements de type de stockage à l'avenir. Pour plus d'informations, consultez cet article Microsoft.

- Indiquez si vous souhaitez chiffrer les données sur les machines provisionnées dans le catalogue. Le chiffrement côté serveur à l'aide d'une clé de chiffrement gérée par le client vous permet de gérer le chiffrement au niveau du disque géré et de protéger les données sur les machines du catalogue. Pour plus d'informations, consultez Chiffrement Azure côté serveur.

- Sur la page **Groupe de ressources**, choisissez si vous souhaitez créer des groupes de ressources ou utiliser des groupes existants.

  - Si vous choisissez de créer des groupes de ressources, sélectionnez **Suivant**.
  - Si vous choisissez d'utiliser des groupes de ressources existants, sélectionnez les groupes dans la liste **Groupes de ressources de provisioning disponibles**. **Rappel** : sélectionnez un nombre suffisant de groupes pour prendre en charge les machines que vous créez dans le catalogue. Un message s'affiche si vous n'en choisissez pas assez. Vous pouvez sélectionner un nombre supérieur au minimum requis si vous envisagez d'ajouter d'autres machine virtuelle au catalogue ultérieurement. Vous ne pouvez pas ajouter d'autres groupes de ressources à un catalogue après que le catalogue a été créé.

  Pour plus d'informations, consultez la rubrique Groupes de ressources Azure.

- Sur la page **Identités des machines**, choisissez un type d'identité et configurez les identités des machines de ce catalogue. Si vous sélectionnez **Joint à Azure Active Directory** pour les machines virtuelles, vous pouvez les ajouter à un groupe de sécurité Azure AD. Les étapes détaillées sont les suivantes :

  1. Dans le champ **Type d'identité**, sélectionnez **Joint à Azure Active Directory**. L'option **Groupe de sécurité Azure AD (facultatif)** s'affiche.
  2. Cliquez sur **Groupe de sécurité Azure AD : Créer un nouveau**.
  3. Entrez un nom de groupe, puis cliquez sur **Créer**.
  4. Suivez les instructions qui s'affichent à l'écran pour vous connecter à Azure.
     Si le nom du groupe n'existe pas dans Azure, une icône verte apparaît. Dans le cas contraire, un message d'erreur s'affiche vous demandant de saisir un nouveau nom.
  5. Entrez le schéma de dénomination des comptes de machines virtuelles.

  Après la création du catalogue, Citrix Virtual Apps and Desktops accède à Azure en votre nom et crée le groupe de sécurité ainsi qu'une règle d'appartenance dynamique pour le groupe. Selon cette règle, les machines virtuelles dont le schéma de dénomination est spécifié dans ce catalogue sont automatiquement ajoutées au groupe de sécurité.

  Pour ajouter des machines virtuelles avec un schéma de dénomination différent à ce catalogue, vous devez vous connecter à Azure. Citrix Virtual Apps and Desktops peut ensuite accéder à Azure et créer une règle d'appartenance dynamique basée sur le nouveau schéma de dénomination.

  Lorsque vous supprimez ce catalogue, la suppression du groupe de sécurité d'Azure nécessite également de vous connecter à Azure.

- Les pages **Informations d'identification du domaine** et **Résumé** ne contiennent pas d'informations spécifiques à Azure. Suivez les instructions de l'article Créer des catalogues de machines.

Suivez les instructions de l'assistant.

### Conditions pour que le disque temporaire Azure puisse être utilisé comme disque de cache en écriture différée

Vous pouvez utiliser le disque temporaire Azure en tant que disque de cache en écriture différée uniquement si toutes les conditions suivantes sont remplies :

- Le disque de cache en écriture différée ne doit pas persister car le disque temporaire Azure n'est pas approprié pour les données persistantes.
- La taille de machine virtuelle Azure choisie doit inclure un disque temporaire.
- Il n'est pas nécessaire d'activer le disque d'OS éphémère.
- Acceptez de placer le fichier de cache en écriture différée sur le disque temporaire Azure.
- La taille du disque temporaire Azure doit être supérieure à la taille totale de (taille du disque du cache en écriture différée + espace réservé pour le fichier d'échange + 1 Go d'espace tampon).

### Scénarios de disque de cache en écriture différée non persistant

Le tableau suivant décrit trois scénarios différents dans lesquels un disque temporaire est utilisé pour le cache en écriture différée lors de la création d'un catalogue de machines.

| Scénario | Résultat |
| --- | --- |
| Toutes les conditions pour utiliser un disque temporaire pour le cache en écriture différée sont remplies. | Le fichier WBC <!JEKYLL@5300@15> est placé sur le disque temporaire. |
| Le disque temporaire ne dispose pas d'espace suffisant pour l'utilisation du cache en écriture différée. | Un disque VHD <!JEKYLL@5300@16> est créé et un fichier WBC <!JEKYLL@5300@17> est placé sur ce disque. |
| Le disque temporaire dispose de suffisamment d'espace pour l'utilisation du cache en écriture différée, mais <!JEKYLL@5300@18> est défini sur **false**. | Un disque VHD <!JEKYLL@5300@19> est créé et un fichier WBC <!JEKYLL@5300@20> est placé sur ce disque. |

### Créer une spécification de modèle Azure

Vous pouvez créer une spécification de modèle Azure dans le portail Azure et l'utiliser dans Web Studio ou exécuter des commandes PowerShell pour créer ou mettre à jour un catalogue de machines MCS.

Pour créer une spécification de modèle Azure pour une machine virtuelle existante :

1. Accédez au portail Azure. Sélectionnez un groupe de ressources, puis sélectionnez la machine virtuelle et l'interface réseau. Dans le menu **...** en haut de la page, cliquez sur **Exporter le modèle**.
2. Décochez la case **Inclure les paramètres** si vous souhaitez créer une spécification de modèle pour le provisioning du catalogue.
3. Cliquez sur **Ajouter à la bibliothèque** pour modifier ultérieurement la spécification de modèle.
4. Sur la page **Importation du modèle**, entrez les informations requises telles que le **nom**, l'**abonnement**, le **groupe de ressources**, l'**emplacement** et **la version**. Cliquez sur **Suivant : Modifier le modèle**.
5. Vous avez également besoin d'une interface réseau en tant que ressource indépendante si vous souhaitez provisionner des catalogues. Par conséquent, vous devez supprimer tout <!JEKYLL@5300@21> spécifié dans la spécification de modèle. Par exemple :

   <!JEKYLL@5300@22>
6. Créez **Examiner et créer** et créez la spécification de modèle.
7. Sur la page **Specs de modèle**, vérifiez la spécification de modèle que vous venez de créer. Cliquez sur la spécification de modèle. Dans le panneau de gauche, cliquez sur **Versions**.
8. Vous pouvez créer une nouvelle version en cliquant sur **Créer version**. Spécifiez un nouveau numéro de version, modifiez la spécification de modèle actuelle, puis cliquez sur **Examiner et créer** pour créer la nouvelle version de la spécification de modèle.

Vous pouvez obtenir des informations sur la spécification de modèle et la version du modèle à l'aide des commandes PowerShell suivantes :

- Pour obtenir des informations sur la spécification de modèle, exécutez :

  <!JEKYLL@5300@23>
- Pour obtenir des informations sur la version de la spécification de modèle, exécutez :

  <!JEKYLL@5300@24>

### Utiliser une spécification de modèle pour créer ou mettre à jour un catalogue

Vous pouvez créer ou mettre à jour un catalogue de machines MCS à l'aide d'une spécification de modèle comme entrée de profil de machine. Pour ce faire, vous pouvez utiliser les commandes Web Studio ou PowerShell.

- Pour Web Studio, voir Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans Web Studio.
- Pour PowerShell, voir Utiliser une spécification de modèle lors de la création ou de la mise à jour d'un catalogue à l'aide de PowerShell.

### Chiffrement Azure côté serveur

Citrix Virtual Apps and Desktops prend en charge les clés de cryptage gérées par le client pour les disques gérés Azure via Azure Key Vault. Cette prise en charge vous permet de gérer vos exigences en matière d'organisation et de conformité en chiffrant les disques gérés de votre catalogue de machines à l'aide de vos propres clés de chiffrement. Pour plus d'informations, consultez Chiffrement côté serveur de stockage sur disque Azure.

Lors de l'utilisation de cette fonctionnalité pour les disques gérés :

- Pour modifier la clé avec laquelle le disque est chiffré, modifiez la clé actuelle dans <!JEKYLL@5300@25>. Toutes les ressources associées à la modification de <!JEKYLL@5300@26> doivent être chiffrées avec la nouvelle clé.
- Lorsque vous désactivez ou supprimez votre clé, toutes les machines virtuelles avec des disques utilisant cette clé s'arrêtent automatiquement. Après l'arrêt, les machines virtuelles ne sont pas utilisables, sauf si la clé est réactivée ou si vous attribuez une nouvelle clé. Tout catalogue utilisant la clé ne peut pas être mis sous tension et vous ne pouvez pas y ajouter de machines virtuelles.

#### Considérations importantes lors de l'utilisation de clés de chiffrement gérées par le client

Tenez compte de ce qui suit lors de l'utilisation de cette fonctionnalité :

- Toutes les ressources associées aux clés gérées par le client (instances Azure Key Vaults, jeux de cryptage de disque, machines virtuelles, disques et instantanés) doivent résider dans le même abonnement et la même région.
- Une fois que vous avez activé la clé de chiffrement gérée par le client, vous ne pouvez pas la désactiver ultérieurement. Si vous souhaitez désactiver ou supprimer la clé de chiffrement gérée par le client, copiez toutes les données sur un autre disque géré qui n'utilise pas la clé de chiffrement gérée par le client.
- Les disques créés à partir d'images personnalisées chiffrées à l'aide du chiffrement côté serveur et des clés gérées par le client doivent être chiffrés à l'aide des mêmes clés gérées par le client. Ces disques doivent résider dans le même abonnement.
- Les instantanés créés à partir de disques chiffrés à l'aide du chiffrement côté serveur et des clés gérées par le client doivent être chiffrés à l'aide des mêmes clés gérées par le client.
- Les disques, instantanés et images chiffrés à l'aide de clés gérées par le client ne peuvent pas être transférés vers un autre groupe de ressources et un autre abonnement.
- Les disques gérés, actuellement ou préalablement chiffrés à l'aide d'Azure Disk Encryption, ne peuvent pas être chiffrés à l'aide de clés gérées par le client.

- Consultez le site Microsoft pour connaître les limitations des jeux de cryptage de disque par région.

> **Remarque :**
>
> Consultez Démarrage rapide : créer un coffre de clés avec le portail Azure pour plus d'informations sur la configuration du cryptage Azure côté serveur.

### Clé de cryptage gérée par le client Azure

Lors de la création d'un catalogue de machines, vous pouvez choisir de chiffrer les données sur les machines provisionnées dans le catalogue. Le chiffrement côté serveur à l'aide d'une clé de chiffrement gérée par le client vous permet de gérer le chiffrement au niveau du disque géré et de protéger les données sur les machines du catalogue. Un jeu de chiffrement de disque (Disk Encryption Set ou DES) représente une clé gérée par le client. Pour utiliser cette fonctionnalité, vous devez d'abord créer votre DES dans Azure. Un DES est dans le format suivant :

- <!JEKYLL@5300@27>

Sélectionnez un DES dans la liste. Le DES sélectionné doit se trouver dans le même abonnement et la même région que vos ressources. Si votre image est chiffrée avec un DES, utilisez le même DES lors de la création du catalogue de machines. Vous ne pouvez pas modifier le DES après avoir créé le catalogue.

Si vous créez un catalogue avec une clé de cryptage et que vous désactivez ultérieurement le DES correspondant dans Azure, vous ne pouvez plus mettre les machines du catalogue sous tension ou y ajouter des machines.

Consultez la section Créer un catalogue de machines à l'aide d'une clé gérée par le client.

### Cryptage de disque sur l'hôte Azure

Vous pouvez créer un catalogue de machines MCS avec fonctionnalité de cryptage sur l'hôte. Actuellement, MCS prend uniquement en charge le workflow de profil de machine pour cette fonctionnalité. Vous pouvez utiliser une machine virtuelle ou une spécification de modèle comme entrée pour un profil de machine.

Cette méthode de chiffrement ne chiffre pas les données via le stockage Azure. Le serveur hébergeant la machine virtuelle chiffre les données, puis les données chiffrées circulent via le serveur de stockage Azure. Par conséquent, cette méthode de chiffrement chiffre les données de bout en bout.

**Restrictions :**

Limites du chiffrement de disque Azure sur l'hôte :

- Non pris en charge pour toutes les tailles de machines Azure
- Incompatible avec le chiffrement de disque Azure

Pour créer un catalogue de machines avec fonctionnalité de chiffrement sur l'hôte, procédez comme suit :

1. Vérifiez si la fonctionnalité de chiffrement sur l'hôte est activée ou non dans l'abonnement. Pour ce faire, voir https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Si elle n'est pas activée, vous devez activer la fonctionnalité pour l'abonnement. Pour plus d'informations sur l'activation de cette fonctionnalité pour votre abonnement, consultez https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Vérifiez si une taille de machine virtuelle Azure particulière prend en charge le chiffrement sur l'hôte ou non. Pour ce faire, dans une fenêtre PowerShell, exécutez l'une des opérations suivantes :

   <!JEKYLL@5300@28>

   <!JEKYLL@5300@29>
3. Créez une machine virtuelle ou une spécification de modèle, en tant qu'entrée pour le profil de la machine, dans le portail Azure avec le chiffrement sur l'hôte activé.

   - Si vous souhaitez créer une machine virtuelle, sélectionnez une taille de machine virtuelle qui prend en charge le chiffrement sur l'hôte. Une fois la machine virtuelle créée, la propriété de la machine virtuelle **Chiffrement sur l'hôte** est activée.
   - Si vous souhaitez utiliser une spécification de modèle, attribuez au paramètre <!JEKYLL@5300@30> la valeur **true** dans <!JEKYLL@5300@31>.
4. Créez un catalogue de machines MCS avec un workflow de profil de machine en sélectionnant une machine virtuelle ou une spécification de modèle.

   - Disque d'OS/disque de données : chiffré via une clé gérée par le client et une clé gérée par la plate-forme
   - Disque d'OS éphémère : chiffré uniquement via une clé gérée par la plate-forme
   - Disque cache : chiffré via une clé gérée par le client et une clé gérée par la plate-forme

   Vous pouvez créer le catalogue de machines à l'aide de Web Studio ou en exécutant des commandes PowerShell.

#### Récupérer les informations de chiffrement sur l'hôte à partir d'un profil de machine

Vous pouvez récupérer les informations de chiffrement sur l'hôte à partir d'un profil de machine lorsque vous exécutez la commande PowerShell avec le paramètre <!JEKYLL@5300@32>. Si le

paramètre <!JEKYLL@5300@33> est **True**, cela indique que le chiffrement sur l'hôte est activé pour le profil de machine.

Par exemple : lorsque l'entrée du profil de machine est une machine virtuelle, exécutez la commande suivante :

<!JEKYLL@5300@34>

Par exemple : lorsque l'entrée du profil de la machine est une spécification de modèle, exécutez la commande suivante :

<!JEKYLL@5300@35>

### Chiffrement double sur disque géré

Vous pouvez créer un catalogue de machines avec chiffrement double. Tous les catalogues créés à l'aide de cette fonctionnalité sont chiffrés côté serveur à l'aide de clés gérées par la plate-forme et par le client. Vous possédez et gérez Azure Key Vault, la clé de chiffrement et les jeux de chiffrement de disque (DES).

Le chiffrement double est un chiffrement côté plate-forme (par défaut) et un chiffrement géré par le client (CMEK). Par conséquent, si vous êtes un client gérant des données sensibles en termes de sécurité et que vous êtes préoccupé par le risque associé à un algorithme de cryptage, à une mise en œuvre ou à une clé compromise, vous pouvez opter pour ce cryptage double. Les disques du système d'exploitation et de données persistants, ainsi que les instantanés et les images sont chiffrés au repos à l'aide du chiffrement double.

> **Remarque :**
>
> - Vous pouvez créer et mettre à jour un catalogue de machines utilisant un chiffrement double à l'aide de Web Studio et de commandes PowerShell. Reportez-vous à la section Créer un catalogue de machines avec chiffrement double pour les commandes PowerShell.
> - Vous pouvez utiliser un workflow non basé sur un profil de machine ou un workflow basé sur un profil de machine pour créer ou mettre à jour un catalogue de machines utilisant un cryptage double.
> - Si vous créez un catalogue de machines à l'aide d'un workflow non basé sur un profil de machine, vous pouvez réutiliser l'ID <!JEKYLL@5300@36> stocké.
> - Si vous utilisez un profil de machine, vous pouvez utiliser une machine virtuelle ou une spécification de modèle comme entrée de profil de machine.

**Limitations :**

- Le chiffrement double n'est pas pris en charge pour les disques Ultra Disks ou Premium SSD v2.
- Le chiffrement double n'est pas pris en charge sur les disques non gérés.

- Si vous désactivez une clé DiskEncryptionSet associée à un catalogue, les machines virtuelles du catalogue sont désactivées.
- Toutes les ressources associées à vos clés gérées par le client (Azure Key Vault, jeux de chiffrement de disque, machines virtuelles, disques et instantanés) doivent résider dans le même abonnement et la même région.
- Vous ne pouvez créer qu'un maximum de 50 jeux de cryptage de disque par région et par abonnement.
- Vous ne pouvez pas mettre à jour un catalogue de machines qui possède déjà un élément <!JEKYLL@5300@37> avec un autre élément <!JEKYLL@5300@38>.

## Groupes de ressources Azure

Les groupes de ressources de provisioning d'Azure permettent de provisionner les machine virtuelle qui fournissent des applications et bureaux aux utilisateurs. Vous pouvez ajouter des groupes de ressources Azure vides existants lorsque vous créez un catalogue de machines MCS, ou ils peuvent être créés pour vous. Pour plus d'informations sur les groupes de ressources Azure, consultez la documentation Microsoft.

### Utilisation du groupe de ressources Azure

Le nombre de machines virtuelles, de disques gérés, d'instantanés et d'images par groupe de ressources Azure n'est pas limité. (La limitation de 240 machines virtuelles/800 disques gérés par groupe de ressources Azure a été supprimée.)

- Lorsque vous utilisez le principal de service à étendue complète pour créer un catalogue de machines, MCS crée uniquement un groupe de ressources Azure et utilise ce groupe pour le catalogue.
- Lorsque vous utilisez le principal de service à étendue limitée pour créer un catalogue de machines, vous devez fournir un groupe de ressources Azure précréé vide pour le catalogue.

## Disques éphémères Azure

Un disque éphémère Azure vous permet de réutiliser le disque cache ou le disque temporaire pour stocker le disque d'OS d'une machine virtuelle compatible Azure. Cette fonctionnalité est utile pour les environnements Azure qui nécessitent un disque SSD plus performant sur un disque dur standard. Pour plus d'informations sur la création d'un catalogue avec un disque éphémère Azure, voir Créer un catalogue avec un disque éphémère Azure.

> **Remarque :**
>
> Les catalogues persistants ne prennent pas en charge les disques d'OS éphémères.

Les disques d'OS éphémères nécessitent que votre schéma de provisioning utilise des disques gérés et une galerie d'images partagées.

### Stockage d'un disque temporaire d'OS éphémère

Vous avez la possibilité de stocker un disque d'OS éphémère sur le disque temporaire de la machine virtuelle ou sur un disque de ressources. Cette fonctionnalité vous permet d'utiliser un disque d'OS éphémère avec une machine virtuelle qui ne possède pas de cache ou dont le cache est insuffisant. Ces machines virtuelles disposent d'un disque temporaire ou de ressources pour stocker un disque d'OS éphémère, tel que <!JEKYLL@5300@39>.

Tenez compte des considérations suivantes :

- Un disque éphémère est stocké soit sur le disque cache de la machine virtuelle, soit sur le disque temporaire (ressource) de la machine virtuelle. Le disque de cache est préféré au disque temporaire, sauf si le disque de cache n'est pas suffisamment grand pour le contenu du disque d'OS.
- Pour les mises à jour, une nouvelle image plus grande que le disque cache mais plus petite que le disque temporaire entraîne le remplacement du disque d'OS éphémère par le disque temporaire de la machine virtuelle.

### Optimisation du stockage MCS (Machine Creation Services) (E/S de MCS) et du disque d'OS éphémère

Le disque d'OS éphémère Azure et les E/S de MCS ne peuvent pas être activés en même temps.

Remarques importantes :

- Vous ne pouvez pas créer un catalogue de machines avec le disque d'OS éphémère et les E/S de MCS activés en même temps.
- Les paramètres PowerShell (<!JEKYLL@5300@40> et <!JEKYLL@5300@41>) échouent avec des messages d'erreur appropriés si vous les définissez sur **true** dans <!JEKYLL@5300@42> ou <!JEKYLL@5300@43>.
- Pour les catalogues de machines existants créés avec les deux fonctionnalités activées, vous pouvez toujours :
  - mettre un catalogue de machines à jour

- ajouter ou supprimer des machines virtuelles
- supprimer un catalogue de machines

### Azure Compute Gallery

Utilisez Azure Compute Gallery (anciennement Azure Shared Image Gallery) en tant que référentiel d'images publiées pour les machines provisionnées avec MCS dans Azure. Vous pouvez stocker une image publiée dans la galerie pour accélérer la création et l'hydratation des disques du système d'exploitation, ce qui améliore les temps de démarrage et de lancement des applications pour les machines virtuelles non persistantes. Shared Image Gallery contient les trois éléments suivants :

- *Galerie* : les images sont stockées ici. MCS crée une galerie pour chaque catalogue de machines.
- *Définition de l'image de la galerie* : cette définition inclut des informations (type et état du système d'exploitation, région Azure) sur l'image publiée. MCS crée une définition d'image pour chaque image créée pour le catalogue.
- *Version d'image de la galerie*: chaque image de Shared Image Gallery peut avoir plusieurs versions, et chaque version peut avoir plusieurs réplicas dans différentes régions. Chaque réplica est une copie complète de l'image publiée.

> **Remarque :**
>
> La fonctionnalité Shared Image Gallery est uniquement compatible avec les disques gérés. Elle n'est pas disponible pour les anciens catalogues de machines.

Pour plus d'informations, consultez la rubrique Vue d'ensemble d'Azure Compute Gallery.

Pour plus d'informations sur la création ou la mise à jour d'un catalogue de machines à l'aide d'une image Azure Compute Gallery avec PowerShell, voir Créer ou mettre à jour un catalogue de machines à l'aide d'une image Azure Compute Gallery.

### Machines virtuelles confidentielles Azure

Les machines virtuelles informatiques confidentielles Azure garantissent que votre bureau virtuel est chiffré en mémoire et protégé lors de son utilisation.

Vous pouvez utiliser MCS pour créer un catalogue avec des machines virtuelles confidentielles Azure. Vous devez utiliser le workflow du profil de machine pour créer un tel catalogue. Vous pouvez utiliser les spécifications de modèle VM et ARM comme entrée de profil de machine.

#### Considérations importantes concernant les machines virtuelles confidentielles

Considérations importantes concernant les tailles de machines virtuelles prises en charge et la création d'un catalogue de machines avec des machines virtuelles confidentielles :

- Tailles de machines virtuelles prises en charge : les machines virtuelles confidentielles prennent en charge les tailles de machines virtuelles suivantes :
  - Série DCasv5
  - Série DCadsv5
  - Série ECasv5
  - Série ECadsv5
- Créez un catalogue de machines avec des machines virtuelles confidentielles.
  - Vous pouvez créer un catalogue de machines virtuelles confidentielles Azure à l'aide des commandes Web Studio et PowerShell.
  - Vous devez utiliser un workflow basé sur le profil de machine pour créer un catalogue de machines avec des machines virtuelles confidentielles Azure. Vous pouvez utiliser une machine virtuelle ou une spécification de modèle comme entrée de profil de machine.
  - L'image principale et l'entrée du profil de la machine doivent toutes deux être activées avec le même type de sécurité confidentiel. Ces types de sécurité sont les suivants :
    - **VMGuestStateOnly** : machine virtuelle confidentielle avec cryptage de l'état invité seulement de la machine virtuelle
    - **DiskWithVMGuestState** : machine virtuelle confidentielle avec cryptage du disque du système d'exploitation et de l'état invité de la machine virtuelle à l'aide d'une clé gérée par la plate-forme ou d'une clé gérée par le client. Les disques du système d'exploitation normal et éphémère peuvent être chiffrés.
  - Le paramètre AdditionalData vous permet d'obtenir des informations de machine virtuelle confidentielle sur différents types de ressources, tels qu'un disque géré, un instantané, une image Azure Compute Gallery, une machine virtuelle et une spécification de modèle ARM. Par exemple :

    <!JEKYLL@5300@44>

    Les champs de données supplémentaires sont les suivants :

    - DiskSecurityType
    - ConfidentialVMDiskEncryptionSetId
    - DiskSecurityProfiles

    Pour obtenir la propriété informatique confidentielle d'une taille de machine, exécutez la commande suivante : <!JEKYLL@5300@45>

    Le champ de données supplémentaire est <!JEKYLL@5300@46>.
  - Vous ne pouvez pas modifier l'image principale ou le profil de la machine d'un type de sécurité confidentiel vers un type de sécurité non confidentiel, ou d'un type de sécurité non confidentiel vers un type de sécurité confidentiel.

- Vous obtenez des messages d'erreur appropriés pour toute configuration incorrecte.

### Préparer des images principales et des profils de machines

Avant de créer un ensemble de machines virtuelles confidentielles, préparez leur image principale et leur profil de machine en procédant comme suit :

1. Dans le portail Azure, créez une machine virtuelle confidentielle avec des paramètres spécifiques, tels que :

   - **Type de sécurité** : machines virtuelles confidentielles
   - **Cryptage des disques confidentiels du système d'exploitation** : activé.
   - **Gestion des clés** : cryptage des disques confidentiels à l'aide d'une clé gérée par la plateforme

     Pour plus d'informations sur la création de machines virtuelles confidentielles, consultez cet article de Microsoft.

2. Préparez l'image principale sur la machine virtuelle créée. Installez les applications et le VDA nécessaires sur la machine virtuelle créée.

   > **Remarque :**
   >
   > La création de machines virtuelles confidentielles à l'aide d'un disque dur virtuel n'est pas prise en charge. Pour cela, utilisez plutôt Azure Compute Gallery, des disques gérés ou des instantanés.

3. Créez le profil de machine en appliquant l'une des méthodes suivantes :

   - Utilisez la machine virtuelle existante créée à l'étape 1 si elle possède les propriétés de machine nécessaires.
   - Si vous optez pour une spécification de modèle ARM comme profil de machine, créez la spécification de modèle selon vos besoins. Plus spécifiquement, vous devez configurer les paramètres qui répondent à la configuration requise de votre machine virtuelle confidentielle, tels que *SecurityEncryptionType* et *diskEncryptionSet* (pour les clés gérées par le client). Pour plus d'informations, consultez Créer une spécification de modèle Azure.

     > **Remarque :**
     >
     > - Assurez-vous que l'image principale et le profil de la machine ont le même type de clé de sécurité.
     > - Pour créer des machines virtuelles confidentielles nécessitant un cryptage des disques confidentiels du système d'exploitation à l'aide d'une clé gérée par le

> client, assurez-vous que les ID du jeu de cryptage de disque sont identiques dans l'image principale et dans le profil de la machine.

#### Créer des machines virtuelles confidentielles à l'aide des commandes Web Studio ou PowerShell

Pour créer un ensemble de machines virtuelles confidentielles, créez un catalogue de machines à l'aide d'une image principale et d'un profil de machine dérivé de la machine virtuelle confidentielle souhaitée.

Pour créer le catalogue à l'aide de Web Studio, suivez les étapes décrites dans l'article Créer des catalogues de machines. Gardez à l'esprit les considérations suivantes :

- Sur la page **Image**, sélectionnez l'image principale et le profil de machine que vous avez préparés en vue de la création d'une machine virtuelle confidentielle. La sélection d'un profil de machine est obligatoire et seuls les profils correspondant au même type de cryptage de sécurité que celui de l'image principale sélectionnée sont disponibles.
- Sur la page **Machines virtuelles**, seules les tailles de machine compatibles avec les machines virtuelles confidentielles s'affichent pour la sélection.
- Sur la page **Paramètres de disque**, vous ne pouvez pas spécifier le jeu de cryptage de disque, car il est hérité du profil de machine sélectionné.

### Azure Marketplace

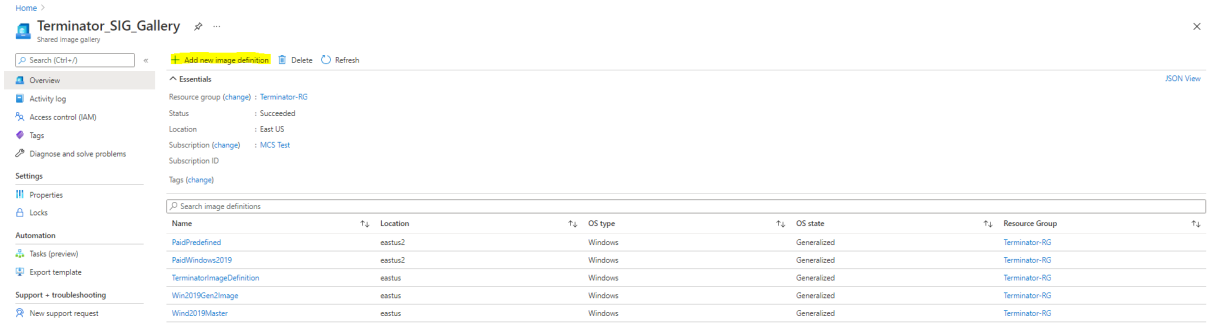
Citrix Virtual Apps and Desktops prend en charge l'utilisation d'une image principale sur Azure qui contient des informations de plan pour créer un catalogue de machines. Pour plus d'informations, consultez Microsoft Azure Marketplace.

> **Conseil :**
>
> Certaines images disponibles sur Azure Marketplace, telles que l'image Windows Server standard, n'ajoutent pas d'informations de plan. La fonctionnalité Citrix Virtual Apps and Desktops est destinée aux images payantes.

#### S'assurer que l'image créée dans Shared Image Gallery contient des informations de plan Azure

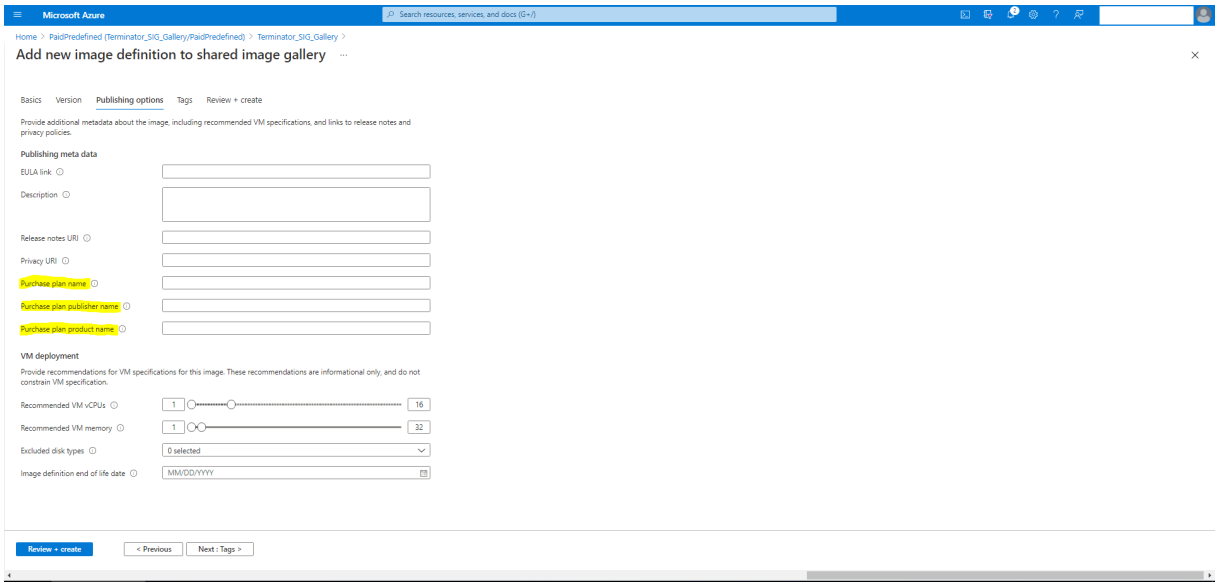
Suivez la procédure décrite dans cette section pour afficher les images de Shared Image Gallery dans Web Studio. Ces images peuvent éventuellement être utilisées pour une image principale. Pour placer l'image dans Shared Image Gallery, créez une définition d'image dans une galerie.



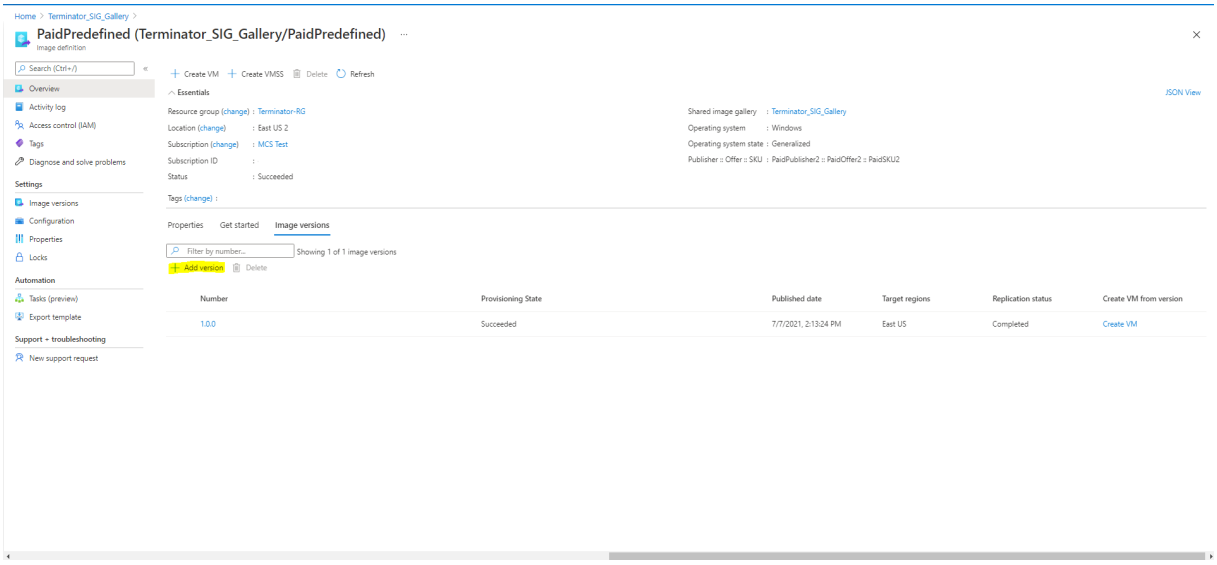

Sur la page **Options de publication**, vérifiez les informations du plan d'achat.

Les champs d'informations sur le plan d'achat sont initialement vides. Renseignez ces champs avec les informations de plan d'achat utilisées pour l'image. Ne pas renseigner les informations du plan d'achat peut entraîner l'échec du processus de catalogue de machines.

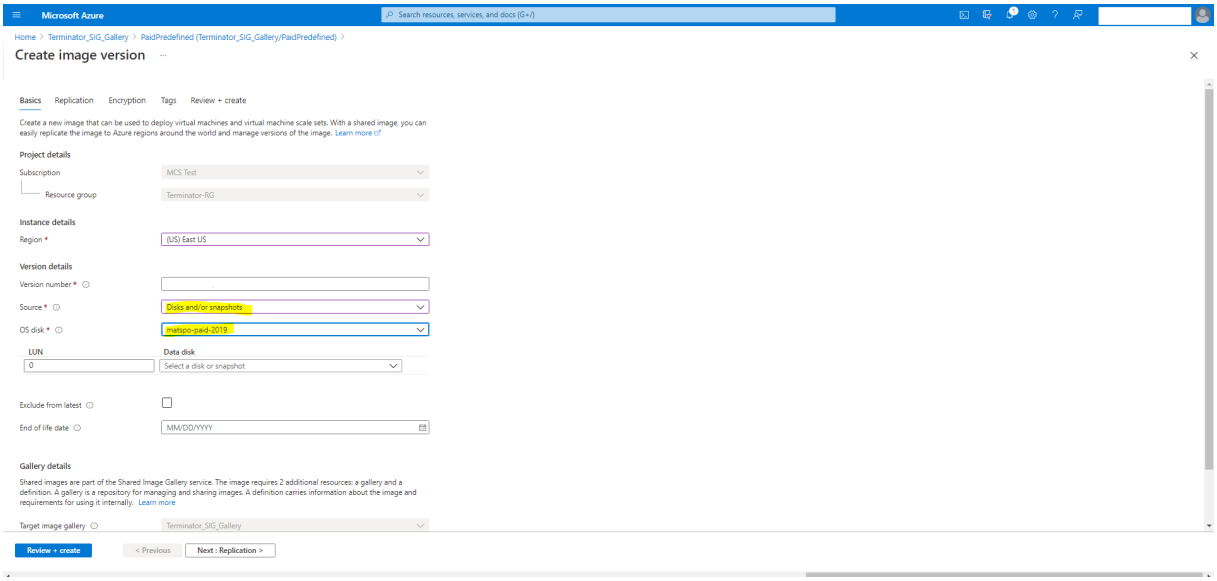



Après avoir vérifié les informations du plan d'achat, créez une version d'image dans la définition. Elle est utilisée comme image principale. Cliquez sur **Ajouter une version** :




Dans la section **Détails de la version**, sélectionnez l'instantané d'image ou le disque géré comme source :




## Créer un catalogue de machines à l'aide de PowerShell

Cette section explique comment créer des catalogues à l'aide de PowerShell :

- Créer un catalogue avec disque de cache en écriture non persistant
- Créer un catalogue avec disque de cache en écriture persistant
- Améliorer les performances de démarrage avec MCSIO
- Utiliser une spécification de modèle lors de la création ou de la mise à jour d'un catalogue à l'aide de PowerShell
- Catalogues de machines avec lancement fiable

- Utiliser les valeurs des propriétés du profil machine
- Créer un catalogue de machines avec une clé de chiffrement gérée par le client
- Créer un catalogue de machines avec cryptage double
- Créer un catalogue avec des disques éphémères Azure
- Hôtes dédiés Azure
- Créer ou mettre à jour un catalogue de machines à l'aide d'une image Azure Compute Gallery
- Configurer Azure Shared Image Gallery
- Provisionner des machines dans des zones de disponibilité spécifiées
- Types de stockage
- Emplacement du fichier d'échange
- Mettre à jour les paramètres du fichier d'échange
- Créer un catalogue à l'aide des machines virtuelles Azure Spot
- Configurer les tailles des machines virtuelles de sauvegarde
- Copier les balises sur toutes les ressources
- Provisionner des machines virtuelles de catalogue avec l'agent Azure Monitor installé

### Créer un catalogue avec disque de cache en écriture non persistant

Pour configurer un catalogue avec un disque de cache en écriture différée non persistant, utilisez le paramètre PowerShell <!JEKYLL@5300@47>. La propriété personnalisée <!JEKYLL@5300@48> indique si vous acceptez d'utiliser le stockage temporaire Azure pour stocker le fichier de cache en écriture différée. Elle doit être configurée sur true lors de l'exécution de <!JEKYLL@5300@49> si vous souhaitez utiliser le disque temporaire comme disque de cache en écriture différée. Si cette propriété n'est pas spécifiée, le paramètre est défini sur **False** par défaut.

Exemple d'utilisation du paramètre <!JEKYLL@5300@50> pour définir la valeur <!JEKYLL@5300@51> sur **true** :

<!JEKYLL@5300@52>

> **Remarque :**
>
> Une fois que vous avez validé le catalogue de machines pour utiliser le stockage temporaire local Azure pour le fichier de cache en écriture différée, il ne peut pas être modifié pour utiliser le disque dur virtuel ultérieurement.

### Créer un catalogue avec disque de cache en écriture persistant

Pour configurer un catalogue avec un disque de cache en écriture différée persistant, utilisez le paramètre PowerShell <!JEKYLL@5300@53>. Ce paramètre prend en charge une propriété supplémentaire, <!JEKYLL@5300@54>, utilisée pour déterminer la façon dont le disque de cache en réécriture persiste pour les machines provisionnées avec MCS. La propriété <!JEKYLL@5300@55>

n'est utilisée que lorsque le paramètre <!JEKYLL@5300@56> est spécifié et lorsque le paramètre <!JEKYLL@5300@57> est défini pour indiquer qu'un disque est créé.

Voici des exemples de propriétés du paramètre <!JEKYLL@5300@58> avant la prise en charge de <!JEKYLL@5300@59> :

<!JEKYLL@5300@60>

Lorsque vous utilisez ces propriétés, notez qu'elles contiennent des valeurs par défaut si elles sont omises du paramètre <!JEKYLL@5300@61>. La propriété <!JEKYLL@5300@62> a deux valeurs possibles : **true** ou **false**.

Lorsque la propriété <!JEKYLL@5300@63> est définie sur **true**, le disque de cache en réécriture n'est pas supprimé lorsque l'administrateur Citrix Virtual Apps and Desktops arrête la machine à l'aide de Web Studio.

Lorsque la propriété <!JEKYLL@5300@64> est définie sur **false**, le disque de cache en réécriture est supprimé lorsque l'administrateur Citrix Virtual Apps and Desktops arrête la machine à l'aide de Web Studio.

> **Remarque :**
>
> Si la propriété <!JEKYLL@5300@65> est omise, la propriété est **false** par défaut et le cache de réécriture est supprimé lors de l'arrêt de la machine à l'aide de Web Studio.

Par exemple, utilisation du paramètre <!JEKYLL@5300@66> pour définir la valeur <!JEKYLL@5300@67> sur true :

<!JEKYLL@5300@68>

> **Important :**
>
> La propriété <!JEKYLL@5300@69> ne peut être définie qu'à l'aide de l'applet de commande PowerShell <!JEKYLL@5300@70>. La tentative de modification de <!JEKYLL@5300@71> pour un schéma de provisioning après la création n'a aucun impact sur le catalogue de machines et la persistance du disque de cache en réécriture lors de l'arrêt d'une machine.

Par exemple, définissez <!JEKYLL@5300@72>pour utiliser le cache en réécriture tout en définissant la propriété <!JEKYLL@5300@73> sur true :

<!JEKYLL@5300@74>

### Améliorer les performances de démarrage avec MCSIO

Vous pouvez améliorer les performances de démarrage des disques gérés par Azure et GCP lorsque MCSIO est activé. Utilisez la propriété personnalisée <!JEKYLL@5300@75> PowerShell dans la

commande <!JEKYLL@5300@76> pour configurer cette fonctionnalité. Les options associées à <!JEKYLL@5300@77> incluent :

<!JEKYLL@5300@78><!JEKYLL@5300@79><!JEKYLL@5300@80>

Pour activer cette fonctionnalité, définissez la propriété personnalisée <!JEKYLL@5300@81> sur <!JEKYLL@5300@82>. Par exemple :

<!JEKYLL@5300@83>

### Utiliser une spécification de modèle lors de la création ou de la mise à jour d'un catalogue à l'aide de PowerShell

Vous pouvez créer ou mettre à jour un catalogue de machines MCS à l'aide d'une spécification de modèle comme entrée de profil de machine. Pour ce faire, vous pouvez utiliser les commandes Web Studio ou PowerShell.

Pour Web Studio, voir Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans Web Studio.

Utilisation des commandes PowerShell :

1. Ouvrez la fenêtre **PowerShell**.
2. Exécutez <!JEKYLL@5300@84>.
3. Créez ou mettez à jour un catalogue.
    - Pour créer un catalogue :
        a) Utilisez la commande <!JEKYLL@5300@85> avec une spécification de modèle comme entrée de profil de machine. Par exemple :
        <!JEKYLL@5300@86>
        b) Terminez la création du catalogue.
    - Pour mettre à jour un catalogue, utilisez la commande <!JEKYLL@5300@87> avec une spécification de modèle comme entrée de profil de machine. Par exemple :
    <!JEKYLL@5300@88>

### Catalogues de machines avec lancement fiable

Pour créer un catalogue de machines avec le lancement fiable, utilisez :

- Un profil de machine avec lancement fiable
- Une taille de machine virtuelle qui prend en charge le lancement fiable
- Une version de machine virtuelle Windows qui prend en charge le lancement fiable. Actuellement, Windows 10, Windows 11, Windows Server 2016, 2019 et 2022 prennent en charge le lancement fiable.

> **Important :**
>
> MCS prend en charge la création d'un catalogue avec des machines virtuelles compatibles avec le lancement fiable. Cependant, pour mettre à jour un catalogue persistant existant et des machines virtuelles existantes, vous devez utiliser le portail Azure. Vous ne pouvez pas mettre à jour le lancement fiable d'un catalogue non persistant. Pour plus d'informations, consultez le document Microsoft Activez le lancement fiable sur une machine virtuelle existante.

Pour afficher les éléments d'inventaire Citrix Virtual Apps and Desktops et pour déterminer si la taille de machine virtuelle prend en charge le lancement fiable, exécutez la commande suivante :

1. Ouvrez une fenêtre PowerShell.
2. Exécutez **asnp citrix*** pour charger des modules PowerShell spécifiques à Citrix.
3. Exécutez la commande suivante :

   <!JEKYLL@5300@89>
4. Exécutez <!JEKYLL@5300@90>.
5. Vérifiez la valeur de l'attribut <!JEKYLL@5300@91>.
   - Si la valeur de <!JEKYLL@5300@92> est **True**, la taille de machine virtuelle prend en charge le lancement fiable.
   - Si la valeur de <!JEKYLL@5300@93> est **False**, la taille de machine virtuelle ne prend pas en charge le lancement fiable.

Avec Azure PowerShell, vous pouvez utiliser la commande suivante pour déterminer les tailles de machine virtuelle qui prennent en charge le lancement fiable :

<!JEKYLL@5300@94>

Vous trouverez ci-dessous des exemples qui indiquent si la taille de machine virtuelle prend en charge le lancement fiable après avoir exécuté la commande Azure PowerShell.

- *Exemple 1* : si la machine virtuelle Azure prend uniquement en charge la génération 1, elle ne prend pas en charge le lancement fiable. Par conséquent, la fonctionnalité <!JEKYLL@5300@95> n'est pas affichée après l'exécution de la commande Azure PowerShell.
- *Exemple 2* : si la machine virtuelle Azure prend uniquement en charge la génération 2 et que la fonctionnalité <!JEKYLL@5300@96> est **True**, la taille de machine virtuelle de génération 2 ne prend pas en charge le lancement fiable.
- *Exemple 3* : si la machine virtuelle Azure prend uniquement en charge la génération 2 et que la fonctionnalité <!JEKYLL@5300@97> n'est pas affichée après l'exécution de la commande PowerShell, la taille de machine virtuelle de génération 2 prend en charge le lancement fiable.

Pour plus d'informations sur le lancement fiable pour les machines virtuelles Azure, consultez le document Microsoft Lancement fiable pour les machines virtuelles Azure.

### Créer un catalogue de machines avec lancement fiable

1. Créez une image principale compatible avec le lancement fiable. Consultez la documentation Microsoft Images de machine virtuelle de lancement fiable.
2. Créez une machine virtuelle ou une spécification de modèle avec le type de sécurité **machines virtuelles de lancement fiable**. Pour plus d'informations sur la création d'une machine virtuelle ou d'une spécification de modèle, consultez le document Microsoft Déployer une machine virtuelle de lancement fiable.
3. Créez un catalogue de machines à l'aide de Web Studio ou des commandes PowerShell.
   - Si vous souhaitez utiliser Web Studio, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans Web Studio.
   - Si vous souhaitez utiliser des commandes PowerShell, utilisez la commande <!JEKYLL@5300@98> avec la machine virtuelle ou la spécification de modèle comme entrée de profil de machine. Pour obtenir la liste complète des commandes permettant de créer un catalogue, consultez la section Création d'un catalogue.

     Exemple de commande <!JEKYLL@5300@99> avec une machine virtuelle comme entrée de profil de machine :

     <!JEKYLL@5300@100>

     Exemple de commande <!JEKYLL@5300@101> avec une spécification de modèle comme entrée de profil de machine :

     <!JEKYLL@5300@102>

### Erreurs lors de la création de catalogues de machines avec le lancement fiable

Vous obtenez les erreurs appropriées dans les scénarios suivants lors de la création d'un catalogue de machines avec le lancement fiable :

| Scénario | Erreur |
| --- | --- |
| Si vous sélectionnez un profil de machine lors de la création d'un catalogue non géré | <!JEKYLL@5300@103> |
| Si vous sélectionnez un profil de machine prenant en charge le lancement fiable lors de la création d'un catalogue avec un disque non géré comme image principale | <!JEKYLL@5300@104> |

| Scénario | Erreur |
| --- | --- |
| Si vous ne sélectionnez pas de profil de machine lors de la création d'un catalogue géré avec une source d'image principale avec le lancement fiable comme type de sécurité | <!JEKYLL@5300@105> |
| Si vous sélectionnez un profil de machine avec un type de sécurité différent du type de sécurité de l'image principale | <!JEKYLL@5300@106> |
| Si vous sélectionnez une taille de machine virtuelle qui ne prend pas en charge le lancement fiable mais que vous utilisez une image principale qui prend en charge le lancement fiable lors de la création d'un catalogue | <!JEKYLL@5300@107> |

### Utiliser les valeurs des propriétés du profil machine

Le catalogue de machines utilise les propriétés suivantes qui sont définies dans les propriétés personnalisées :

- Zone de disponibilité
- ID de groupe d'hôtes dédié
- ID de jeu de chiffrement de disque
- Type d'OS
- Type de licence
- Type de stockage

Si ces propriétés personnalisées ne sont pas définies explicitement, les valeurs de propriété sont définies à partir de la spécification du modèle ARM ou de la machine virtuelle, selon celle qui est utilisée comme profil de machine. De plus, si <!JEKYLL@5300@108> n'est pas spécifié, il est défini à partir du profil de la machine.

> **Remarque :**
>
> Si certaines propriétés sont absentes du profil de la machine et ne sont pas définies dans les propriétés personnalisées, les valeurs par défaut de ces propriétés sont appliquées le cas échéant.

La section suivante décrit certains scénarios <!JEKYLL@5300@109> et <!JEKYLL@5300@110> lorsque toutes les propriétés sont définies pour <!JEKYLL@5300@111> ou que les valeurs sont dérivées de MachineProfile.

- Scénarios New-ProvScheme
  - MachineProfile a toutes les propriétés et les propriétés CustomProperties ne sont pas définies. Exemple :

    <!JEKYLL@5300@112>

    Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    <!JEKYLL@5300@113>
  - MachineProfile a certaines propriétés et les propriétés CustomProperties ne sont pas définies. Exemple : MachineProfile a uniquement LicenseType et OSType.

    <!JEKYLL@5300@114>

    Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    <!JEKYLL@5300@115>
  - MachineProfile et CustomProperties définissent toutes les propriétés. Exemple :

    <!JEKYLL@5300@116>

    Les propriétés personnalisées sont prioritaires. Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    <!JEKYLL@5300@117>
  - Certaines propriétés sont définies dans MachineProfile et certaines sont définies dans CustomProperties. Exemple :
    - CustomProperties définit LicenseType et StorageAccountType
    - MachineProfile définit LicenseType, OSType et Zones

    <!JEKYLL@5300@118>

    Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    <!JEKYLL@5300@119>
  - Certaines propriétés sont définies dans MachineProfile et certaines sont définies dans CustomProperties. ServiceOffering n'est pas défini. Exemple :
    - CustomProperties définit StorageType
    - MachineProfile définit LicenseType

    <!JEKYLL@5300@120>

Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

<!JEKYLL@5300@121>

- Si OSType ne figure ni dans CustomProperties ni dans MachineProfile, alors :
  - La valeur est lue à partir de l'image principale.
  - Si l'image principale est un disque non géré, OSType est défini sur Windows. Exemple :

<!JEKYLL@5300@122>

La valeur de l'image principale est écrite dans les propriétés personnalisées, dans ce cas Linux.

<!JEKYLL@5300@123>

- Scénarios Set-ProvScheme
  - Un catalogue existant avec :
    - CustomProperties pour <!JEKYLL@5300@124> et OSType
    - MachineProfile <!JEKYLL@5300@125> qui définit les zones
  - Mises à jour :
    - MachineProfile mpB.machine virtuelle qui définit StorageAccountType
    - Un nouveau jeu de propriétés personnalisées $CustomPropertiesB qui définit LicenseType et OSType

<!JEKYLL@5300@126>

Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

<!JEKYLL@5300@127>

  - Un catalogue existant avec :
    - CustomProperties pour S<!JEKYLL@5300@128> et OSType
    - MachineProfile <!JEKYLL@5300@129> qui définit StorageAccountType et LicenseType
  - Mises à jour :
    - Un nouveau jeu de propriétés personnalisées $CustomPropertiesB qui définit StorageAccountType et OSType

<!JEKYLL@5300@130>

Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

<!JEKYLL@5300@131>

- Un catalogue existant avec :
  - CustomProperties pour <!JEKYLL@5300@132> et OSType
  - MachineProfile <!JEKYLL@5300@133> qui définit les zones
- Mises à jour :
  - MachineProfile mpB.machine virtuelle qui définit StorageAccountType et LicenseType
  - <!JEKYLL@5300@134> n'est pas spécifié

<!JEKYLL@5300@135>

Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

<!JEKYLL@5300@136>

## Provisionner des machines virtuelles de catalogue avec l'agent Azure Monitor installé

Le service de surveillance Azure vous permet de collecter, d'analyser et d'exploiter des données de télémétrie provenant de vos environnements Azure et locaux.

L'agent Azure Monitor Agent (AMA) collecte les données de surveillance à partir de ressources de calcul telles que des machines virtuelles et les transmet à Azure Monitor. Il prend actuellement en charge la collecte des journaux d'événements, du syslog et des métriques de performance et les envoie aux sources de données Azure Monitor Metrics et Azure Monitor Logs.

Pour surveiller en identifiant de manière unique les machines virtuelles dans les données de surveillance, vous pouvez provisionner les machines virtuelles d'un catalogue de machines MCS avec l'agent AMA installé en tant qu'extension.

### Exigences

- Autorisations : assurez-vous de disposer des autorisations Azure minimales spécifiées dans la section Autorisations Azure requises et des autorisations suivantes pour utiliser Azure Monitor :
  - <!JEKYLL@5300@137>
  - <!JEKYLL@5300@138>
  - <!JEKYLL@5300@139>
  - <!JEKYLL@5300@140>
  - <!JEKYLL@5300@141>

- Règle de collecte de données : configurez une règle de collecte de données dans le portail Azure. Pour plus d'informations sur la configuration d'une règle de collecte de données, consultez la section Créer une règle de collecte de données. Une règle de collecte de données est spécifique à une plate-forme (Windows ou Linux). Assurez-vous de créer une règle pour la plate-forme requise.
  L'agent AMA utilise des règles de collecte de données (DCR) pour gérer le mappage entre les ressources, telles que les machines virtuelles, et les sources de données, telles qu'Azure Monitor Metrics et Azure Monitor Logs.
- Espace de travail par défaut : créez un espace de travail dans le portail Azure. Pour plus d'informations sur la création d'un espace de travail, voir Créer un espace de travail Log Analytics. Lorsque vous collectez des journaux et des données, les informations sont stockées dans un espace de travail. Un espace de travail possède un identifiant d'espace de travail et un identifiant de ressource uniques. Le nom de l'espace de travail doit être unique pour un groupe de ressources donné. Après avoir créé un espace de travail, configurez les sources de données et les solutions pour stocker leurs données dans l'espace de travail.
- Extension Monitor ajoutée à la liste blanche : les extensions <!JEKYLL@5300@142> et <!JEKYLL@5300@143> sont des extensions sur liste blanche définies par Citrix. Pour afficher la liste des extensions figurant sur la liste blanche, utilisez la commande PoSH, <!JEKYLL@5300@144>.
- Image principale : Microsoft recommande de supprimer les extensions d'une machine existante avant d'en créer une nouvelle à partir de celle-ci. Si les extensions ne sont pas supprimées, des fichiers peuvent rester et un comportement inattendu peut se produire. Pour plus d'informations, consultez Si la machine virtuelle est recréée à partir d'une machine virtuelle existante.

Pour provisionner des machines virtuelles de catalogue avec l'agent AMA activé :

1. Configurez un modèle de profil de machine.
   - Si vous souhaitez utiliser une machine virtuelle comme modèle de profil de machine :
     a) Créez une machine virtuelle dans le portail Azure.
     b) Allumez la machine virtuelle.
     c) Ajoutez la machine virtuelle à la règle de collecte de données sous **Ressources**. Cela appelle l'installation de l'agent sur la machine virtuelle modèle.

     > **Remarque :**
     >
     > Si vous devez créer un catalogue Linux, configurez une machine Linux.

   - Si vous souhaitez utiliser une spécification de modèle comme modèle de profil de machine :
     a) Configurez une spécification de modèle.

b) Ajoutez l'association d'extension et de règle de collecte de données suivantes à la spécification de modèle générée :

<!JEKYLL@5300@145>

2. Créez ou mettez à jour un catalogue de machines MCS existant.

   - Pour créer un nouveau catalogue MCS :

     a) Sélectionnez cette machine virtuelle ou une spécification de modèle en tant que profil de machine dans Web Studio.
     b) Procédez aux étapes suivantes pour créer le catalogue.

   - Pour mettre à jour un catalogue MCS existant, utilisez les commandes PoSH suivantes :

     – Pour que les nouvelles machines virtuelles obtiennent le modèle de profil de machine mis à jour, exécutez la commande suivante :

       <!JEKYLL@5300@146>

     – Pour mettre à jour les machines virtuelles existantes avec le modèle de profil de machine mis à jour :

       <!JEKYLL@5300@147>

3. Allumez les machines virtuelles du catalogue.
4. Accédez au portail Azure et vérifiez si l'extension Monitor est installée sur la machine virtuelle et si la machine virtuelle apparaît sous les ressources de DCR. Après quelques minutes, les données de surveillance s'affichent sur Azure Monitor.

#### Dépannage

Pour des conseils de dépannage pour Azure Monitor Agent, consultez :

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

### Créer un catalogue de machines avec une clé de chiffrement gérée par le client

Les étapes détaillées pour créer un catalogue de machines avec une clé de chiffrement gérée par le client sont les suivantes :

1. Ouvrez une fenêtre PowerShell.

2. Exécutez <!JEKYLL@5300@148> pour charger des modules PowerShell propres à Citrix.
3. Entrez <!JEKYLL@5300@149>.
4. Entrez <!JEKYLL@5300@150>.
5. Entrez <!JEKYLL@5300@151>.
6. Entrez <!JEKYLL@5300@152> pour obtenir la liste des jeux de chiffrement de disque.
7. Copiez l'ID d'un jeu de chiffrement de disque.
8. Créez une chaîne de propriétés personnalisée pour inclure l'ID du jeu de chiffrement de disque. Par exemple :

   <!JEKYLL@5300@153>
9. Créez un pool d'identités s'il n'a pas déjà été créé. Par exemple :

   <!JEKYLL@5300@154>
10. Exécutez la commande New-ProvScheme. Par exemple :

    <!JEKYLL@5300@155>
11. Terminez la création du catalogue de machines.

### Créer un catalogue de machines avec cryptage double

Vous pouvez créer et mettre à jour un catalogue de machines utilisant un chiffrement double à l'aide de Web Studio et de commandes PowerShell.

Les étapes détaillées pour créer un catalogue de machines avec chiffrement double sont les suivantes :

1. Créez une instance Azure Key Vault et un jeu de chiffrement de disque avec des clés gérées par la plate-forme et gérées par le client. Pour plus d'informations sur la création d'une instance Azure Key Vault et d'un jeu de chiffrement de disque (DES), consultez la section Utiliser le portail Azure pour activer le chiffrement double au repos pour les disques gérés.
2. Pour parcourir les jeux de chiffrement de disque disponibles dans votre connexion d'hébergement, procédez comme suit :

   a) Ouvrez une fenêtre **PowerShell**.
   b) Exécutez les commandes PowerShell suivantes :
      i. <!JEKYLL@5300@156>
      ii. <!JEKYLL@5300@157>
      iii. <!JEKYLL@5300@158>
      iv. <!JEKYLL@5300@159> (par exemple, azure-east)

v. <!JEKYLL@5300@160>
vi. <!JEKYLL@5300@161>

Vous pouvez utiliser un identifiant de <!JEKYLL@5300@162> pour créer ou mettre à jour un catalogue à l'aide de propriétés personnalisées.

3. Si vous souhaitez utiliser le workflow du profil de machine, créez une machine virtuelle ou une spécification de modèle en tant qu'entrée de profil de machine.

   - Si vous souhaitez utiliser une machine virtuelle comme entrée de profil de machine :
     a) Créez une machine virtuelle dans le portail Azure.
     b) Accédez à **Disques > Gestion des clés** pour chiffrer la machine virtuelle directement avec n'importe quel <!JEKYLL@5300@163>.
   - Si vous souhaitez utiliser une spécification de modèle comme entrée de profil de machine :
     a) Dans le modèle, sous <!JEKYLL@5300@164>, ajoutez un paramètre <!JEKYLL@5300@165> et ajoutez l'identifiant du jeu de chiffrement de disque utilisant le chiffrement double.

4. Créez le catalogue de machines.

   - Si vous utilisez Web Studio, effectuez l'une des opérations suivantes en plus des étapes décrites dans la section Créer des catalogues de machines.
     - Si vous n'utilisez pas de workflow basé sur le profil de la machine, sur la page **Paramètres du disque**, sélectionnez **Utilisez la clé suivante pour chiffrer les données sur chaque machine**. Sélectionnez ensuite le chiffrement de disque utilisant le chiffrement double dans la liste déroulante. Continuez à créer le catalogue.
     - Si vous utilisez le workflow basé sur le profil de la machine, sur la page **Image**, sélectionnez une image principale et un profil de machine. Assurez-vous que le profil de la machine est associé à un identifiant de jeu de chiffrement de disque dans ses propriétés.

     Le chiffrement double est appliqué à toutes les machines créées dans le catalogue via la clé associée au jeu de chiffrement de disque que vous avez sélectionné.
   - Si vous utilisez les commandes PowerShell, effectuez l'une des opérations suivantes :
     - Si vous n'utilisez pas de workflow basé sur le profil de la machine, ajoutez la propriété personnalisée <!JEKYLL@5300@166> dans la commande <!JEKYLL@5300@167>. Par exemple :

       <!JEKYLL@5300@168>
     - Si vous utilisez un workflow basé sur le profil de la machine, utilisez une entrée de profil de machine dans la commande <!JEKYLL@5300@169>. Par exemple :

       <!JEKYLL@5300@170>

5. Terminez la création du catalogue à l'aide de Remote PowerShell SDK. Pour plus d'informations sur la création d'un catalogue à l'aide du SDK Remote PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Le chiffrement double est appliqué à toutes les machines créées dans le catalogue via la clé associée au jeu de chiffrement de disque que vous avez sélectionné.

#### Convertir un catalogue non crypté en catalogue avec cryptage double

Vous pouvez mettre à jour le type de chiffrement d'un catalogue de machines (à l'aide de propriétés personnalisées ou d'un profil de machine) uniquement si le catalogue a déjà été déchiffré.

- Si vous n'utilisez pas de workflow basé sur le profil de la machine, ajoutez la propriété personnalisée DiskEncryptionSetId dans la commande <!JEKYLL@5300@171>. Par exemple :

  <!JEKYLL@5300@172>

- Si vous utilisez un workflow basé sur le profil de la machine, utilisez une entrée de profil de machine dans la commande <!JEKYLL@5300@173>. Par exemple :

  <!JEKYLL@5300@174>

Si l'opération réussit, le chiffrement double est appliqué à toutes les nouvelles machines virtuelles que vous ajoutez à votre catalogue via la clé associée au jeu de chiffrement de disque que vous avez sélectionné.

#### Vérifier que le cryptage double est appliqué au catalogue

- Dans Web Studio :

  1. Accédez à **Catalogues de machines**.
  2. Sélectionnez le catalogue que vous souhaitez vérifier. Cliquez sur l'onglet **Propriétés du modèle** situé en bas de l'écran.
  3. Dans **Détails Azure**, vérifiez l'ID du jeu de chiffrement de disque dans **Jeu de chiffrement de disque**. Si l'ID du jeu de chiffrement de disque associé au catalogue est vide, le catalogue n'est pas chiffré.
  4. Dans le portail Azure, vérifiez que le type de cryptage du jeu de cryptage de disque associé à l'ID DES est une clé gérée par la plate-forme et une clé gérée par le client.

- À l'aide de la commande PowerShell :

  1. Ouvrez la fenêtre **PowerShell**.
  2. Exécutez <!JEKYLL@5300@175> pour charger des modules PowerShell propres à Citrix.

3. Utilisez <!JEKYLL@5300@176> pour obtenir les informations de votre catalogue de machines. Par exemple :

   <!JEKYLL@5300@177>

4. Récupérez la propriété personnalisée de l'ID du jeu de chiffrement de disque associé au catalogue de machines. Par exemple :

   <!JEKYLL@5300@178>

5. Dans le portail Azure, vérifiez que le type de cryptage du jeu de cryptage de disque associé à l'ID DES est une clé gérée par la plate-forme et une clé gérée par le client.

## Créer un catalogue avec des disques éphémères Azure

Pour utiliser des disques éphémères, vous devez définir la propriété personnalisée <!JEKYLL@5300@179> sur **true** lors de l'exécution de <!JEKYLL@5300@180>.

> **Remarque :**
>
> Si la propriété personnalisée <!JEKYLL@5300@181> est définie sur **false** ou si une valeur n'est pas spécifiée, tous les VDA provisionnés continuent d'utiliser un disque d'OS provisionné.

Voici un exemple d'ensemble de propriétés personnalisées à utiliser dans le schéma de provisioning :

<!JEKYLL@5300@182>

### Configurer un disque éphémère pour un catalogue

Pour configurer un disque d'OS éphémère Azure pour un catalogue, utilisez le paramètre <!JEKYLL@5300@183> dans <!JEKYLL@5300@184>. Définissez la valeur du paramètre <!JEKYLL@5300@185> sur **true**.

> **Remarque :**
>
> Pour utiliser cette fonctionnalité, vous devez également activer les paramètres <!JEKYLL@5300@186> et <!JEKYLL@5300@187>.

Par exemple :

<!JEKYLL@5300@188>

#### Remarques importantes sur les disques éphémères

Pour provisionner des disques d'OS éphémères en utilisant <!JEKYLL@5300@189>, tenez compte des contraintes suivantes :

- La taille de machine virtuelle utilisée pour le catalogue doit prendre en charge les disques d'OS éphémères.
- La taille du cache ou du disque temporaire associé à la taille de la machine virtuelle doit être supérieure ou égale à la taille du disque d'OS.
- La taille du disque temporaire doit être supérieure à la taille du disque de cache.

Tenez également compte de ces points lors des opérations suivantes :

- Création du schéma de provisioning.
- Modification du schéma de provisioning.
- Mise à jour de l'image.

### Hôtes dédiés Azure

Vous pouvez utiliser MCS pour provisionner des machines virtuelles sur des hôtes dédiés Azure. Avant de provisionner des machines virtuelles sur des hôtes dédiés Azure :

- Créez un groupe d'hôtes.
- Créez des hôtes dans ce groupe d'hôtes.
- Assurez-vous que la capacité des hôtes est suffisante pour la création de catalogues et de machines virtuelles.

Vous pouvez créer un catalogue de machines avec la location d'hôte définie à l'aide du script PowerShell suivant :

<!JEKYLL@5300@190>

Lorsque vous utilisez MCS pour provisionner des machines virtuelles sur des hôtes dédiés Azure, tenez compte des éléments suivants :

- Un *hôte dédié* est une propriété de catalogue et ne peut pas être modifié une fois le catalogue créé. La location dédiée n'est actuellement pas prise en charge sur Azure.
- Un groupe d'hôtes Azure préconfiguré, dans la région de l'unité d'hébergement, est requis lors de l'utilisation du paramètre <!JEKYLL@5300@191>.
- Le placement automatique Azure est requis. Cette fonctionnalité effectue une demande d'intégration à l'abonnement associé au groupe d'hôtes. Pour plus d'informations, consultez Échelle MV définie sur les hôtes dédiés Azure - Version préliminaire publique. Si le placement automatique n'est pas activé, MCS génère une erreur lors de la création du catalogue.

### Créer ou mettre à jour un catalogue de machines à l'aide d'une image Azure Compute Gallery

Lorsque vous sélectionnez une image à utiliser pour créer un catalogue de machines, vous pouvez sélectionner les images que vous avez créées dans Azure Compute Gallery.

Pour que ces images apparaissent, vous devez :

1. Configurer un site Citrix Virtual Apps and Desktops.
2. Connectez-vous à Azure Resource Manager.
3. Dans le portail Azure, créez un groupe de ressources. Pour plus d'informations, consultez Créer une instance Azure Compute Gallery à l'aide du portail.
4. Dans le groupe de ressources, créez une instance Azure Compute Gallery.
5. Dans Azure Compute Gallery, créez une définition d'image.
6. Dans la définition de l'image, créez une version d'image.

Utilisez les commandes PowerShell suivantes pour créer ou mettre à jour un catalogue de machines à l'aide d'une image provenant d'Azure Compute Gallery :

1. Ouvrez une fenêtre PowerShell.
2. Exécutez <!JEKYLL@5300@192> pour charger des modules PowerShell propres à Citrix.
3. Sélectionnez un groupe de ressources, puis répertoriez toutes les galeries de ce groupe de ressources.

   <!JEKYLL@5300@193>

4. Sélectionnez une galerie, puis répertoriez toutes les définitions d'images de cette galerie.

   <!JEKYLL@5300@194>

5. Sélectionnez une définition d'image, puis répertoriez toutes les versions d'image de cette définition d'image.

   <!JEKYLL@5300@195>

6. Créez et mettez à jour un catalogue MCS à l'aide des éléments suivants :

   - Groupe de ressources
   - Galerie
   - Définition de l'image de la galerie
   - Version d'image de la galerie

   Pour plus d'informations sur la création d'un catalogue à l'aide du SDK Remote PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

### Configurer Azure Shared Image Gallery

Utilisez la commande <!JEKYLL@5300@196> pour créer un schéma de provisioning avec la prise en charge de Shared Image Gallery. Utilisez la commande <!JEKYLL@5300@197> pour activer ou désactiver cette fonctionnalité pour un schéma de provisioning et pour modifier le ratio de réplica et les valeurs maximales de réplicas.

Trois propriétés personnalisées ont été ajoutées aux schémas de provisioning pour prendre en charge la fonctionnalité Shared Image Gallery :

<!JEKYLL@5300@198>

- Indique si vous souhaitez utiliser Shared Image Gallery pour stocker les images publiées. Si cette propriété est définie sur **True**, l'image est stockée en tant qu'image Shared Image Gallery, sinon l'image est stockée sous la forme d'un instantané.
- Les valeurs valides sont **True** et **False**.
- Si la propriété n'est pas définie, la valeur par défaut est **False**.

<!JEKYLL@5300@199>

- Définit le ratio entre les machines et les réplicas de version d'image de la galerie.
- Les valeurs valides sont des nombres entiers supérieurs à 0.
- Si la propriété n'est pas définie, les valeurs par défaut sont utilisées. La valeur par défaut pour les disques du système d'exploitation persistants est de 1 000 ; la valeur par défaut pour les disques du système d'exploitation non persistants est de 40.

<!JEKYLL@5300@200>

- Définit le nombre maximal de réplicas pour chaque version d'image de la galerie.
- Les valeurs valides sont des nombres entiers supérieurs à 0.
- Si la propriété n'est pas définie, la valeur par défaut est 10.
- Azure prend actuellement en charge jusqu'à 10 réplicas pour une version unique d'image de la galerie. Si la propriété est définie sur une valeur supérieure à celle prise en charge par Azure, MCS tente d'utiliser la valeur spécifiée. Azure génère une erreur, que MCS consigne, puis laisse le nombre de réplicas actuel inchangé.

> **Conseil :**
>
> Lors de l'utilisation de Shared Image Gallery pour stocker une image publiée pour les catalogues provisionnés avec MCS, MCS définit le nombre de réplicas de version d'image de galerie en fonction du nombre de machines dans le catalogue, du ratio de réplica et du maximum de réplicas. Le nombre de réplicas est calculé en divisant le nombre de machines du catalogue par le ratio de réplica (arrondi à la valeur entière la plus proche), puis en plafonnant la valeur au nombre maximal de réplicas. Par exemple, avec un ratio de réplica de 20 et un maximum de 5, 0 à 20

> machines ont un réplica, 21—40 ont 2 réplicas, 41—60 ont 3 réplicas, 61 à 80 ont 4 réplicas, 81+ 5 réplicas.

### Cas d'utilisation : mise à jour du ratio de réplica Shared Image Gallery et du maximum de réplicas

Le catalogue de machines existant utilise Shared Image Gallery. Utilisez la commande <!JEKYLL@5300@201> pour mettre à jour les propriétés personnalisées de toutes les machines existantes du catalogue et de toutes les futures machines :

<!JEKYLL@5300@202>

### Cas d'utilisation : conversion d'un catalogue d'instantanés en catalogue Shared Image Gallery

Pour ce cas d'utilisation :

1. Exécutez <!JEKYLL@5300@203> avec l'indicateur <!JEKYLL@5300@204> défini sur **True**. Vous pouvez également inclure les propriétés <!JEKYLL@5300@205> et <!JEKYLL@5300@206>.
2. Mettez le catalogue à jour.
3. Effectuez un cycle d'alimentation sur les machines pour forcer une mise à jour.

Par exemple :

<!JEKYLL@5300@207>

> **Conseil :**
>
> Les paramètres <!JEKYLL@5300@208> et <!JEKYLL@5300@209> ne sont pas obligatoires. Une fois la commande <!JEKYLL@5300@210> terminée, l'image Shared Image Gallery n'a pas encore été créée. Une fois que le catalogue est configuré pour utiliser la galerie, l'opération suivante de mise à jour du catalogue stocke l'image publiée dans la galerie. La commande de mise à jour du catalogue crée la galerie, l'image de la galerie et la version de l'image. Le cycle d'alimentation des machines les met à jour, et le nombre de réplicas est mis à jour, le cas échéant. À partir de ce moment, toutes les machines non persistantes existantes sont réinitialisées à l'aide de l'image Shared Image Gallery et toutes les machines nouvellement provisionnées sont créées à l'aide de l'image. L'ancien instantané est nettoyé automatiquement en quelques heures.

### Cas d'utilisation : conversion d'un catalogue Shared Image Gallery en catalogue d'instantanés

Pour ce cas d'utilisation :

1. Exécutez <!JEKYLL@5300@211> avec l'indicateur <!JEKYLL@5300@212> défini sur **False** ou non défini.

2. Mettez le catalogue à jour.
3. Effectuez un cycle d'alimentation sur les machines pour forcer une mise à jour.

Par exemple :

<!JEKYLL@5300@213>

> **Conseil :**
>
> Contrairement à la mise à jour d'un instantané vers un catalogue Shared Image Gallery, les données personnalisées de chaque machine ne sont pas encore mises à jour pour refléter les nouvelles propriétés personnalisées. Exécutez la commande suivante pour afficher les propriétés personnalisées Shared Image Gallery d'origine : <!JEKYLL@5300@214>. Une fois la commande <!JEKYLL@5300@215> terminée, l'instantané de l'image n'a pas encore été créé. Une fois que le catalogue est configuré pour ne pas utiliser la galerie, la prochaine opération de mise à jour du catalogue stocke l'image publiée sous forme d'instantané. À partir de ce moment, toutes les machines non persistantes existantes sont réinitialisées à l'aide de l'instantané et toutes les machines nouvellement provisionnées sont créées à partir de l'instantané. Le cycle d'alimentation des machines les met à jour, et les données de machine personnalisées sont mises à jour pour refléter que <!JEKYLL@5300@216> est défini sur **False**. Les anciennes ressources Shared Image Gallery (galerie, image et version) sont automatiquement nettoyées en quelques heures.

## Provisionner des machines dans des zones de disponibilité spécifiées

Vous pouvez provisionner des machines dans une zone de disponibilité spécifique dans les environnements Azure. Vous pouvez pour cela utiliser PowerShell.

> **Remarque :**
>
> Si aucune zone n'est spécifiée, MCS laisse Azure placer les machines dans la région. Si plusieurs zones sont spécifiées, MCS distribue les machines de manière aléatoire dans ces zones.

### Configurer des zones de disponibilité via PowerShell

À l'aide de PowerShell, vous pouvez afficher les éléments d'inventaire de l'offre en utilisant <!JEKYLL@5300@217>. Par exemple, pour consulter l'offre de services de la *région États-Unis de l'Est* <!JEKYLL@5300@218> :

<!JEKYLL@5300@219>

Pour afficher les zones, utilisez le paramètre <!JEKYLL@5300@220> de l'élément :

<!JEKYLL@5300@221>

Si les zones de disponibilité ne sont pas spécifiées, les machines sont provisionnées de la même façon.

Pour configurer les zones de disponibilité via PowerShell, utilisez la propriété personnalisée **Zones** disponible avec l'opération <!JEKYLL@5300@222>. La propriété **Zones** définit une liste de zones de disponibilité dans lesquelles provisionner les machines. Ces zones peuvent inclure une ou plusieurs zones de disponibilité. Par exemple, <!JEKYLL@5300@223> pour les zones 1 et 3.

Utilisez la commande <!JEKYLL@5300@224> pour mettre à jour les zones d'un schéma de provisioning.

Si une zone non valide est fournie, le schéma de provisioning n'est pas mis à jour et un message d'erreur apparaît indiquant comment corriger la commande non valide.

> **Conseil :**
>
> Si vous spécifiez une propriété personnalisée non valide, le schéma de provisioning n'est pas mis à jour et un message d'erreur correspondant s'affiche.

### Types de stockage

Sélectionnez différents types de stockage pour les machines virtuelles dans des environnements Azure utilisant MCS. Pour les machines virtuelles cibles, MCS prend en charge :

- Disque d'OS : SSD premium, SSD ou HDD
- Disque de cache en écriture différée : SSD premium, SSD ou HDD

Lorsque vous utilisez ces types de stockage, tenez compte des points suivants :

- Assurez-vous que votre machine virtuelle prend en charge le type de stockage sélectionné.
- Si votre configuration utilise un disque éphémère Azure, vous ne voyez pas l'option pour le paramètre de disque de cache en écriture différée.

> **Conseil :**
>
> <!JEKYLL@5300@225> est configuré pour un type d'OS et un compte de stockage. <!JEKYLL@5300@226> est configuré pour le type de stockage Cache en écriture différée. Pour un catalogue normal, <!JEKYLL@5300@227> est requis. Si <!JEKYLL@5300@228> n'est pas configuré, <!JEKYLL@5300@229> est utilisé par défaut pour <!JEKYLL@5300@230>.

Si WBCDiskStorageType n'est pas configuré, StorageType est utilisé par défaut pour WBCDiskStorageType.

### Configurer des types de stockage

Pour configurer les types de stockage pour machine virtuelle, utilisez le paramètre <!JEKYLL@5300@231> dans <!JEKYLL@5300@232>. Définissez la valeur du paramètre <!JEKYLL@5300@233> sur l'un des types de stockage pris en charge.

Voici un exemple du paramètre <!JEKYLL@5300@234> dans un schéma de provisioning :

<!JEKYLL@5300@235>

### Activer le stockage redondant interzone

Vous pouvez sélectionner le stockage redondant interzone (ZRS) lors de la création de catalogue. Il réplique de manière synchrone votre disque géré par Azure sur plusieurs zones de disponibilité, ce qui vous permet de récupérer d'une panne dans une zone en utilisant la redondance dans d'autres.

Vous pouvez spécifier **Premium_ZRS** et **StandardSSD_ZRS** dans les propriétés personnalisées du type de stockage. Le stockage ZRS peut être défini à l'aide de propriétés personnalisées existantes ou via le modèle **MachineProfile**. Le stockage ZRS est également compatible avec la commande <!JEKYLL@5300@236> et les paramètres <!JEKYLL@5300@237> et <!JEKYLL@5300@238>. Vous pouvez changer une machine existante d'un stockage LRS vers un stockage ZRS.

**Limitations :**

- Pris en charge uniquement pour les disques gérés
- Compatible uniquement avec les disques SSD (SSD) haut de gamme et standard
- Non compatible avec <!JEKYLL@5300@239>
- Disponible uniquement dans certaines régions.
- Les performances d'Azure diminuent lors de la création de disques ZRS à grande échelle. Par conséquent, lors de la première mise sous tension, allumez les machines par lots plus petits (moins de 300 machines à la fois)

**Définir le stockage redondant interzone comme type de stockage sur disque** Vous pouvez sélectionner le stockage redondant interzone lors de la création initiale du catalogue, ou vous pouvez mettre à jour votre type de stockage dans un catalogue existant.

**Sélectionner le stockage redondant interzone à l'aide des commandes PowerShell** Lorsque vous créez un catalogue dans Azure à l'aide de la commande PowerShell <!JEKYLL@5300@240>, utilisez <!JEKYLL@5300@241> comme valeur dans <!JEKYLL@5300@242>.
Par exemple :

<!JEKYLL@5300@243>

Lorsque vous définissez cette valeur, elle est validée par une API dynamique qui détermine si elle peut être utilisée correctement. Les exceptions suivantes peuvent se produire si l'utilisation de ZRS n'est pas valide pour votre catalogue :

- **StorageTypeAtShutdownNotSupportedForZrsDisks** : la propriété personnalisée StorageTypeatShutdown ne peut pas être utilisée avec le stockage ZRS.
- **StorageAccountTypeNotSupportedInRegion** : cette exception se produit si vous essayez d'utiliser le stockage ZRS dans une région Azure qui ne prend pas en charge ZRS
- **ZrsRequiresManagedDisks** : vous ne pouvez utiliser le stockage redondant interzone qu'avec des disques gérés.

Vous pouvez définir le type de stockage de disque à l'aide des propriétés personnalisées suivantes :

- <!JEKYLL@5300@244>
- <!JEKYLL@5300@245>
- <!JEKYLL@5300@246>

> **Remarque :**
>
> Lors de la création du catalogue, le disque d'OS du profil de machine <!JEKYLL@5300@247> est utilisé si les propriétés personnalisées ne sont pas définies.

## Capturez les paramètres de diagnostic sur les machine virtuelle et les cartes d'interface réseau à partir d'un profil de machine

Vous pouvez capturer les paramètres de diagnostic des machine virtuelle et des cartes d'interface réseau à partir d'un profil de machine au moment de créer un catalogue de machines, de mettre à jour un catalogue de machines existant et de mettre à jour des machine virtuelle existantes.

Vous pouvez créer une spécification de machine virtuelle ou de modèle en tant que source de profil de machine.

### Étapes clés

1. Configurez les identifiants requis dans Azure. Vous devez fournir ces identifiants dans la spécification du modèle.
    - Compte de stockage
    - Espace de travail Log Analytics
    - Espace de noms Event Hub avec tarification standard
2. Créez une source de profil de machine.
3. Créez un nouveau catalogue de machines, mettez à jour un catalogue existant ou mettez à jour des machine virtuelle existantes.

### Configurer les identifiants requis dans Azure

Configurez l'une des options suivantes dans Azure :

- Compte de stockage
- Espace de travail Log Analytics
- Espace de noms Event Hub avec tarification standard

**Configurer un compte de stockage** Créez un compte de stockage standard dans Azure. Dans la spécification du modèle, indiquez <!JEKYLL@5300@248> comme ResourceID complet du compte de stockage.

Une fois que les machine virtuelle sont configurées pour enregistrer les données sur le compte de stockage, les données se trouvent sous le conteneur <!JEKYLL@5300@249>.

**Configurer un espace de travail Log Analytics** Créez un espace de travail Log Analytics. Dans la spécification du modèle, indiquez le ResourceID complet de l'espace de travail Log Analytics tel que le WorkspaceID.

Une fois que les machine virtuelle sont configurées pour enregistrer les données dans l'espace de travail, les données peuvent être interrogées dans Logs in Azure. Vous pouvez exécuter la commande suivante dans Azure, sous Logs, pour afficher le décompte de toutes les mesures enregistrées par une ressource :

'AzureMetrics

**Mettre en place un hub d'événements** Pour configurer un hub d'événements dans le portail Azure, procédez comme suit :

1. Créez un espace de noms pour le hub d'événements avec la tarification standard.
2. Créez un hub d'événements sous l'espace de noms.
3. Cliquez sur **Capturer** dans le hub d'événements. Activez le bouton pour capturer avec le type de sortie Avro.
4. Créez un nouveau conteneur dans un compte de stockage existant pour capturer les journaux.
5. Dans la spécification du modèle, spécifiez le `eventHubAuthorizationRuleId` au format suivant : `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Spécifiez le nom du hub d'événements.

Une fois que les machine virtuelle sont configurées pour enregistrer les données dans le hub d'événements, les données sont capturées dans le conteneur de stockage configuré.

### Créer une source de profil de machine

Vous pouvez créer une spécification de machine virtuelle ou de modèle en tant que source de profil de machine.

**Créer un profil de machine basé sur une machine virtuelle avec des paramètres de diagnostic** Si vous souhaitez créer une machine virtuelle en tant que profil de machine, configurez d'abord les paramètres de diagnostic sur la machine virtuelle modèle elle-même. Vous pouvez consulter les instructions détaillées fournies dans la documentation Microsoft Paramètres de diagnostic dans Azure Monitor.

Vous pouvez exécuter les commandes suivantes pour vérifier que des paramètres de diagnostic sont désormais associés à la machine virtuelle ou à la carte d'interface réseau :

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2659 --resource-type microsoft.network/
    networkInterfaces
<!--NeedCopy-->
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
<!--NeedCopy-->
```

**Créer un modèle de profil de machine basé sur les spécifications avec des paramètres de diagnostic** Si vous souhaitez utiliser une machine virtuelle sur laquelle les paramètres de diagnostic sont déjà activés et l'exporter dans une spécification de modèle ARM, ces paramètres ne seront pas automatiquement inclus dans le modèle. Vous devez ajouter ou modifier manuellement les paramètres de diagnostic dans le modèle ARM.

Toutefois, si vous souhaitez utiliser une machine virtuelle comme profil de machine, MCS veille à ce que les paramètres de diagnostic importants soient capturés avec précision et appliqués aux ressources de votre catalogue MCS.

1. Créez une spécification de modèle standard qui définit une machine virtuelle et une ou plusieurs cartes d'interface réseau.
2. Ajoutez des ressources supplémentaires pour déployer les paramètres de diagnostic conformément à la spécification : Microsoft.Insights DiagnosticSettings. Pour connaître l'étendue, indiquez une machine virtuelle ou une carte d'interface réseau figurant dans le modèle par son nom avec un ID partiel. Par exemple, pour créer des paramètres de diagnostic associés à une machine virtuelle nommée test-VM dans la spécification du modèle, indiquez la portée comme suit :

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

```
<!--NeedCopy-->
```

3. Utilisez la spécification du modèle comme source de profil de machine.

#### Créer ou mettre à jour un catalogue avec des paramètres de diagnostic

Après avoir créé une source de profil de machine, vous pouvez désormais créer un catalogue de machines à l'aide de la commande `New-ProvScheme`, mettre à jour un catalogue de machines existant à l'aide de la commande `Set-ProvScheme` et mettre à jour les machines virtuelles existantes à l'aide de la commande `Request-ProvVMUpdate`.

### Emplacement du fichier d'échange

Dans les environnements Azure, le fichier d'échange est configuré à un emplacement approprié lorsque la machine virtuelle est créée pour la première fois. Le paramètre du fichier d'échange est configuré au format `<page file location>[min size] [max size]` (taille en Mo). Pour plus d'informations, consultez le document Microsoft Déterminer la taille du fichier d'échange appropriée.

Lorsque vous créez `ProvScheme` pendant la préparation de l'image, MCS détermine l'emplacement du fichier d'échange en fonction de certaines règles. Après avoir créé `ProvScheme` :

- La modification de la taille de la machine virtuelle est bloquée si la taille de la machine virtuelle entrante entraîne une modification du paramètre du fichier d'échange.
- La mise à jour du profil de la machine est bloquée si l'offre de service est modifiée en raison de la mise à jour du profil de la machine qui entraîne une modification des paramètres du fichier d'échange.
- Les propriétés du disque OS éphémère (EOS) et du MCSIO ne peuvent pas être modifiées.

#### Détermination de l'emplacement du fichier de page

Les fonctionnalités telles que EOS et MCSIO disposent de leur propre emplacement de fichier d'échange attendu et s'excluent mutuellement. Le tableau indique l'emplacement attendu du fichier d'échange pour chaque fonctionnalité :

| Fonctionnalité | Emplacement attendu du fichier d'échange |
|---|---|
| EOS | Disque OS |
| MCSIO | Disque temporaire Azure en premier lieu, puis disque de cache en écriture différée |

> **Remarque :**
>
> Même si la préparation de l'image est déconnectée de la création du schéma de provisioning, MCS détermine correctement l'emplacement du fichier d'échange. Le fichier d'échange par défaut se trouve sur le disque du système d'exploitation.

**Scénarios de configuration du fichier de page**

Le tableau décrit certains scénarios possibles de configuration du fichier d'échange lors de la préparation de l'image et de la mise à jour du schéma de provisioning :

| Pendant | Scénario | Résultat |
|---|---|---|
| Préparation de l'image | Le fichier d'échange de l'image source est défini sur le disque temporaire, tandis que la taille de machine virtuelle spécifiée dans le schéma de provisioning ne dispose pas de disque temporaire. | Le fichier d'échange est placé sur le disque du système d'exploitation. |
| Préparation de l'image | Le fichier d'échange de l'image source est défini sur le disque du système d'exploitation, tandis que la taille de la machine virtuelle spécifiée dans le schéma de provisioning dispose d'un disque temporaire. | Le fichier d'échange est placé sur le disque temporaire. |
| Préparation de l'image | Le fichier d'échange de l'image source est défini sur le disque temporaire, tandis que le disque éphémère du système d'exploitation est activé dans le schéma de provisioning. | Le fichier d'échange est placé sur le disque du système d'exploitation. |

| Pendant | Scénario | Résultat |
| --- | --- | --- |
| Mise à jour du schéma de provisioning | Vous essayez de mettre à jour le schéma de provisioning, la taille de la machine virtuelle d'origine dispose d'un disque temporaire et la machine virtuelle cible ne dispose pas de disque temporaire. | Rejette la modification avec un message d'erreur. |
| Mise à jour du schéma de provisioning | Vous essayez de mettre à jour le schéma de provisioning, la taille de la machine virtuelle d'origine ne dispose pas de disque temporaire et la machine virtuelle cible dispose d'un disque temporaire. | Rejette la modification avec un message d'erreur. |

### Mettre à jour les paramètres du fichier d'échange

Vous pouvez également spécifier le paramètre du fichier de page, y compris l'emplacement et la taille, de manière explicite à l'aide de la commande PowerShell. Cela remplace la valeur déterminée par MCS. Pour ce faire, exécutez la commande `New-ProvScheme` et incluez les propriétés personnalisées suivantes :

- `PageFileDiskDriveLetterOverride` : lettre du lecteur de disque de l'emplacement du fichier d'échange
- `InitialPageFileSizeInMB` : taille initiale du fichier d'échange en Mo
- `MaxPageFileSizeInMB` : taille maximale du fichier d'échange en Mo

Exemple d'utilisation des propriétés personnalisées :

```
1 -CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
    /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
    XMLSchema-instance"> `
2 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
    "/> `
3 <Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
4 <Property xsi:type="StringProperty" Name="
    PageFileDiskDriveLetterOverride" Value="d"/> `
5 <Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
    Value="2048"/> `
6 <Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
    ="8196"/> `
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client"/> `
</CustomProperties>'
<!--NeedCopy-->
```

Contraintes :

- Vous pouvez mettre à jour le paramètre du fichier d'échange uniquement lors de la création du schéma de provisioning en exécutant la commande `New-ProvScheme`. Le paramètre du fichier d'échange ne peut pas être modifié ultérieurement.
- Fournissez toutes les propriétés relatives des paramètres du fichier d'échange (`PageFileDiskDriveLet` , `InitialPageFileSizeInMB` et `MaxPageFileSizeInMB`) dans les propriétés personnalisées ou n'en fournissez aucune.
- La taille initiale du fichier d'échange doit être comprise entre 16 Mo et 16777216 Mo.
- La taille maximale du fichier d'échange doit être supérieure ou égale à la taille initiale du fichier d'échange et inférieure à 16777216 Mo.
- Cette fonctionnalité n'est pas prise en charge dans Web Studio.

### Créer un catalogue à l'aide des machines virtuelles Azure Spot

Les machines virtuelles Azure Spot vous permettent d'exploiter la capacité de calcul inutilisée d'Azure tout en réalisant des économies importantes. Toutefois, la possibilité d'allouer une machine virtuelle Azure Spot dépend de la capacité et de la tarification actuelles. Azure peut donc expulser votre machine virtuelle en cours d'exécution, ne pas créer la machine virtuelle ou ne pas la mettre sous tension conformément à la Politique en matière d'expulsion. Par conséquent, les machines virtuelles Azure Spot conviennent à certaines applications et bureaux non essentiels. Pour en savoir plus, consultez Utiliser les machines virtuelles Azure Spot.

#### Limitations

- Toutes les tailles de machines virtuelles ne sont pas prises en charge pour les machines virtuelles Azure Spot. Pour en savoir plus, consultez Limitations.

  Vous pouvez exécuter la commande PowerShell suivante pour vérifier si la taille d'une machine virtuelle prend en charge les machines virtuelles Spot ou non. Si la taille d'une machine virtuelle prend en charge Spot machine virtuelle, la valeur de `SupportsSpotVM` est **Vrai**.

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.
      folder\Standard_D2ds_v4.serviceoffering"). AdditionalData
  <!--NeedCopy-->
  ```

- Actuellement, les machines virtuelles Azure Spot ne prennent pas en charge la mise en veille prolongée.

#### Exigences

Lors de la création de la source du profil de machine (machine virtuelle ou spécification de modèle) pour le catalogue de machines virtuelles Azure Spot, vous devez sélectionner instance Azure Spot (si vous utilisez une machine virtuelle) ou définir `priority` sur `Spot` (si vous utilisez une spécification de modèle).

#### Étapes pour créer un catalogue à l'aide des machines virtuelles Azure Spot

1. Créez une source de profil de machine (machine virtuelle ou modèle de lancement).
   - Pour créer une machine virtuelle à l'aide du portail Azure, consultez Déployer des machines virtuelles Azure Spot à l'aide du portail Azure.
   - Pour créer une spécification de modèle, ajoutez les propriétés suivantes sous **Ressources > type : Microsoft.Compute/VirtualMachines > propriétés** dans la spécification de modèle. Par exemple :

```
"priority": "Spot",
"evictionPolicy": "Deallocate",
"billingProfile": {

"maxPrice": 0.01
 }

<!--NeedCopy-->
```

> **Remarque :**
>
> - La stratégie d'expulsion peut être **Désallouer** ou **Supprimer**.
>   - Pour les machines virtuelles non persistantes, MCS définit toujours la stratégie d'expulsion sur **Supprimer**. Si la machine virtuelle est expulsée, elle et tous les disques non persistants sont supprimés (par exemple, le disque du système d'exploitation). Les disques persistants (par exemple, le disque d'identité) ne sont pas supprimés. Cependant, un disque du système d'exploitation est persistant si le type de catalogue est persistant ou si la propriété personnalisée `PersistOsDisk` est définie sur Vrai. De même, un disque WBC est persistant si la propriété personnalisée `PersistWbc` est définie sur **Vrai**.
>   - Pour les machines virtuelles persistantes, MCS définit toujours la stratégie d'expulsion sur Désallouer. Si la machine virtuelle est expulsée, elle est désallouée.

> Aucune modification n'est apportée aux disques.
> - Le prix maximum est le prix que vous êtes prêt à payer par heure. Si vous utilisez **Capacité seulement**, il s'agit de **-1**. Le prix maximum ne peut être que nul, -1 ou une décimale supérieure à zéro. Pour en savoir plus, consultez Tarification.

2. Vous pouvez exécuter la commande PowerShell suivante pour vérifier si un profil de machine est activé ou non pour les machines virtuelles Azure Spot. Si le paramètre `SpotEnabled` est **Vrai** et que `SpotEvictionPolicy` est défini sur **Désallouer** ou **Supprimer**, le profil de la machine est activé pour les machines virtuelles Azure Spot. Par exemple,

   - Si la source du profil de la machine est une machine virtuelle, exécutez la commande suivante :

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\kb-spot-delete.vm").
       AdditionalData
   <!--NeedCopy-->
   ```

   - Si la source du profil de la machine est une spécification de modèle, exécutez la commande suivante :

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.
       templatespec\14.0.0-spot-delete.templatespecversion").
       AdditionalData
   <!--NeedCopy-->
   ```

3. Créez un catalogue de machines à l'aide d'un profil de machine à l'aide de la commande PowerShell `New-ProvScheme`.

Vous pouvez mettre à jour un catalogue à l'aide de la commande `Set-ProvScheme`. Vous pouvez également mettre à jour les machines virtuelles existantes à l'aide de la commande PowerShell `Set-ProvVmUpdateTimeWindow`. Le profil de la machine est mis à jour lors de la prochaine mise sous tension.

#### Expulsions sur une machine virtuelle Azure Spot en cours d'exécution

Si la capacité informatique n'est pas disponible ou si le prix horaire dépasse le prix maximum configuré, Azure expulse une machine virtuelle Spot en cours d'exécution. Par défaut, vous n'êtes pas averti d'une expulsion. La machine virtuelle se bloque simplement et elle est expulsée. Microsoft recommande d'utiliser les événements planifiés pour surveiller les expulsions. Consultez Surveiller en permanence les expulsions. Vous pouvez également exécuter des scripts depuis une machine virtuelle pour recevoir une notification avant l'expulsion. Par exemple, Microsoft dispose d'un script de sondage dans Python, ScheduledEvents.cs.

**Dépannage**

- Vous pouvez voir les propriétés de la machine virtuelle Spot dans les données customMachineData de la machine virtuelle provisionnée à l'aide de la commande `Get-ProvVM`. Si le champ de priorité est défini sur **Spot**, cela signifie que Spot est utilisé.
- Vous pouvez vérifier si une machine virtuelle utilise Spot dans Azure Portal :
  1. Trouvez la machine virtuelle dans Azure Portal.
  2. Accédez à la page **Présentation**.
  3. Faites défiler l'écran vers le bas et localisez la section **Azure Spot**.
     - Si Spot n'est pas utilisé, ce champ est vide.
     - Si Spot est utilisé, les champs **Azure Spot** et **Politique en matière d'expulsion d'Azure Spot** sont définis.

1. Vous pouvez vérifier le profil de facturation ou le prix maximum par heure de la machine virtuelle sur la page de configuration.

## Configurer les tailles des machines virtuelles de sauvegarde

Les clouds publics peuvent parfois manquer de capacité pour une certaine taille de machine virtuelle. De plus, si vous utilisez des machines virtuelles Azure Spot, celles-ci sont expulsées à tout moment en fonction des besoins en capacité d'Azure. En cas de capacité insuffisante sur Azure ou en cas de panne d'alimentation d'une machine virtuelle Spot, MCS se limite aux tailles de la machine virtuelle de sauvegarde. Vous pouvez indiquer une liste des tailles de machines virtuelles de sauvegarde à l'aide d'une propriété personnalisée `BackupVmConfiguration` lors de la création ou de la mise à jour d'un catalogue de machines MCS. MCS essaie de revenir aux tailles des machines virtuelles de sauvegarde dans l'ordre que vous avez indiqué dans la liste.

Lorsque MCS utilise une configuration de sauvegarde particulière pour la machine virtuelle, il continue à utiliser cette configuration jusqu'au prochain arrêt. Lors de la prochaine mise sous tension, MCS essaie de démarrer la configuration principale de la machine virtuelle. En cas d'échec, MCS essaie à nouveau de démarrer une configuration de taille de machine virtuelle de sauvegarde conformément à la liste.

Cette fonctionnalité est prise en charge sur :

- un catalogue qui utilise un profil de machine
- les catalogues de machines MCS persistants et non persistants
- les environnements Azure actuels

**Remarques importantes**

- Vous pouvez indiquer plusieurs tailles de machine virtuelle de sauvegarde dans la liste.
- La liste doit être unique.
- Vous pouvez ajouter la propriété de type d'instance pour chacune des machines virtuelles de la liste. Le type est **Spot** ou **Normal**. Si le type n'est pas spécifié, MCS considère le statut de la machine virtuelle comme **Normal**.
- Vous pouvez modifier la liste des tailles des machines virtuelles de sauvegarde d'un catalogue existant à l'aide des commandes PowerShell `Set-ProvScheme`.
- Vous pouvez mettre à jour les machines virtuelles existantes créées à partir du schéma de provisioning associé au catalogue à l'aide de la commande `Set-ProvVMUpdateTimeWindow`.
- Vous pouvez configurer la liste des tailles des machines virtuelles de sauvegarde pour un nombre sélectionné de machines virtuelles MCS existantes à l'aide de la commande `Set-ProvVM`. Toutefois, pour appliquer les mises à jour, définissez une fenêtre temporelle de mise à jour pour les machines virtuelles à l'aide de `Set-ProvVMUpdateTimeWindow` et démarrez les machines virtuelles dans cette fenêtre. Si la commande `Set-ProvVm` est utilisée sur une machine virtuelle, celle-ci continue d'utiliser la liste des tailles de machines virtuelles de sauvegarde définie sur cette machine virtuelle spécifique, même si la liste du schéma de provisioning est mise à jour ultérieurement. Vous pouvez utiliser `Set-ProvVM` avec `-RevertToProvSchemeConfiguration` pour que la machine virtuelle utilise la liste de sauvegarde du schéma de provisioning.

**Créer un catalogue avec les taille des machines virtuelles de sauvegarde**

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Créez un catalogue de brokers. Ce catalogue contient des machines qui sont sur le point d'être créées.
4. Créez un pool d'identités. Cela devient un conteneur pour les comptes AD créés pour les machines sur le point d'être créées.
5. Créez un schéma de provisioning avec le profil de la machine. Par exemple :

    - Si vous souhaitez fournir une liste de tailles de machines virtuelles normales uniquement, exécutez la commande suivante :

```
1  New-ProvScheme -ProvisioningSchemeName "azure-catalog" -
       MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.
       folder\helenli.resourcegroup\helenli-master1-mcsio-
       snapshot.snapshot"
2  -CustomProperties
```

```
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`"/>  <Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`" Value=`"['ServiceOffering': 'Standard_D2as_v4', 'ServiceOffering': 'Standard_D2s_v3', 'ServiceOffering': 'C']`"/>
</CustomProperties>"
<!--NeedCopy-->
```

- Si vous souhaitez fournir une liste de tailles de machines virtuelles mixtes (machines virtuelles normales et Spot), exécutez la commande suivante :

```
New-ProvScheme -ProvisioningSchemeName "azure-catalog" -MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.folder\helenli.resourcegroup\helenli-master1-mcsio-snapshot.snapshot"
-CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`"/>  <Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`" Value=`"[{
'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
, {
'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
, {
'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
]`"/>
</CustomProperties>"
<!--NeedCopy-->
```

6. Mettez à jour le BrokerCatalog avec l'ID unique du schéma de provisioning.
7. Créez et ajoutez des machines virtuelles au catalogue.

### Mettre à jour un catalogue existant

Vous pouvez mettre à jour un schéma de provisioning à l'aide de la commande `Set-ProvScheme`. Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName "azure-catalog"
-CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"
    true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value
    =`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"
    Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`
    "/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
    Value=`"[{
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
<!--NeedCopy-->
```

### Mettre à jour les machines virtuelles existantes

Vous pouvez mettre à jour les machines virtuelles existantes dans un catalogue à l'aide de la commande PowerShell `Set-ProvVMUpdateTimeWindow`. La commande met à jour les machines virtuelles créées à partir du schéma de provisioning associé au catalogue lors de la prochaine mise sous tension dans la fenêtre horaire donnée. Par exemple :

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am"-DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

> **Remarque :**
>
> `StartsNow` indique l'heure de début prévue. `DurationInMinutes` est la fenêtre horaire du calendrier.

Vous pouvez configurer la liste des tailles des machines virtuelles de sauvegarde pour un nombre sélectionné de machines virtuelles MCS existantes à l'aide de la commande `Set-ProvVM`. Toutefois,

pour appliquer les mises à jour, définissez une fenêtre temporelle de mise à jour pour les machines virtuelles à l'aide de `Set-ProvVMUpdateTimeWindow` et démarrez les machines virtuelles dans cette fenêtre. Par exemple :

1. Exécutez la commande `Set-ProvVM` pour configurer la liste des tailles des machines virtuelles de sauvegarde pour une machine virtuelle MCS existante sélectionnée. Par exemple :

```
Set-ProvVM -VMName "Vm-001"
-CustomProperties
"<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`"xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
    Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`"
    Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`
    "Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
    true`"/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration
    `" Value=`"[{
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
<!--NeedCopy-->
```

2. Exécutez la commande `Set-ProvVMUpdateTimeWindow` pour appliquer les mises à jour. Par exemple :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    StartsNow -DurationInMinutes 60
<!--NeedCopy-->
```

### Copier les balises sur toutes les ressources

Vous pouvez copier les balises spécifiées dans un profil de machine sur toutes les ressources telles que plusieurs cartes réseau et disques (disque du système d'exploitation, disque d'identité et disque de cache à écriture différée) d'une nouvelle machine virtuelle ou d'une machine virtuelle existante dans un catalogue de machines. La source du profil de machine peut être une machine virtuelle ou une spécification de modèle ARM.

> **Remarque :**
>
> Vous devez ajouter la stratégie aux balises (voir Affecter des définitions de stratégie pour la conformité des balises) ou ajouter les balises dans une source de profil de machine pour conserver les balises sur les ressources.

#### Logiciel requis

Créez la source du profil de machine (machine virtuelle ou spécification de modèle ARM) pour avoir des balises sur la machine virtuelle, les disques et les cartes réseau de cette machine virtuelle.

- Si vous souhaitez utiliser une machine virtuelle comme entrée de profil de machine, appliquez des balises sur la machine virtuelle et sur toutes les ressources du portail Azure. Consultez la section Ajouter des balises avec le portail Azure.
- Si vous souhaitez utiliser la spécification du modèle ARM comme entrée de profil de machine, ajoutez le bloc de balises suivant sous chaque ressource.

```
1   "tags": {
2
3  "TagC": "Value3"
4   }
5  ,
6  <!--NeedCopy-->
```

> **Remarque :**
>
> Vous pouvez avoir au maximum un disque et au moins une carte réseau dans la spécification du modèle.

#### Copier des balises sur les ressources d'une machine virtuelle d'un nouveau catalogue de machines

1. Créez un catalogue permanent ou non persistant avec une spécification de modèle machine virtuelle ou ARM comme entrée de profil de machine.
2. Ajoutez une machine virtuelle au catalogue et allumez-la. Les balises spécifiées dans le profil de la machine doivent être copiées dans les ressources correspondantes de cette machine virtuelle.

   > **Remarque :**
   >
   > Un message d'erreur s'affiche si le nombre de cartes réseau indiqué dans le profil de la machine ne correspond pas au nombre de cartes réseau que vous souhaitez que les machines virtuelles utilisent.

### Modifier les balises sur les ressources d'une machine virtuelle existante

1. Créez un profil de machine avec les balises de toutes les ressources.
2. Mettez à jour le catalogue de machines existant avec le profil de machine mis à jour. Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
    MachineProfile <PathToYourMachineProfile>
<!--NeedCopy-->
```

3. Éteignez la machine virtuelle sur laquelle vous souhaitez appliquer les mises à jour.
4. Demandez une mise à jour planifiée pour la machine virtuelle. Par exemple :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
    YourCatalogName>  -VMName machine1 -StartsNow -
    DurationInMinutes -1
<!--NeedCopy-->
```

5. Allumez la machine virtuelle.
6. Les balises spécifiées dans le profil de la machine doivent être copiées dans les ressources correspondantes.

> **Remarque :**
>
> Un message d'erreur s'affiche si le nombre de cartes réseau indiqué dans le profil de la machine ne correspond pas au nombre de cartes réseau fournies dans `Set-ProvScheme`.

## Autres ressources

- S'il s'agit du premier catalogue créé, Web Studio vous explique comment créer un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, consultez la section Installer et configurer.
- Pour gérer les catalogues, consultez Gérer les catalogues de machines et Gérer un catalogue Microsoft Azure.

## Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à Microsoft Azure Resource Manager
- Créer des catalogues de machines

# Créer un catalogue Microsoft System Center Virtual Machine Manager

June 27, 2024

La section Créer des catalogues de machines décrit les assistants qui permettent de créer un catalogue de machines. Les informations suivantes fournissent des informations spécifiques aux environnements de virtualisation Microsoft System Center Virtual Machine Manager (machine virtuelleM).

> **Remarque :**
>
> Avant de créer un catalogue machine virtuelleM, vous devez terminer la création d'une connexion à machine virtuelleM. Voir Connexion à Microsoft System Center Virtual Machine Manager.

## Créer une machine virtuelle principale

1. Installez un VDA sur la machine virtuelle principale et sélectionnez l'option d'optimisation du bureau pour améliorer les performances.
2. Réalisez un instantané de la machine virtuelle principale à utiliser comme sauvegarde.
3. Créez des bureaux virtuels.

## MCS sur des partages de fichiers SMB 3

Pour les catalogues de machines créés avec MCS sur les partages de fichiers SMB 3 pour le stockage de machine virtuelle, assurez-vous que les informations d'identification répondent aux exigences suivantes. Ces exigences garantissent que les appels de la bibliothèque HCL du Controller se connectent correctement au stockage SMB :

- Les informations d'identification de l'utilisateur machine virtuelleM doivent inclure un accès en écriture complet au stockage SMB.
- Les opérations de disque virtuel de stockage pendant les événements du cycle de vie des machine virtuelle sont effectuées par le biais du serveur Hyper-V à l'aide des informations d'identification de l'utilisateur machine virtuelleM.

Lorsque vous utilisez SMB comme stockage, activez Authentication Credential Security Support Provider (CredSSP) du Controller sur différentes machines Hyper-V individuelles. Utilisez ce processus pour machine virtuelleM 2012 SP1 avec Hyper-V sur Windows Server 2012. Pour plus d'informations, veuillez consulter l'article CTX137465.

La bibliothèque HCL utilise `CredSSP` pour ouvrir une connexion à la machine Hyper-V. Cette fonctionnalité transmet les informations d'identification de l'utilisateur chiffrées Kerberos à la machine Hyper-V. Les commandes **PowerShell** de la session sur la machine Hyper-V distante s'exécutent avec

les informations d'identification fournies. Dans ce cas, les informations d'identification de l'utilisateur machine virtuelleM, de sorte que les commandes de communication avec le stockage fonctionnent correctement.

Les tâches suivantes utilisent des scripts PowerShell constituées initialement dans le HCL et sont alors envoyées à la machine Hyper-V pour agir sur le stockage SMB 3.0.

- **Consolider l'image principale :** une image principale crée un schéma de provisioning MCS (catalogue de machines). Il clone et écrase la machine virtuelle principale en préparation pour la création de machine virtuelle à partir du nouveau disque créé (et supprime une dépendance sur la machine virtuelle principale originale).

  ConvertVirtualHardDisk sur l'espace de noms root\virtualization\v2

  Exemple :

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
<!--NeedCopy-->
```

- **Créer un disque de différence :** crée un disque de différence à partir de l'image principale générée par la consolidation de l'image principale. Le disque de différence est alors attaché à une nouvelle machine virtuelle.

  CreateVirtualHardDisk sur l'espace de noms root\virtualization\v2

  Exemple :

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
<!--NeedCopy-->
```

- **Charger des disques d'identité :** le HCL ne peut pas directement charger le disque d'identité sur le stockage SMB. Par conséquent, la machine Hyper-V doit télécharger et copier le disque d'identité vers le stockage. Étant donné que la machine Hyper-V ne peut pas lire le disque à partir du Controller, HCL doit tout d'abord copier le disque d'identité via la machine Hyper-V comme suit.

  1. HCL télécharge l'identité de la machine Hyper-V via le partage d'administrateur.
  2. La machine Hyper-V copie le disque vers le stockage SMB via un script PowerShell exécuté dans la session à distance PowerShell. Un dossier est créé sur la machine Hyper-V et les permissions sur ce dossier sont verrouillées pour l'utilisateur machine virtuelleM uniquement (via la connexion PowerShell distante).
  3. HCL supprime le fichier à partir du partage de l'administrateur.

4. Lorsque la bibliothèque HCL termine le téléchargement du disque d'identité vers la machine Hyper-V, la session PowerShell distante copie les disques d'identité vers le stockage SMB. Elle le supprime ensuite de la machine Hyper-V.

Le dossier du disque d'identité est recréé s'il est supprimé de façon à ce qu'il soit disponible pour une éventuelle réutilisation.

- **Télécharger des disques d'identité :** comme pour les chargements, les disques d'identité transitent via la machine Hyper-V vers le HCL. Le processus suivant permet de créer un dossier qui ne possède que des permissions utilisateur machine virtuelleM sur le serveur Hyper-V s'il n'existe pas.

  1. La machine Hyper-V copie le disque à partir du stockage SMB vers le stockage Hyper-V local au travers d'un script PowerShell. Ce script s'exécute dans la session distante PowerShell V3.
  2. HCL lit le disque depuis le partage administrateur de la machine Hyper-V dans la mémoire.
  3. HCL supprime le fichier à partir du partage de l'administrateur.

## Créer un catalogue avec un profil de machine

Vous pouvez utiliser un profil de machine pour créer et mettre à jour un catalogue de machines MCS dans les environnements System Center Virtual Machine Manager (SCVMM). Vous pouvez également activer la virtualisation imbriquée et le vTPM.

### Remarques importantes

- L'image principale ne peut être qu'un instantané et non une machine virtuelle.
- Vous ne pouvez utiliser une machine virtuelle que comme source de profil de machine.
- Vous pouvez configurer VTPM depuis la console Hyper-V et non depuis la console SCVMM.
- Si le vTPM est activé sur l'image principale, vous devez activer le vTPM sur la source du profil de la machine.
- Le vTPM n'est pris en charge que sur les machines de deuxième génération.
- Les paramètres suivants remplacent les valeurs capturées dans un profil de machine s'ils sont fournis séparément :
  - VMCpuCount
  - VMMemoryMB
  - Stockage sur disque
- Vous pouvez mettre à jour un catalogue existant à l'aide de la commande `Set-ProvScheme`.

### Étapes pour créer un catalogue à l'aide d'un profil de machine

1. Créez une machine virtuelle en tant que source de profil de machine. Pour en savoir plus, consultez Provisionner des machines virtuelles dans la structure VMM. Une fois sélectionnée, vous ne pouvez plus modifier la **génération**.
    - Si vous souhaitez activer la virtualisation imbriquée, cochez la case **Activer la virtualisation imbriquée** sur la page **Sélectionner la source**.
    - Si vous souhaitez activer vTPM, connectez-vous à l'hôte Hyper-V après avoir créé la machine virtuelle et recherchez votre machine virtuelle dans le **gestionnaire Hyper-V**. Cliquez avec le bouton droit sur la machine virtuelle, puis sur **Paramètres**. Dans **Sécurité**, cochez la case **Activer le module de plateforme sécurisée (TPM)**.
2. Ouvrez une fenêtre **PowerShell**.
3. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
4. Créez un catalogue de brokers. Ce catalogue contient des machines qui sont sur le point d'être créées.
5. Créez un pool d'identités. Cela devient un conteneur pour les comptes AD créés pour les machines sur le point d'être créées.
6. Créez un schéma de provisioning avec le profil de la machine. Par exemple :

```
1 New-ProvScheme -HostingUnitName "<hostingunit name>"
2 -IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1<
     path to the checkpoint/snapshot>"
3 -ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:<
     path to the machine profile VM>"
4 <!--NeedCopy-->
```

7. Met à jour le catalogue Broker avec l'identifiant unique du schéma de provisioning.
8. Créez et ajoutez des machines virtuelles au catalogue.

Vous pouvez mettre à jour un catalogue existant à l'aide de la commande Set-ProvScheme. Par exemple :

```
1 Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
     "XDHyp:<path to the machine profile VM>"
2 <!--NeedCopy-->
```

### Autres ressources

- S'il s'agit du premier catalogue créé, Web Studio vous explique comment créer un groupe de mise à disposition.

- Pour passer en revue l'ensemble du processus de configuration, consultez la section Installer et configurer.
- Pour gérer les catalogues, consultez Gérer les catalogues de machines et Gérer un catalogue Microsoft System Center Virtual Machine Manager.

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à Microsoft System Center Virtual Machine Manager
- Créer des catalogues de machines

## Créer un catalogue Nutanix

June 27, 2024

La section Créer des catalogues de machines décrit les assistants qui permettent de créer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements de virtualisation Nutanix.

> **Remarque :**
>
> Avant de créer un catalogue Nutanix, vous devez terminer la création d'une connexion à Nutanix. Voir Connexion à Nutanix.

### Créer un catalogue de machines à l'aide d'un instantané Nutanix

L'instantané que vous sélectionnez représente le modèle qui est utilisé pour créer les machines virtuelles dans le catalogue. Avant de créer le catalogue, créez des images et des instantanés dans Nutanix. Pour plus d'informations, consultez la documentation Nutanix.

Dans l'assistant de création de catalogues :

- Les pages **Système d'exploitation** et **Gestion des machines** ne contiennent aucune information spécifique à Nutanix.
- La page **Container** ou **Cluster and Container** est spécifique à Nutanix.

  Si vous déployez des machines à l'aide de Nutanix AHV XI comme ressources, la page **Container** s'affiche. Sélectionnez un conteneur dans lequel les disques d'identité des machines virtuelles seront placés.

Si vous déployez des machines à l'aide de Nutanix AHV Prism Central (PC) comme ressources, la page **Cluster and Container** s'affiche. Sélectionnez le cluster à utiliser pour le déploiement de machines virtuelles, puis un conteneur.

- Sur la page **Image**, sélectionnez l'instantané d'image. Les noms des instantanés Acropolis doivent être précédés de « XD_ » pour pouvoir être utilisés dans Citrix Virtual Apps and Desktops. Utilisez la console Acropolis pour renommer vos instantanés, le cas échéant. Si vous renommez des instantanés, redémarrez l'assistant de création de catalogues pour afficher une liste actualisée.
- Sur la page **Machines virtuelles**, indiquez le nombre de processeurs virtuels et le nombre de cœurs par vCPU.
- Sur la page **Cartes réseau**, sélectionnez le type de carte réseau pour filtrer les réseaux associés. Il existe deux types de cartes réseau : **VLAN** et **OVERLAY**. Sélectionnez une ou plusieurs cartes réseau contenues dans l'image principale, puis sélectionnez un réseau virtuel associé pour chaque carte réseau.
- Les pages **Identités des machines**, **Informations d'identification du domaine**, **Étendues** et **Résumé** ne contiennent pas d'informations spécifiques à Nutanix.

### Limitation

Lors de la création d'un catalogue MCS avec une connexion hôte Nutanix (en particulier, le plugin Nutanix AHV 2.7.1), la taille du disque dur des machines virtuelles provisionnées s'affiche de manière incorrecte dans Web Studio. La taille affichée est beaucoup plus petite (1 Go) que la taille de stockage réelle (50 Go). La taille du disque dur s'affiche correctement sur la console Nutanix.

### Autres ressources

- S'il s'agit du premier catalogue créé, Web Studio vous explique comment créer un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, consultez la section Installer et configurer.
- Pour gérer les catalogues, consultez Gérer les catalogues de machines.

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à Nutanix
- Connexion aux solutions partenaires et cloud Nutanix
- Créer des catalogues de machines

# Créer un catalogue VMware

June 27, 2024

La section Créer des catalogues de machines décrit les assistants qui permettent de créer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements de virtualisation VMware.

> **Remarque :**
>
> Avant de créer un catalogue VMware, vous devez terminer la création d'une connexion à VMware. Voir Connexion à VMware.

## Créer une machine virtuelle principale

Utilisez une VM principale pour fournir les bureaux et les applications des utilisateurs dans un catalogue de machines. Sur votre hyperviseur :

1. Installez un VDA sur la VM principale, en sélectionnant l'option d'optimisation du bureau, ce qui améliore les performances.
2. Réalisez un instantané de la MV principale à utiliser comme sauvegarde.

> **Remarque :**
>
> Vous pouvez utiliser MCS pour provisionner des machines virtuelles dans un environnement vSAN 8.0.

## Créer un catalogue de machines à l'aide d'un profil de machine

Vous pouvez créer un catalogue de machines MCS à l'aide d'un profil de machine. La source de l'entrée de profil de machine est un modèle VMware. Le profil de machine capture les propriétés matérielles à partir d'un modèle VMware et les applique aux machines virtuelles récemment provisionnées dans le catalogue.

> **Remarque :**
>
> - L'entrée d'image principale (instantané) et l'entrée de profil de machine (modèle VMware) doivent être activées ou désactivées. Cette règle s'applique à la fois à `New-ProvScheme` et `Set-ProvScheme`.
> - Si le vTPM est activé sur l'image principale, le modèle VMware ne peut provenir que de la même source de machine virtuelle que l'image principale.
> - La stratégie de stockage chiffré ne prend en charge que le clonage complet.

Le modèle VMware figurant dans le profil de la machine doit exister pendant le cycle de vie du catalogue pour permettre le provisioning des machines virtuelles dans le catalogue. Sans modèle VMware, vous ne pouvez pas provisionner de nouvelles machines virtuelles. Lorsqu'un modèle VMware est supprimé, vous devez fournir un nouveau modèle à l'aide de la commande `Set-ProvScheme`.

- MCS capture les propriétés d'un modèle VMware. Vous pouvez créer un modèle VMware faisant référence aux propriétés stockées du modèle VMware à l'aide de la commande Get-Provscheme.
- Si le catalogue de machines et les machines virtuelles provisionnées existent, une machine provisionnée avec MCS peut également être utilisée pour créer un modèle VMware

En fonction de différents systèmes d'exploitation, vous pouvez créer un catalogue de machines avec différentes configurations :

- Si Windows 11 est installé sur l'image principale, le vTPM doit être activé pour l'image principale. Par conséquent, le modèle VMware, qui est une source de profil de machine, doit être associé au vTPM.
- Si Windows 10 est installé sur l'image principale sans vTPM associé, vous pouvez créer un catalogue de machines avec un modèle VMware non vTPM comme source pour le profil de machine.

Il existe une autre configuration avec laquelle vous pouvez créer un catalogue de machines à l'aide du mode de copie complète du disque qui utilise un modèle de profil de machine appliqué avec une stratégie de stockage chiffré.

Pour créer un catalogue de machines à l'aide des commandes PowerShell avec le profil de la machine comme entrée :

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*`.
3. Exécutez les commandes suivantes :

    - Pour créer un catalogue de machines avec le modèle VMware associé au vTPM comme source pour l'entrée de profil de machine et l'image principale installée sous Windows 11 :

```
$identityPool = New-AcctIdentityPool  -IdentityPoolName "<
    string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "vSanRg"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
```

```
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<network name>.
   network" }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4
-VMMemoryMB 6144
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template" -TenancyType Shared
-FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9'
-Name "<catalog name>"
-ProvisioningType 'MCS'
-Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Pour créer un catalogue de machines avec un modèle VMware non vTPM comme source pour le profil de la machine et l'image principale installée sous Windows 10 :

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###" -NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme
-CleanOnBoot -HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
    }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
    -VMMemoryMB 8192
```

```
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
    template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
    ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Pour créer un catalogue de machines à l'aide du mode de copie complète du disque qui utilise un modèle de profil de machine appliqué avec une stratégie de stockage chiffré :

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme
-HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
    snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
     }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "
    XDHyp:\HostingUnits<hosting unit name><template name>.
    template"
-TenancyType Shared
-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"  -IsRemotePC $False
```

```
-MinimumFunctionalLevel 'L7_9'
-Name "<string>" -ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

Pour mettre à jour le profil d'une machine, utilisez la commande Set-ProvScheme. Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
    -MachineProfile 'XDHyp:\HostingUnits<hosting unit name><template
    name>.template'
<!--NeedCopy-->
```

### Vérifier la présence de plusieurs cartes d'interface réseau

Vous recevez plusieurs messages d'erreur lors des vérifications préalables de la présence de plusieurs cartes d'interface réseau lorsque vous utilisez un profil de machine et le paramètre `NetworkMapping` dans les commandes `New-ProvScheme` et `Set-ProvScheme`.

La liste des vérifications préalables de la présence de plusieurs cartes d'interface réseau est la suivante :

- Seul le nombre de cartes d'interface réseau provenant du modèle de profil de machine est utilisé et validé. Le réseau vers lequel pointent ces cartes d'interface réseau n'est ni utilisé ni validé par rapport aux réseaux de l'unité d'hébergement.
- Si le nombre de cartes d'interface réseau dans le modèle de profil de machine est supérieur au nombre de réseaux de l'unité d'hébergement, un message d'erreur s'affiche.
- Si le nombre de cartes d'interface réseau dans le modèle de profil de machine est égal à zéro, un message d'erreur s'affiche.
  Lorsque le nombre de cartes d'interface réseau dans le modèle de profil de machine est égal à un :
  - If no network mapping is specified in the `New-ProvScheme` or `Set-ProvScheme` command, and the hosting unit network is one, then the hosting unit network is used.
  - If network mapping is specified, then the specified network mapping is used if it is valid.
- Lorsque le nombre de cartes d'interface réseau dans le modèle de profil de machine est supérieur à 1 ou que le nombre de réseaux de l'unité d'hébergement est supérieur à 1 :
  - Un mappage réseau valide est requis dans la commande et il doit fournir un mappage pour chaque carte d'interface réseau (c'est-à-dire que le nombre de cartes d'interface réseau doit être identique au nombre de cartes d'interface réseau du profil de la machine).

  - Plusieurs cartes d'interface réseau ne peuvent pas être mappées au même réseau dans l'unité d'hébergement.
  - Le nombre `NetworkMapping` et le nombre de cartes d'interface réseau de profil de machine doivent être inférieurs ou égaux au nombre de réseaux de l'unité d'hébergement.
  - `NetworkMapping` doit être fourni pour chaque identifiant compris entre 0 et n-1, où n est le nombre d'adaptateurs réseau dans le modèle de profil de machine.

### Dépannage

Si la création du catalogue échoue, consultez CTX294978.

### Autres ressources

- S'il s'agit du premier catalogue créé, Web Studio vous explique comment créer un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, consultez la section Installer et configurer.
- Pour gérer les catalogues, consultez Gérer les catalogues de machines et Gérer un catalogue VMware.

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à VMware
- Créer des catalogues de machines

## Créer des catalogues de différents types de jointure

June 27, 2024

À l'aide de MCS, vous pouvez provisionner des machines en tant que machines jointes à AD sur site ou jointes à Azure AD Hybride.

Pour plus d'informations sur la configuration des identités de machines dans Web Studio, consultez la section Créer des catalogues de machines.

Pour des informations spécifiques sur la façon de créer des catalogues joints à des identités de machines, consultez les rubriques suivantes :

- Créer des catalogues joints à Azure Active Directory hybride

# Créer des catalogues joints à Azure Active Directory hybride

June 27, 2024

> **Remarque :**
>
> Depuis juillet 2023, Microsoft a renommé Azure Active Directory (Azure AD) Microsoft Entra ID. Dans ce document, toute occurrence de l'appellation Azure Active Directory, Azure AD ou de l'acronyme AAD fait désormais référence à Microsoft Entra ID.

Cet article explique comment créer des catalogues joints à Azure Active Directory (AD) Hybride.

Vous pouvez créer des catalogues joints à Azure AD à l'aide de Web Studio ou de PowerShell.

Pour plus d'informations sur les exigences, les limites et les considérations, consultez la section Joint à Azure Active Directory Hybride.

## Utiliser Web Studio

Les informations suivantes étayent les instructions disponibles dans la section Créer des catalogues de machines. Pour créer des catalogues joints à Azure AD Hybride, suivez les instructions générales de cet article, en tenant compte des détails spécifiques aux catalogues joints à Azure AD Hybride.

Dans l'assistant de création de catalogues :

- Sur la page **Identités des machines**, sélectionnez **Joint à Azure Active Directory Hybride**. Les machines créées appartiennent à une organisation et sont connectées avec un compte des services de domaine Active Directory appartenant à cette organisation. Elles existent dans le cloud et sur site.

> **Remarque :**
>
> Si vous sélectionnez **Joint à Azure Active Directory Hybride** comme type d'identité, chaque machine du catalogue doit avoir un compte d'ordinateur Active Directory correspondant.

## Utiliser PowerShell

Voici des étapes PowerShell équivalentes aux opérations Web Studio. Pour plus d'informations sur la création d'un catalogue à l'aide du SDK Remote PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

La différence entre les catalogues joints à AD sur site et ceux joints à Azure AD Hybride réside dans la création du pool d'identités et des comptes de machines.

Pour créer un pool d'identités avec les comptes pour les catalogues joints à Azure AD Hybride :

```
New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -
    Domain "corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -
    NamingScheme "HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU "CN=
    AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-d2f2-49
    d2-ab12-bae5bbd0df05"
New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
    -ADUserName "corp\admin1" -ADPassword $password
Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
<!--NeedCopy-->
```

> **Remarque :**
>
> `$password` est le mot de passe correspondant à un compte utilisateur AD doté d'autorisations d'écriture.

Toutes les autres commandes utilisées pour créer des catalogues joints à Azure AD Hybride sont les mêmes que pour les catalogues joints à AD sur site traditionnels.

### Afficher l'état Azure AD Hybride

Dans l'interface Web Studio, l'état Azure AD Hybride est visible lorsque les machines jointes à Azure AD Hybride dans un groupe de mise à disposition sont sous tension. Pour afficher l'état, utilisez la fonction Rechercher pour identifier ces machines, puis vérifiez **Identité de la machine** dans l'onglet **Détails** du volet inférieur. Les informations suivantes peuvent apparaître dans **Identité de la machine** :

- Joint à Azure AD Hybride
- Pas encore joint à Azure AD

> **Remarque :**
>
> - La jonction à Azure AD Hybride peut être retardée lors de la mise sous tension initiale de la machine. Cela est dû à l'intervalle de synchronisation de l'identité de la machine par défaut (30 minutes d'Azure AD Connect). La machine est définie sur l'état Joint à Azure AD Hybride uniquement après la synchronisation des identités de la machine avec Azure AD via Azure AD Connect.
> - Si des machines ne sont pas définies sur l'état Joint à Azure AD Hybride, elles ne sont pas enregistrées auprès du Delivery Controller. Leur état d'enregistrement indique **Initialisation**.

En outre, à l'aide de Web Studio, vous pouvez découvrir pourquoi les machines ne sont pas disponibles. Pour ce faire, cliquez sur une machine dans le nœud **Rechercher**, cochez **Enregistrement** dans l'onglet **Détails** dans le volet inférieur, puis lisez l'infobulle pour plus d'informations.

### Dépannage

Si des machines ne peuvent pas être jointes à Azure AD Hybride, procédez comme suit :

- Vérifiez si le compte de la machine a été synchronisé avec Azure AD via le portail Microsoft Azure AD. S'il est synchronisé, **Pas encore joint à Azure AD** apparaît, indiquant que l'inscription est en attente.

  Pour synchroniser des comptes de machines avec Azure AD, assurez-vous que :

  - Le compte de machine se trouve dans l'unité d'organisation configurée pour être synchronisée avec Azure AD. Les comptes de machines sans attribut **userCertificate** ne sont pas synchronisés avec Azure AD même s'ils se trouvent dans l'unité d'organisation configurée pour être synchronisée.
  - L'attribut **userCertificate** est renseigné dans le compte de la machine. Utilisez Active Directory Explorer pour afficher l'attribut.
  - Azure AD Connect doit avoir été synchronisé au moins une fois après la création du compte de machine. Sinon, exécutez manuellement la commande `Start-ADSyncSyncCycle -PolicyType Delta` dans la console PowerShell de la machine Azure AD Connect pour déclencher une synchronisation immédiate.

- Vérifiez si la paire de clés de périphérique géré par Citrix pour la jointure à Azure AD Hybride est correctement transmise à la machine en interrogeant la valeur de **DeviceKeyPairRestored** sous **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**.

  Vérifiez que la valeur est 1. Si ce n'est pas le cas, les raisons possibles sont les suivantes :

  - Le paramètre `IdentityType` du pool d'identités associé au schéma de provisioning n'est pas défini sur `HybridAzureAD`. Vous pouvez le vérifier en exécutant `Get-AcctIdentityPool`.
  - La machine n'est pas provisionnée à l'aide du même schéma de provisioning que le catalogue de machines.
  - La machine n'est pas jointe au domaine local. La jonction au domaine local est une condition préalable à la jonction à Azure AD.

- Vérifiez les messages de diagnostic en exécutant la commande `dsregcmd /status /debug` sur la machine provisionnée par MCS.

  - Si la jonction à Azure AD Hybride réussit, **AzureAdJoined** et **DomainJoined** ont la valeur **YES** dans la sortie de la ligne de commande.

  - Si ce n'est pas le cas, consultez la documentation Microsoft pour résoudre les problèmes : https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current.

- Si vous voyez le message d'erreur **Message du serveur : Le certificat utilisateur est introuvable sur l'appareil avec l'ID : xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxx**, exécutez la commande PowerShell suivante pour réparer le certificat utilisateur :

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
   UserCertificate
<!--NeedCopy-->
```

Pour plus d'informations sur le problème du certificat utilisateur, consultez CTX566696.

## Gérer des catalogues de machines

June 28, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

### Introduction

Vous pouvez ajouter ou supprimer des machines dans un catalogue de machines, renommer, modifier la description ou gérer les comptes d'ordinateurs Active Directory d'un catalogue.

Il peut également être nécessaire de s'assurer que chaque machine dispose des dernières mises à jour du système d'exploitation, y compris les mises à jour antivirus, les mises à niveau du système d'exploitation ou les modifications de configuration.

- Les catalogues contenant des machines regroupées au hasard créées à l'aide de Machine Creation Services (MCS) gèrent les machines en mettant à jour l'image principale utilisée dans le catalogue, puis en mettant à jour les machines. Cette méthode vous permet de mettre à jour de manière efficace un grand nombre de machines utilisateur.
- Pour les catalogues contenant des machines Remote PC Access et statiques, gérez les mises à jour des machines des utilisateurs en dehors de Web Studio. Effectuez cette tâche individuellement ou collectivement en utilisant des outils de distribution de logiciels tiers.

Pour de plus amples informations sur la création et la gestion de connexions à des hyperviseurs hôtes, consultez l'article Connexions et ressources.

> **Remarque :**
>
> MCS ne prend pas en charge Windows 10 IoT Standard et Windows 10 IoT Entreprise. Consultez le site Microsoft pour obtenir des informations supplémentaires.

#### À propos des instances persistantes

Lors de la mise à jour d'un catalogue MCS créé à l'aide d'instances persistantes ou dédiées, toutes les nouvelles machines créées pour le catalogue utilisent l'image mise à jour. Les instances préexistantes continuent d'utiliser l'instance d'origine. Le processus de mise à jour d'une image se fait de la même manière pour tout autre type de catalogue. Tenez compte des considérations suivantes :

- Pour les catalogues de disques persistants, les machines préexistantes ne sont pas mises à jour vers la nouvelle image, mais toutes les nouvelles machines ajoutées au catalogue utilisent la nouvelle image.
- Pour les catalogues de disques non persistants, l'image de la machine est mise à jour lors de la prochaine réinitialisation de la machine.
- Pour les catalogues de machines persistantes, la mise à jour de l'image met également à jour les instances du catalogue qui l'utilisent.
- Pour les catalogues non persistants, si vous souhaitez des images différentes pour différentes machines, les images doivent résider dans des catalogues distincts.

### Gérer des catalogues de machines

Vous pouvez gérer un catalogue de machines de deux manières :

- Utilisation de Web Studio
- Utilisation de PowerShell

### Utiliser Web Studio

Cette section explique comment gérer les catalogues à l'aide de Web Studio :

- Afficher les détails du catalogue
- Ajouter des machines à un catalogue
- Supprimer des machines d'un catalogue
- Modifier un catalogue
- Renommer un catalogue
- Déplacer un catalogue vers une autre zone
- Supprimer un catalogue

- Gérer les comptes d'ordinateurs Active Directory dans un catalogue
- Mettre un catalogue à jour
- Modifier le niveau fonctionnel ou annuler la modification
- Cloner un catalogue
- Organiser les catalogues sous forme de dossiers

### Afficher les détails du catalogue

1. Utilisez la fonction de recherche pour localiser un catalogue de machines spécifique. Pour obtenir des instructions, reportez-vous à la section Rechercher des instances.
2. Dans les résultats de la recherche, sélectionnez un catalogue selon vos besoins.
3. Pour obtenir la description des colonnes du catalogue, reportez-vous au tableau suivant.
4. Pour plus d'informations sur ce catalogue, cliquez sur un onglet dans le volet d'informations inférieur.

| Colonne | Description |
| --- | --- |
| Catalogue de machines | Nom et type d'allocation du catalogue. Les types d'allocation incluent<br>Aléatoire : les machines du catalogue sont attribuées à un utilisateur de manière aléatoire.<br>Permanent : les machines du catalogue sont attribuées à un utilisateur de façon permanente. |
| Type de machine | Type de session pris en charge pour les machines du catalogue. Les valeurs possibles incluent<br>Type d'OS : OS multi-session (virtuel). Données utilisateur : Abandonner.<br>Type d'OS : OS multi-session (virtuel). Données utilisateur : Sur le disque local<br>Type d'OS : OS mono-session (Remote PC Access)<br>Type d'OS : OS mono-session (virtuel). Données utilisateur : Abandonner.<br>Type d'OS : OS mono-session (virtuel). Données utilisateur : Sur le disque local<br>Type d'OS : OS mono-session (virtuel). Machines Creation Services (machine MCS), Machines et méthode de provisioning Citrix Provisioning Services. |
| Nombre de machines | Nombre de machines du catalogue. |
| Nombre alloué | Nombre de machines du catalogue attribuées à un groupe de mise à disposition. |

| Colonne | Description |
| --- | --- |
| Folder | Emplacement du catalogue dans l'arborescence **Catalogues de machines**. Affiche le nom du dossier dans lequel se trouve le catalogue (y compris la barre oblique inverse de fin) ou indique − si le catalogue se trouve au niveau racine. |
| Mise à niveau de VDA | État de la mise à niveau de VDA. Les valeurs possibles sont les suivantes : Non configuré, Programmé, Disponible et À jour. |
| État de l'image | État de mise à jour de l'image du catalogue. Applicable uniquement aux catalogues de machines non persistants. Les valeurs possibles incluent : Entièrement mise à jour, Partiellement mise à jour, Mises à jour en attente, Préparation |

### Ajouter des machines à un catalogue

Avant de commencer :

- Assurez-vous que l'ordinateur hôte de virtualisation dispose de suffisamment de processeurs, de mémoire et de stockage pour prendre en charge les machines supplémentaires.
- Vérifiez que vous disposez de suffisamment de comptes d'ordinateurs Active Directory inutilisés. Si vous utilisez des comptes existants, le nombre de machines que vous pouvez ajouter est limité par le nombre de comptes disponibles.
- Si vous utilisez Web Studio pour créer des comptes d'ordinateurs Active Directory pour les machines supplémentaires, vous devez disposer des droits d'administrateur de domaine.

Pour ajouter des machines à un catalogue :

1. Connectez-vous à Web Studio.
2. Sélectionnez **Catalogues de machines** dans le volet de gauche.
3. Sélectionnez un catalogue de machines, puis sélectionnez **Ajouter des machines** dans la barre d'actions.
4. Sélectionnez le nombre de machines virtuelles à ajouter.
5. S'il n'y a pas suffisamment de comptes Active Directory pour le nombre de machines virtuelles que vous ajoutez, sélectionnez le domaine et l'emplacement où les comptes sont créés. Spécifiez un schéma d'attribution de nom du compte, à l'aide des marques de hachage pour indiquer l'emplacement où les numéros séquentiels ou les lettres apparaissent. N'utilisez pas de

barre oblique (/) dans un nom d'unité d'organisation. Un nom ne peut pas commencer par un chiffre. Par exemple, un principe de dénomination de PC-Sales-## (avec 0-9 sélectionné) dans les comptes d'ordinateur nommés PC-Sales-01, PC-Sales-02, PC-Sales-03, etc.

6. Si vous utilisez des comptes Active Directory existants, vous pouvez sélectionner les comptes ou cliquer sur **Importer** et spécifier un fichier .csv contenant les noms de compte. Assurez-vous qu'il existe suffisamment de comptes pour toutes les machines que vous ajoutez. Web Studio gère ces comptes. Autorisez Web Studio à réinitialiser les mots de passe de tous les comptes ou spécifiez le mot de passe de compte (qui doit être le même pour tous les comptes).

Les machines sont créées en tant que processus en arrière-plan, qui peut être long lors de la création de plusieurs machines. La création de la machine se poursuit même si vous fermez Web Studio.

### Supprimer des machines d'un catalogue

Lorsque vous supprimez une machine d'un catalogue de machines, les utilisateurs ne peuvent plus y accéder ; donc, avant de supprimer une machine, assurez-vous que :

- Les données utilisateur sont sauvegardées ou ne sont plus nécessaires.
- Tous les utilisateurs sont déconnectés. L'activation du mode maintenance empêche les nouvelles connexions à une machine.
- Les machines sont hors tension.

Pour supprimer des machines d'un catalogue :

1. Connectez-vous à Web Studio.
2. Sélectionnez **Catalogues de machines** dans le volet de gauche.
3. Sélectionner un catalogue, puis sélectionnez **Afficher les machines** dans la barre d'actions.
4. Sélectionnez une ou plusieurs machines, puis sélectionnez **Supprimer** dans la barre d'actions.

Choisissez si vous souhaitez supprimer les machines en cours de suppression. Si vous choisissez de supprimer les machines, indiquez si les comptes Active Directory pour ces machines doivent être conservés, désactivés ou supprimés.

### Modifier un catalogue

1. Sur la page **Description**, modifiez la description du catalogue.
2. Sélectionnez **Catalogues de machines** dans le volet de gauche.
3. Sélectionnez un catalogue, puis sélectionnez **Modifier le catalogue de machines** dans la barre d'actions.
4. Sur la page **Étendues**, modifiez les étendues.

5. D'autres pages peuvent s'afficher en fonction du type de catalogue.

   Pour les catalogues créés à l'aide d'une image Azure Resource Manager, les pages suivantes sont visibles. N'oubliez pas que les modifications que vous apportez ne s'appliquent qu'aux machines que vous ajouterez ultérieurement au catalogue. Les machines existantes restent inchangées.

   - Sur la page **Machines virtuelles**, modifiez la taille de la machine et les zones de disponibilité dans lesquelles vous souhaitez créer des machines.

     > **Remarque :**
     >
     > – Seules les tailles de machines prises en charge par le catalogue sont affichées.
     > – Si nécessaire, sélectionnez **Afficher uniquement les tailles de machines utilisées dans d'autres catalogues de machines** pour filtrer la liste des tailles de machines.

   - Sur la page **Profil de la machine**, choisissez d'utiliser ou de modifier un profil de machine.
   - (Uniquement visible lorsque le catalogue est configuré avec un hôte de groupe dédié) Sur la page **Groupe d'hôtes dédié**, choisissez si vous souhaitez modifier un groupe d'hôtes.
   - Sur la page **Types de stockage et de licence**, choisissez de modifier le type de stockage, le type de licence et les paramètres Azure Computer Gallery (disponibles uniquement lorsque l'option **Placer une image préparée dans Azure Gallery** est utilisé).

     > **Remarque :**
     >
     > Si le nouveau paramètre sélectionné ne prend pas en charge la taille actuelle de la machine, une boîte de dialogue d'avertissement apparaît, vous informant que la modification du paramètre réinitialise le paramètre de taille de la machine. Si vous choisissez de continuer, un point rouge apparaît à côté du menu **Machines virtuelles**, vous invitant à sélectionner une nouvelle taille de machine.

   - Sur la page **Types de licence**, indiquez si vous souhaitez modifier le paramètre de licence Windows ou Linux.

   Pour les catalogues Remote PC Access, les pages suivantes sont visibles :

   - Sur la page **Gestion de l'alimentation**, modifiez les paramètres de gestion de l'alimentation et sélectionnez une connexion de gestion de l'alimentation.
   - Sur la page **Unités d'organisation**, ajoutez ou supprimez des unités d'organisation Active Directory.

6. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et cliquez sur **Enregistrer** pour quitter la page.

### Renommer un catalogue

1. Connectez-vous à Web Studio.
2. Sélectionnez **Catalogues de machines** dans le volet de gauche.
3. Sélectionnez un catalogue, puis sélectionnez **Renommer le catalogue de machines** dans la barre d'actions.
4. Entrez le nouveau nom.

### Déplacer un catalogue vers une autre zone

Si votre déploiement contient plusieurs zones, vous pouvez déplacer un catalogue d'une zone vers une autre.

Le déplacement d'un catalogue vers une zone autre que l'hyperviseur contenant les machine virtuelle de ce catalogue affecte les performances.

1. Connectez-vous à Web Studio.
2. Sélectionnez **Catalogues de machines** dans le volet de gauche.
3. Sélectionnez un catalogue, puis sélectionnez **Déplacer** dans la barre d'actions.
4. Sélectionnez la zone vers laquelle vous souhaitez déplacer le catalogue.

### Supprimer un catalogue

Avant de supprimer un catalogue, vérifiez ce qui suit :

- Tous les utilisateurs sont déconnectés et vous n'exécutez aucune session déconnectée.
- Le mode de maintenance est activé pour toutes les machines du catalogue, de sorte qu'il ne soit pas possible d'effectuer de nouvelles connexions.
- Toutes les machines des catalogues sont hors tension.
- Le catalogue n'est pas associé à un groupe de mise à disposition. En d'autres termes, le groupe de mise à disposition ne contient pas les machines du catalogue.

Pour supprimer un catalogue :

1. Connectez-vous à Web Studio.
2. Sélectionnez **Catalogues de machines** dans le volet de gauche.
3. Sélectionnez un catalogue, puis sélectionnez **Supprimer le catalogue de machines** dans la barre d'actions.
4. Indiquez si les machines du catalogue doivent être supprimées. Si vous choisissez de supprimer les machines, indiquez si les comptes d'ordinateur Active Directory pour ces machines doivent être conservés, désactivés ou supprimés.

### Gérer les comptes d'ordinateurs Active Directory dans un catalogue

Pour gérer les comptes Active Directory dans un catalogue de machines, vous pouvez :

- Libérer des comptes de machines non utilisés en supprimant les comptes d'ordinateurs Active Directory des catalogues de machines avec OS mono-session et avec OS multi-session. Ces comptes peuvent ensuite être utilisés pour d'autres machines.
- Ajoutez des comptes de façon à ce que lorsque plus de machines sont ajoutées au catalogue, les comptes d'ordinateurs soient déjà en place N'utilisez pas de barre oblique (/) dans un nom d'unité d'organisation.

Pour gérer les comptes Active Directory :

1. Connectez-vous à Web Studio.
2. Sélectionnez **Catalogues de machines** dans le volet de gauche.
3. Sélectionnez un catalogue, puis sélectionnez **Gérer les comptes AD** dans la barre d'actions.
4. Choisissez si vous souhaitez ajouter ou supprimer des comptes d'ordinateurs. Si vous ajoutez des comptes, indiquez la marche à suivre avec les mots de passe de compte : les réinitialiser ou entrer un mot de passe qui s'applique à tous les comptes.

   Vous pouvez réinitialiser les mots de passe si vous ne connaissez pas les mots de passe de compte actuels, vous devez avoir l'autorisation d'effectuer une réinitialisation du mot de passe. Lorsque vous entrez un mot de passe, le mot de passe est modifié sur les comptes lors de leur importation. Lorsque vous supprimez un compte, indiquez si le compte dans Active Directory doit être conservé, désactivé ou supprimé.

Indiquez si les comptes Active Directory doivent être conservés, désactivés ou supprimés lorsque vous supprimez les machines d'un catalogue ou supprimez un catalogue.

### Mettre un catalogue à jour

Nous vous recommandons de sauvegarder des copies ou des instantanés des images principales avant de mettre à jour les machines dans le catalogue. La base de données conserve un enregistrement historique des images principales utilisées avec chaque catalogue de machines. Restaurez les machines d'un catalogue pour utiliser la version précédente de l'image principale. Effectuez cette tâche si les utilisateurs rencontrent des problèmes avec les mises à jour déployées sur leurs bureaux. Cela réduit les temps d'inactivité des utilisateurs. Ne supprimez, déplacez ou renommez pas les images principales. Vous ne pouvez pas rétablir leur utilisation pour un catalogue.

Après qu'une machine a été mise à jour, elle redémarre automatiquement.

### Mettre à jour ou créer une image principale

Avant de mettre à jour le catalogue de machines, mettez à jour une image principale existante ou créez une image sur votre hyperviseur hôte.

1. Sur votre hyperviseur, prenez un instantané de la machine virtuelle et donnez à l'instantané un nom significatif. Cet instantané peut être utilisé pour rétablir (restaurer) des machines dans le catalogue, si nécessaire.
2. Si nécessaire, démarrez l'image principale et ouvrez une session.
3. Installez les mises à jour ou apportez les modifications requises à l'image principale.
4. Arrêtez la machine virtuelle.
5. Prenez un instantané de la machine virtuelle. Donnez-lui un nom significatif qui sera reconnu lorsque le catalogue sera mis à jour dans Web Studio. Bien que Web Studio puisse créer un instantané, Citrix vous recommande de le créer à l'aide de la console de gestion de l'hyperviseur. Sélectionnez ensuite cet instantané dans Web Studio. Cette méthode vous permet de choisir un nom et une description significatifs plutôt qu'un nom généré automatiquement. Pour les images principales GPU, vous ne pouvez modifier l'image principale que via la console XenCenter de XenServer.

### Modifier l'image principale

Pour préparer et distribuer la mise à jour à toutes les machines d'un catalogue :

1. Connectez-vous à Web Studio.
2. Sélectionnez **Catalogues de machines** dans le volet de gauche.
3. Sélectionnez un catalogue, puis sélectionnez **Modifier image principale** dans la barre d'actions.
4. Sur la page **Image**, sélectionnez l'hôte et l'image que vous voulez déployer.

   > **Conseil :**
   >
   > Pour un catalogue créé par MCS, vous pouvez annoter son image en ajoutant une note pour l'image. Une note peut contenir jusqu'à 500 caractères. Chaque fois que vous modifiez l'image principale, une entrée liée à la note est créée, que vous ajoutiez ou non une note. Si vous mettez à jour un catalogue sans ajouter de note, l'entrée apparaît sous la forme null (-). Pour afficher l'historique des notes de l'image, sélectionnez le catalogue, cliquez sur **Propriétés du modèle** dans le volet inférieur, puis sur **Afficher l'historique des notes**.

5. Sur la page **Stratégie de déploiement**, indiquez lorsque les machines du catalogue de machines doivent être mises à jour avec la nouvelle image principale : lors de la prochaine fermeture de session ou immédiatement.

> **Remarque :**
>
> La page **Stratégie de déploiement** n'est pas disponible pour les machines virtuelles persistantes car le déploiement ne s'applique qu'aux machines virtuelles non persistantes.

6. Sur la page **Résumé**, vérifiez les informations et cliquez sur **Terminer**. Chaque machine redémarre automatiquement après sa mise à jour.

Pour suivre la progression de la mise à jour, localisez le catalogue dans **Catalogues de machines** pour afficher la barre de progression intégrée et le graphique de progression étape par étape.

Lors de la mise à jour d'un catalogue directement à l'aide du SDK du PowerShell, plutôt que de Web Studio, spécifiez un modèle d'hyperviseur (**machine virtuelleTemplates**). Utilisez-le comme alternative à une image ou un instantané d'image.

**Stratégie de déploiement :**

La mise à jour des images lors de l'arrêt suivant affectera immédiatement toutes les machines qui ne sont pas en cours d'utilisation, c'est-à-dire les machines sur lesquelles aucune session utilisateur n'est active. Un système utilisé reçoit la mise à jour à la fin de la session active en cours. Tenez compte des considérations suivantes :

- Il n'est pas possible de lancer de nouvelles sessions tant que la mise à jour n'est pas terminée sur les machines applicables.
- Les machines avec OS mono session sont immédiatement mises à jour lorsque la machine n'est pas utilisée ou lorsque des utilisateurs ne sont pas connectés.
- Pour un OS multi-session avec des machines enfants, les redémarrages ne se produisent pas automatiquement. Ils doivent être arrêtés manuellement et redémarrés.

> **Conseil :**
>
> Limitez le nombre de machines redémarrées à l'aide des paramètres avancés d'une connexion hôte. Utilisez ces paramètres pour modifier les actions effectuées pour un catalogue donné ; les paramètres avancés varient en fonction de l'hyperviseur.

Si vous souhaitez activer le programme de redémarrage unique à l'aide de PowerShell, consultez la section Activer le programme de redémarrage unique.

### Restaurer l'image principale

Après avoir déployé une image principale mise à jour ou nouvelle, vous pouvez la restaurer. Cette opération peut être nécessaire si des problèmes se produisent avec les machines mises à jour. Lors de la restauration, les machines du catalogue reviennent à la dernière image fonctionnelle. Les nouvelles fonctionnalités qui nécessitent la nouvelle image ne sont plus disponibles. Comme avec le déploiement, restaurer une machine implique un redémarrage.

1. Connectez-vous à Web Studio.
2. Sélectionnez **Catalogues de machines** dans le volet de gauche.
3. Sélectionnez le catalogue, puis sélectionnez **Restaurer image principale** dans la barre d'actions.
4. Spécifiez quand appliquer la version antérieure de l'image principale aux machines, comme dans la section précédente pour l'opération de déploiement.

La restauration n'est appliquée qu'aux machines qui doivent être rétablies. Les machines qui n'ont pas été mises à jour avec l'image principale nouvelle ou mise à jour ne reçoivent pas de messages de notification et ne sont pas forcées de fermer la session.

Pour suivre la progression de la restauration, localisez le catalogue dans **Catalogues de machines** pour afficher la barre de progression intégrée et le graphique de progression étape par étape.

### Modifier le niveau fonctionnel ou annuler la modification

Modifiez le niveau fonctionnel du catalogue de machines après avoir mis à niveau les VDA des machines vers une version plus récente. Citrix recommande de mettre à niveau tous les VDA vers la version la plus récente de façon à ce qu'ils puissent tous accéder à toutes les fonctionnalités les plus récentes.

Avant de modifier le niveau fonctionnel d'un catalogue de machines :

- Démarrez les machines mises à niveau afin qu'elles s'enregistrent auprès du Controller. Cela permet à Web Studio de déterminer si les machines du catalogue doivent être mises à niveau.

Pour modifier le niveau fonctionnel d'un catalogue :

1. Connectez-vous à Web Studio.
2. Sélectionnez **Catalogues de machines** dans le volet de gauche.
3. Sélectionnez le catalogue. L'onglet **Détails** dans le volet inférieur affiche les informations de version.
4. Sélectionnez **Modifier le niveau fonctionnel**. Si Web Studio détecte que le catalogue a besoin de procéder à la mise à niveau, il affiche un message. Suivez les invites. Si une ou plusieurs machines ne peut pas être mise à niveau, un message explique pourquoi. Pour garantir le bon fonctionnement de toutes les machines, Citrix vous recommande de résoudre ces problèmes avant de cliquer sur **Modifier**.

Une fois la modification du catalogue terminée, vous pouvez rétablir les machines vers leurs versions de VDA précédentes en sélectionnant le catalogue, puis en sélectionnant **Annuler modification du niveau fonctionnel** dans la barre d'actions.

### Cloner un catalogue

Avant de cloner un catalogue, prenez en compte les informations suivantes :

- Vous ne pouvez pas modifier les paramètres associés à la gestion des systèmes d'exploitation et des machines. Le catalogue cloné hérite de ces paramètres de l'original.
- Le clonage d'un catalogue peut prendre un certain temps. Si nécessaire, sélectionnez **Masquer la progression** pour exécuter le clonage en arrière-plan.
- Le catalogue cloné hérite du nom de l'original et comporte un suffixe Copy. Vous pouvez modifier le nom. Consultez la section Renommer un catalogue.
- Une fois le clonage terminé, veillez à attribuer le catalogue cloné à un groupe de mise à disposition.

1. Connectez-vous à Web Studio, puis sélectionnez **Catalogues de machines** dans le volet de gauche.
2. Sélectionnez un catalogue, puis sélectionnez **Cloner** dans la barre d'actions.
3. Dans la fenêtre **Cloner le catalogue de machines sélectionné**, affichez les paramètres du catalogue cloné et configurez les paramètres le cas échéant. Sélectionnez **Suivant** pour passer à la page suivante.
4. Sur la page **Résumé**, affichez un résumé des paramètres et sélectionnez **Terminer** pour commencer le clonage.
5. Si nécessaire, sélectionnez **Masquer la progression** pour exécuter le clonage en arrière-plan.

### Organiser les catalogues sous forme de dossiers

Vous pouvez créer des dossiers pour organiser les catalogues afin d'en faciliter l'accès. Par exemple, vous pouvez organiser les catalogues par type d'image ou par structure organisationnelle.

#### Créer un dossier de catalogues

Avant de commencer, planifiez d'abord comment organiser vos catalogues. Tenez compte des considérations suivantes :

- Vous pouvez imbriquer des dossiers sur un maximum de cinq niveaux de profondeur (à l'exception du dossier racine par défaut).
- Un dossier de catalogues peut contenir des catalogues et des sous-dossiers.
- Tous les nœuds dans Web Studio (tels que les nœuds **Catalogues de machines** et **Applications**) partagent une arborescence de dossiers dans le back-end. Pour éviter les conflits de nom avec d'autres nœuds lorsque vous renommez ou déplacez des dossiers, nous vous recommandons de donner des noms différents aux dossiers de premier niveau dans différents nœuds.

Pour créer un dossier de catalogues, procédez comme suit :

1. Sélectionnez **Catalogues de machines** dans le volet de gauche.
2. Dans la hiérarchie des dossiers, sélectionnez un dossier, puis sélectionnez **Créer un dossier** dans la barre **d'actions**.
3. Entrez un nom pour le nouveau dossier, puis cliquez sur **Terminé**.

> **Conseil :**
>
> Si vous créez un dossier dans le mauvais emplacement, vous pouvez le faire glisser vers l'emplacement approprié.

#### Déplacer un catalogue

Vous pouvez déplacer un catalogue d'un dossier à l'autre. Les étapes détaillées sont les suivantes :

1. Sélectionnez **Catalogues de machines** dans le volet de gauche.
2. Afficher les catalogues par dossier. Vous pouvez également activer **Afficher tout** au-dessus de la hiérarchie des dossiers pour afficher tous les catalogues à la fois.
3. Cliquez avec le bouton droit sur un catalogue puis sélectionnez **Déplacer catalogue de machines**
4. Sélectionnez le dossier vers lequel vous souhaitez déplacer le catalogue, puis cliquez sur **Terminé**.

> **Conseil :**
>
> Vous pouvez faire glisser un catalogue vers un dossier.

#### Gérer les dossiers de catalogues

Vous pouvez supprimer, renommer et déplacer des dossiers de catalogues.

Vous ne pouvez supprimer un dossier que si celui-ci et ses sous-dossiers ne contiennent pas de catalogues.

Pour gérer un dossier, procédez comme suit :

1. Sélectionnez **Catalogues de machines** dans le volet de gauche.
2. Dans la hiérarchie des dossiers, sélectionnez un dossier, puis sélectionnez une action dans la barre **d'actions** selon vos besoins :
   - Pour renommer le dossier, sélectionnez **Renommer le dossier**.
   - Pour supprimer le dossier, sélectionnez **Supprimer le dossier**.
   - Pour déplacer le dossier, sélectionnez **Déplacer le dossier**.

3. Suivez les instructions à l'écran pour effectuer les étapes restantes.

### Utiliser PowerShell

Cette section explique comment gérer les catalogues à l'aide de PowerShell :

- Récupérer les erreurs et les avertissements associés à un catalogue
- Activer le calendrier de redémarrage unique
- Ajouter des descriptions à une image
- Réinitialiser le disque d'OS
- Modifier le paramètre réseau pour un schéma de provisioning existant
- Gérer les versions d'un catalogue de machines
- Convertissez un catalogue de machines non basé sur un profil de machine vers un catalogue de machines basé sur un profil de machine
- Réparer les informations d'identité des comptes d'ordinateur actifs
- Modifier la configuration du cache sur un catalogue de machines existant
- Prise en charge des mises à jour du VDA via l'accès au partage de fichiers local

### Récupérer les erreurs et les avertissements associés à un catalogue

Vous pouvez consulter l'historique des erreurs et des avertissements pour comprendre les problèmes liés à votre catalogue de machines MCS et les résoudre.

À l'aide des commandes PowerShell, vous pouvez :

- Obtenir une liste d'erreurs ou d'avertissements
- Changer l'état d'avertissement de **New** à **Acknowledged**
- Supprimer les erreurs ou les avertissements

Pour exécuter les commandes PowerShell :

1. Ouvrez une fenêtre PowerShell.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.

Pour obtenir la liste des erreurs et des avertissements :

Exécutez la commande `Get-ProvOperationEvent`.

- Aucun paramètre : affiche toutes les erreurs et tous les avertissements.
- Paramètre `LinkedObjectType` et `LinkedObjectUid` : affiche toutes les erreurs et tous les avertissements associés à un schéma de provisioning spécifique.
- Paramètre `EventId` : affiche une erreur ou un avertissement spécifique correspondant à cet ID d'événement.

- Paramètre `Filter` : affiche des erreurs ou des avertissements par filtre personnalisé.

Pour changer l'état des erreurs ou des avertissements de **New** à **Acknowledged** :

Exécutez la commande `Confirm-ProvOperationEvent`.

- Paramètre `EventId` : définit l'état d'une erreur ou d'un avertissement spécifique correspondant à cet ID d'événement. Vous pouvez obtenir l'élément `EventId` d'une erreur ou d'un avertissement spécifique en tant que sortie de la commande `Get-ProvOperationEvent`.
- Paramètre `LinkedObjectType` et `LinkedObjectUid` : définit l'état de toutes les erreurs et de tous les avertissements associés à un schéma de provisioning spécifique.
- Paramètre `All` : définit l'état de toutes les erreurs et de tous les avertissements sur **Acknowledged**.

Pour supprimer les erreurs ou les avertissements :

Exécutez la commande `Remove-ProvOperationEvent`.

- Paramètre `EventId` : supprime une erreur ou un avertissement spécifique correspondant à cet ID d'événement. Vous pouvez obtenir l'élément `EventId` d'une erreur ou d'un avertissement spécifique en tant que sortie de la commande `Get-ProvOperationEvent`.
- Paramètre `LinkedObjectType` et `LinkedObjectUid` : supprime toutes les erreurs et tous les avertissements associés à un schéma de provisioning spécifique.
- Paramètre `All` : supprime toutes les erreurs et tous les avertissements.

Pour plus d'informations, accédez à cette page sur le SDK Citrix PowerShell.

### Activer le calendrier de redémarrage unique

Si vous souhaitez activer le programme de redémarrage unique à l'aide de PowerShell, utilisez les commandes PowerShell `BrokerCatalogRebootSchedule` suivantes pour créer, modifier et supprimer un programme de redémarrage :

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- Remove-BrokerCatalogRebootSchedule
- Rename-BrokerCatalogRebootSchedule

Par exemple,

- Pour créer un programme de redémarrage des machines virtuelles du catalogue nommé **BankTellers**, qui débute le 3 février 2022, entre 2 h et 4 h du matin.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -
    CatalogName BankTellers  -StartDate "2022-02-03" -StartTime "
    02:00" -Enabled $true -RebootDuration 120
<!--NeedCopy-->
```

- Pour créer un programme de redémarrage des machines virtuelles du catalogue ayant l'UID 17, qui débute le 3 février 2022, entre 1 h et 5 h du matin. Dix minutes avant le redémarrage, chaque machine virtuelle est configurée pour afficher un message avec le titre, **WARNING: Reboot pending**, et le message **Save your work** à chaque session utilisateur.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot' -
    CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -
    Enabled $true -RebootDuration 240 -WarningTitle "WARNING:
    Reboot pending" -WarningMessage "Save your work" -
    WarningDuration 10
<!--NeedCopy-->
```

- Pour renommer le programme de redémarrage de catalogue intitulé **Old Name** en **New Name**.

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -
    NewName "New Name"
<!--NeedCopy-->
```

- Pour afficher tous les programmes de redémarrage de catalogue avec l'UID 1, puis renommer le programme de redémarrage du catalogue avec l'UID 1 en **New Name**.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
    BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
<!--NeedCopy-->
```

- Pour définir le programme de redémarrage de catalogue nommé **Accounting** afin d'afficher un message intitulé **WARNING: Reboot pending et le message Save your work** dix minutes avant le redémarrage de chaque machine virtuelle. Le message apparaît à chaque session utilisateur sur cette machine virtuelle.

  ‘‘‘

  C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage “Save your work”-WarningDuration 10 -WarningTitle “WARNING: Reboot pending”

- Pour afficher tous les programmes de redémarrage désactivés, puis activer tous les programmes de redémarrage désactivés.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
    BrokerCatalogRebootSchedule -Enabled $true
<!--NeedCopy-->
```

- Pour définir le programme de redémarrage de catalogue avec l'UID 17 afin d'afficher le message **Rebooting in %m% minutes** quinze, dix et cinq minutes avant le redémarrage de chaque machine virtuelle.

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "
    Rebooting in %m% minutes." -WarningDuration 15 -
    WarningRepeatInterval 5
<!--NeedCopy-->
```

- Pour configurer le fuseau horaire du catalogue nommé **MyCatalog**.

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
<!--NeedCopy-->
```

### Ajouter des descriptions à une image

Vous pouvez ajouter des descriptions informatives sur les modifications liées aux mises à jour des images pour les catalogues de machines. Utilisez cette fonctionnalité pour ajouter une description lors de la création d'un catalogue ou lorsque vous mettez à jour une image principale existante pour un catalogue. Vous pouvez également afficher des informations pour chaque image principale du catalogue. Utilisez les commandes suivantes pour ajouter ou afficher des descriptions d'images :

- Pour ajouter une note lors de la création d'un catalogue de machines avec une image principale, utilisez le paramètre `MasterImageNote` de la commande `NewProvScheme`. Par exemple :

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -
    HostingUnitName <name> -IdentityPoolName <name> -MasterImageVM
XDHyp:\HostingUnits<hosting unit name><vm name>.vm\Base.snapshot
    -MasterImageNote "Note"
<!--NeedCopy-->
```

- Pour mettre à jour l'image principale associée à un catalogue de machines, utilisez le paramètre `MasterImageNote` de la commande `Publish-ProvMasterVMImage`. Par exemple :

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name> -
    MasterImageVM XDHyp:\HostingUnits<hosting unit name><vm name>.
    vm\base.snapshot -MasterImageNote "Note"
<!--NeedCopy-->
```

- Pour afficher les informations relatives à chaque image, utilisez la commande Get-ProvSchemeMasterVMImageHistory. Par exemple :

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall
<!--NeedCopy-->
```

Pour suivre la progression de la restauration, localisez le catalogue dans **Catalogues de machines** pour afficher la barre de progression intégrée et le graphique de progression étape par étape.

Vous ne pouvez pas effectuer de restauration dans certains scénarios, notamment les suivants. (L'option **Restaurer image principale** n'est pas visible).

- Vous n'êtes pas autorisé à effectuer de restauration.
- Le catalogue n'a pas été créé à l'aide de MCS.
- Le catalogue a été créé à l'aide d'une image du disque du système d'exploitation.
- L'instantané utilisé pour créer le catalogue est endommagé.
- Les modifications apportées par l'utilisateur aux machines du catalogue ne sont pas conservées.
- Les machines du catalogue sont en cours d'exécution.

### Réinitialiser le disque d'OS

Utilisez la commande PowerShell `Reset-ProvVMDisk` pour réinitialiser le disque d'OS d'une machine virtuelle persistante dans un catalogue de machines créé par MCS. Actuellement, cette fonctionnalité est applicable à AWS, Azure, XenServer et Google Cloud. Environnements de virtualisation SCVMM et VMware.

Pour exécuter correctement la commande PowerShell, assurez-vous que :

- Les machines virtuelles cibles se trouvent dans un catalogue MCS persistant.
- Le catalogue de machines MCS fonctionne correctement.
- Cela implique que le schéma de provisioning et l'hôte existent et que le schéma de provisioning contient des entrées correctes.
- L'hyperviseur n'est pas en mode de maintenance.
- Les machines virtuelles cibles sont hors tension et en mode de maintenance.

Procédez comme suit pour réinitialiser le disque d'OS :

1. Ouvrez une fenêtre PowerShell.
2. Exécutez **asnp citrix*** pour charger des modules PowerShell spécifiques à Citrix.
3. Exécutez la commande PowerShell `Reset-ProvVMDisk` de l'une des manières suivantes :

    - Spécifiez la liste des machines virtuelles sous forme de liste séparée par des virgules et effectuez la réinitialisation sur chaque machine virtuelle :

    ```
    Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc"
        ,"def") -OS
    <!--NeedCopy-->
    ```

    - Spécifiez la liste des machines virtuelles sous forme de sortie de la commande `Get-ProvVM` et effectuez la réinitialisation sur chaque machine virtuelle :

    ```
    (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
        "abc" -OS
    <!--NeedCopy-->
    ```

- Spécifiez une seule machine virtuelle par son nom :

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS
<!--NeedCopy-->
```

- Créez des tâches de réinitialisation distinctes pour chacune des machines virtuelles renvoyées par la commande `Get-ProvVM`. Cette méthode est moins efficace car chaque tâche effectuera les mêmes vérifications redondantes, telles que la vérification de la capacité de l'hyperviseur et la vérification de la connexion pour chaque machine virtuelle.

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -OS
<!--NeedCopy-->
```

4. Une invite de confirmation apparaît, répertoriant les machines virtuelles à réinitialiser, ainsi qu'un message d'avertissement indiquant qu'il s'agit d'une opération irrécupérable. Si vous ne fournissez pas de réponse et que vous appuyez sur **Entrée**, aucune autre action n'aura lieu.

> **Remarque :**
>
> Ne retirez pas les machines virtuelles du mode de maintenance et ne les mettez pas sous tension avant la fin du processus de réinitialisation.

Vous pouvez exécuter la commande PowerShell `-WhatIf` pour afficher l'action qu'elle entreprendrait et quitter sans effectuer l'action.

Vous pouvez également contourner l'invite de confirmation en utilisant l'une des méthodes suivantes :

- Fournissez le paramètre `-Force` :

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Force
<!--NeedCopy-->
```

- Fournissez le paramètre `-Confirm:$false` :

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Confirm:$false
<!--NeedCopy-->
```

- Avant d'exécuter `Reset-ProvVMDisk`, définissez `$ConfirmPreference` sur **None** :

```
PS C:\Windows\system32> $ConfirmPreference='None'
PS C:\Windows\system32> $ConfirmPreference
None
PS C:\Windows\system32> Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -VMName "abc" -OS
<!--NeedCopy-->
```

5. Exécutez `Get-ProvTask` pour obtenir l'état des tâches renvoyées par la commande `Reset-ProvVMDisk`.

### Modifier le paramètre réseau pour un schéma de provisioning existant

Vous pouvez modifier le paramètre réseau d'un schéma de provisioning existant afin que les nouvelles machines virtuelles soient créées sur le nouveau sous-réseau. Utilisez le paramètre `-NetworkMapping` dans la commande `Set-ProvScheme` pour modifier le paramètre réseau.

> **Remarque :**
>
> Cette fonctionnalité est compatible avec Citrix Virtual Apps and Desktops 2203 LTSR CU3 et les versions ultérieures.

Pour modifier le paramètre réseau d'un schéma de provisioning existant, procédez comme suit :

1. Dans la fenêtre PowerShell, exécutez la commande `asnp citrix*` pour charger les modules PowerShell.
2. Exécutez `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` pour accéder au chemin réseau que vous souhaitez modifier.
3. Affectez une variable au nouveau paramètre réseau. Par exemple :

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }

<!--NeedCopy-->
```

4. Exécutez `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap`.
5. Exécutez `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` pour vérifier le nouveau paramètre réseau pour le schéma de provisioning existant.

### Gérer les versions d'un catalogue de machines

Lorsqu'un catalogue de machines MCS est mis à jour à l'aide de la commande `Set-ProvScheme`, la configuration actuelle est enregistrée en tant que version. Vous pouvez ensuite gérer les différentes versions du catalogue de machines à l'aide des commandes PowerShell. Vous pouvez :

- Voir la liste des versions d'un catalogue de machines
- Utiliser n'importe quelle version précédente pour mettre à jour le catalogue de machines
- Supprimer manuellement une version si elle n'est pas utilisée par une machine virtuelle de ce catalogue de machines

- Modifier le nombre maximum de versions à conserver par le catalogue de machines (la valeur par défaut est 99)

Une version inclut les informations suivantes relatives à un catalogue de machines :

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

Exécutez les commandes suivantes (fournies à titre d'exemples) pour gérer les différentes versions d'un catalogue de machines.

- Pour consulter les détails de configuration des différentes versions d'un catalogue de machines :

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

- Pour consulter les détails de configuration d'une version spécifique d'un catalogue de machines :

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
    Version 2
<!--NeedCopy-->
```

- Pour voir le nombre total de versions associées à un catalogue de machines :

  ‘‘‘

  (Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count

- Pour utiliser une version précédente afin de mettre à jour le catalogue de machines :

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
<!--NeedCopy-->
```

- Pour supprimer manuellement une version non utilisée par une machine virtuelle de ce catalogue de machines :

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
    Version 3
<!--NeedCopy-->
```

- Pour définir le nombre maximum de versions à conserver par le catalogue de machines (la valeur par défaut est 99). Ce paramètre est appliqué à tous les catalogues. Par exemple, dans ce cas, un maximum de 15 versions seront conservées pour tous les catalogues fournis par MCS.

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -
    Value 15
<!--NeedCopy-->
```

Si le nombre de versions atteint le nombre maximum de versions, aucune nouvelle version ne peut être créée si d'anciennes versions sont utilisées par l'une des machines virtuelles du catalogue de machines. Effectuez alors l'une des opérations suivantes :

- Augmentez la limite du nombre maximum de versions à conserver par le catalogue de machines.
- Mettez à jour certaines machines virtuelles qui se trouvent sur des versions plus anciennes afin que ces anciennes versions ne soient plus référencées par aucune machine virtuelle et puissent être supprimées.

### Convertissez un catalogue de machines non basé sur un profil de machine vers un catalogue de machines basé sur un profil de machine

Vous pouvez utiliser une machine virtuelle, une spécification de modèle (dans le cas d'Azure) ou un modèle de lancement (dans le cas d'AWS) comme entrée de profil de machine pour convertir un catalogue de machines non basé sur un profil de machine vers un catalogue de machines basé sur un profil de machine. Les nouvelles machines virtuelles ajoutées au catalogue utilisent les valeurs des propriétés du profil de la machine, à moins qu'elles ne soient remplacées par des propriétés personnalisées explicites.

> **Remarque :**
>
> Un catalogue de machines existant basé sur un profil de machine ne peut pas être remplacé par un catalogue de machines non basé sur un profil de machine.

Pour ce faire :

1. Créez un catalogue de machines persistant ou non persistant avec des machines virtuelles et sans profil de machine.
2. Ouvrez la fenêtre **PowerShell**.
3. Exécutez la commande `Set-ProvScheme` pour appliquer les valeurs des propriétés du profil de machine aux nouvelles machines virtuelles ajoutées au catalogue de machines. Par exemple :
    - Dans le cas d'Azure :

```
Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
    -MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    machineprofile.folder<ResourceGroupName><TemplateSpecName
    ><VersionName>
```

```
<!--NeedCopy-->
```

- Dans le cas d'AWS :

```
Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
    -MachineProfile "XDHyp:\HostingUnits<hosting-unit><launch-
    template>.launchtemplate<launch-template-version>.
    launchtemplateversion"
<!--NeedCopy-->
```

### Réparer les informations d'identité des comptes d'ordinateur actifs

Vous pouvez réinitialiser les informations d'identité des comptes informatiques actifs présentant des problèmes liés à l'identité. Vous pouvez choisir de réinitialiser uniquement le mot de passe de la machine et les clés de confiance, ou de réinitialiser toute la configuration du disque d'identité. Cette mise en œuvre est applicable aux catalogues de machines MCS persistants et non persistants.

> **Remarque :**
>
> Actuellement, cette fonctionnalité n'est prise en charge que pour les environnements de virtualisation Azure et VMware.

#### Conditions

Prenez compte des points suivants pour réinitialiser correctement le disque d'identité :

- Éteignez et réglez la machine virtuelle en mode maintenance
- N'incluez pas le paramètre -OS dans la commande PowerShell

#### Réinitialiser le disque d'identité

Pour réinitialiser le disque d'identité :

1. Ouvrez la fenêtre **PowerShell**.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Réinitialisez les informations d'identité.
    - Pour réinitialiser uniquement le mot de passe de la machine et les clés de confiance, exécutez les commandes suivantes dans l'ordre suivant :

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
    PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
    $password -Target IdentityInfo
<!--NeedCopy-->
```

Descriptions des paramètres utilisés dans la commande :

- `IdentityAccountName` : nom du compte d'identité qui doit être réparé.
- `PrivilegedUserName` : compte utilisateur disposant d'une autorisation d'écriture sur le fournisseur d'identité (AD ou AzureAD).
- `PrivilegedUserPassword` : mot de passe pour PrivilegedUserName.
- `Target` : cible de l'action de réparation. Cela peut être IdentityInfo pour réparer le mot de passe/la clé de confiance du compte, et UserCertificate pour réparer les attributs du certificat utilisateur des identités de machines jointes à AzureAD hybride.

```
1  Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name
       > -Identity -ResetIdentityInfo
2  <!--NeedCopy-->
```

Le paramètre `ResetIdentityInfo` réinitialise les éléments suivants :

- Mot de passe et clés de confiance : si la machine virtuelle est jointe au domaine AD (pour la documentation DaaS uniquement)
- Clés de confiance uniquement : si la machine virtuelle n'est pas jointe au domaine AD (pour la documentation DaaS uniquement)
- Mot de passe uniquement : si la machine virtuelle est jointe au domaine AD (pour la documentation CVAD sur site uniquement)

- Pour réinitialiser toutes les configurations du disque d'identité, exécutez ces commandes dans l'ordre suivant :

```
1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
       PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
       $password -Target IdentityInfo
2  <!--NeedCopy-->
```

```
1  Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
        -Identity
2  <!--NeedCopy-->
```

4. Tapez **y** pour confirmer l'action. Vous pouvez également ignorer l'invite de confirmation à l'aide du paramètre `-Force`. Par exemple :

```
1 Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
     Identity -Force
2 <!--NeedCopy-->
```

5. Exécutez `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` pour vérifier les paramètres de disque d'identité mis à jour. Les attributs du disque d'identité (par exemple, `IdentityDiskId`) doivent être mis à jour. `StorageId` et `IdentityDiskIndex` ne doivent pas changer.

### Modifier la configuration du cache sur un catalogue de machines existant

Après avoir créé un catalogue non persistant avec MCSIO activé, vous pouvez utiliser la commande Set-ProvScheme pour modifier les paramètres suivants :

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

Cette fonctionnalité est actuellement applicable à :

- des environnements GCP et Microsoft Azure, et
- un catalogue non persistant avec MCSIO activé

#### Exigences

Les conditions requises pour modifier la configuration du cache sont les suivantes :

- Effectuez la mise à jour vers la dernière version du VDA (2308 ou version ultérieure).
- Activez le paramètre `UseWriteBackCache` pour le catalogue de machines existant. Utilisez-`New-ProvScheme` pour créer un catalogue de machines avec `UseWriteBackCache` activé. Par exemple :

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -
   HostingUnitUid $HostingUnitUid `
-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
-MasterImageVM $MasterImage `
-ServiceOffering $ServiceOffering `
-NetworkMap $NetworkMap `
-SecurityGroup $SecurityGroup `
-UseWriteBackCache -WriteBackCacheDiskSize 8
<!--NeedCopy-->
```

#### Modifier la configuration du cache

Exécutez la commande Set-ProvScheme. Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.
   ProvisioningSchemeName -WriteBackCacheDisk32 -
   WriteBackCacheMemorySize 128
<!--NeedCopy-->
```

> **Remarque :**
>
> - La valeur de `WriteBackCacheDiskSize` doit être supérieure à zéro car un minimum de 1 Go de stockage sur disque cache est requis.

> - La valeur de `WriteBackCacheMemorySize` doit être inférieure à la taille de la mémoire du catalogue de machines.
> - Ces modifications n'affectent que les nouvelles machines virtuelles ajoutées au catalogue une fois la modification apportée. Les machines virtuelles existantes ne sont pas affectées par ces modifications.

## Prise en charge des mises à jour du VDA via l'accès au partage de fichiers local

Spécifiez l'emplacement du programme d'installation du VDA via les applets de commande PowerShell, ce qui vous évite d'avoir à fournir des règles réseau permettant à chaque VDA d'aller récupérer le nouveau programme d'installation du VDA depuis le CDN Azure géré par Citrix.

### Applets de commande PowerShell

Deux nouveaux paramètres facultatifs ont été ajoutés aux applets de commande **New-VusCatalogSchedule** et **New-VusMachineUpgrade**, qui vous permettent d'utiliser des programmes d'installation à partir d'un partage de fichiers local.

- **VdaWorkstationPackageUri** : pour spécifier le chemin d'accès UNC vers le programme d'installation du VDA du système d'exploitation du poste de travail
- **VdaServerPackageUri** : pour spécifier le chemin d'accès UNC vers le programme d'installation du VDA du système d'exploitation du serveur

### Logiciel requis

- Programme d'installation de l'agent VUS fourni avec le VDA 2311
- Agent de mise à niveau de VDA vers la version 7.40.0.35 ou ultérieure (à l'aide de la version 2311 ou ultérieure du programme d'installation de VDA)
- Virtual Apps and Desktops Remote PowerShell SDK version 7.40 ou ultérieure (publié le 10 janvier 2024 ou version ultérieure)

### Procédure pour définir les autorisations de partage de fichiers

Les partages réseau contenant les packages d'installation de VDA doivent disposer d'un accès en lecture pour le service VDA Upgrade Agent qui s'exécute en tant que système local (principal NT AUTHORITY\SYSTEM).

- **Autorisation de partage de fichiers joints à un domaine**

Lorsque la machine VDA est jointe à un domaine, le compte **Système local** (VUA s'exécute en tant que Système local) utilise les informations d'identification de l'ordinateur pour accéder aux partages réseau.

L'autorisation de moindre privilège peut être définie en accordant l'accès en **lecture** aux ordinateurs du domaine.

1. Choisissez les personnes de votre réseau avec lesquelles vous souhaitez partager le fichier.
2. Cliquez sur **Advanced Sharing Settings** et activez **File and Printer Sharing**.

- **Autorisation de partage de fichiers non joints au domaine**

  Lorsque la machine VDA n'est pas jointe à un domaine, le compte **Système local** (VUA s'exécute en tant que Système local) utilise **ANONYMOUS LOGON** pour accéder aux partages réseau.

  1. Sélectionnez un dossier partagé.
  2. Désactivez la protection par mot de passe.
     a) Accédez aux **Propriétés** du dossier.
     b) Sélectionnez **Centre Réseau et partage**.
     c) Désactivez l'option **Partage protégé par mot de passe**.
  3. Cliquez sur **Partage avancé** pour accorder une autorisation de partage.
     a) Sélectionnez **Autorisations**.
     b) Accordez une autorisation de partage en **lecture** à **ANONYMOUS LOGON**.
  4. Sélectionnez l'**onglet Sécurité** pour accorder des autorisations sur les dossiers.
     a) Cliquez sur **Modifier** pour ajouter des autorisations au dossier partagé.
     b) Sélectionnez le dossier partagé pour accorder des autorisations de dossier à **ANONYMOUS LOGON**.
  5. Cliquez sur **Avancé** pour activer le **Partage de fichiers et d'imprimantes**.
  6. Ajoutez le nom du dossier partagé à la **Stratégie de sécurité d'accès réseau**.

  > **Remarque :**
  >
  > Redémarrez votre machine pour que la modification prenne effet immédiatement.

#### Mises à jour du VDA à partir d'un partage de fichiers local

1. Téléchargez le programme d'installation du VDA et placez-le dans le fichier partagé.

   > **Remarque :**
   >
   > Avec Virtual Upgrade Service, vous pouvez choisir entre la voie Current Release ou la voie LTSR.
   >
   > **Par exemple :** si le catalogue de machines est défini sur la version actuelle qui est 2311 et

> que la version du VDA est 2305, vous devez mettre à niveau le VDA vers la version 2311.

a) Accédez à la page **Téléchargements** de notre site Web.
b) Sélectionnez le produit **Citrix Virtual Apps and Desktops**.
c) Sélectionnez **Citrix Virtual Apps and Desktops 7 2311, All Editions**.
d) Sélectionnez le programme d'installation du VDA dans le menu déroulant **Components that are on product ISO but also packaged separately**.

2. Sélectionnez le programme d'installation VDA approprié en fonction du type de catalogue.

   - Téléchargez **Multi-session OS VDA installer** si le type de catalogue est **multi-session**.
   - Téléchargez **Single-session OS VDA installer** si le type de catalogue est **mono-session**.
   - Téléchargez **Single-session OS Core Services VDA installer** si le type de catalogue est **Remote PC Access**.

> **Remarque :**
>
> La version du programme d'installation du partage de fichiers doit correspondre **exactement** à la version de la dernière version du programme d'installation publiée par VUS sur le cloud.

### Dépannage

- Pour les machines affichant un « état d'alimentation inconnu », consultez l'article CTX131267 pour plus d'informations.
- Pour réparer les machines virtuelles qui affichent en permanence un état d'alimentation inconnu, consultez l'article How to fix machine virtuelles that continuously show an unknown power state.

### Autres ressources

Pour plus d'informations sur la gestion de catalogues de services cloud spécifiques, consultez :

- Gérer un catalogue AWS
- Gérer un catalogue XenServer
- Gérer un catalogue Google Cloud Platform
- Gérer un catalogue Microsoft Azure
- Gérer un catalogue Microsoft System Center Virtual Machine Manager
- Gérer un catalogue VMware

# Gérer un catalogue AWS

June 27, 2024

Gérer les catalogues de machines décrit les assistants qui permettent de gérer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements de cloud AWS.

> **Remarque :**
>
> Avant de gérer un catalogue AWS, vous devez terminer de créer un catalogue AWS. Voir Créer un catalogue AWS.

## Supprimer les balises

Lorsque vous créez un catalogue ou une machine virtuelle, des balises sont créées par MCS sur les ressources suivantes :

- Machine virtuelle
- Volume du disque racine
- Volume du disque d'identité
- Carte d'interface réseau
- Image du disque racine (AMI)
- Modèle de lancement
- Capture d'écran de l'AMI ou du disque racine

Vous pouvez supprimer des machines virtuelles et des catalogues de machines de la base de données Citrix et supprimer les balises créées par Citrix. Vous pouvez utiliser :

- `Remove-ProvVM` avec le paramètre `ForgetVM` pour supprimer des balises créées par MCS et machines virtuelles d'une machine virtuelle unique ou d'une liste d'entre elles d'un catalogue de machines.
- `Remove-ProvScheme` avec le paramètre `ForgetVM` pour supprimer un catalogue de machines de la base de données Citrix et les ressources d'un catalogue de machines.

Cette fonctionnalité s'applique uniquement aux machines virtuelles persistantes.

Pour ce faire :

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Déverrouillez la machine virtuelle avant de la supprimer. Par exemple :

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
<!--NeedCopy-->
```

4. Exécutez l'une des commandes suivantes pour supprimer des machines virtuelles, un catalogue de machines et des balises créees par MCS de ressources.

   - Exécutez `Remove-ProvVM` avec `ForgetVM` pour supprimer des machines virtuelles de la base de données Citrix et des balises de machines virtuelles. Par exemple :

     ```
     Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name
        >" -ForgetVM
     <!--NeedCopy-->
     ```

   - Exécutez `Remove-ProvScheme` pour supprimer un catalogue de machines de la base de données Citrix et des ressources d'un catalogue de machines. Par exemple :

     ```
     Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -
        ForgetVM
     <!--NeedCopy-->
     ```

5. Vérifiez que la machine virtuelle est supprimée du Delivery Controller, mais pas de l'hyperviseur.

   a) Exécutez `Get-ProvVM -ProvisioningSchemeName "<name>"-VMName "<name>"`. Cela ne doit rien retourner.

   b) Accédez à la console EC2 d'AWS. Vous devez voir les machines virtuelles, mais les balises sont maintenant supprimées. Les balises des ressources suivantes sont supprimées :

      - Machine virtuelle
      - Volume du disque racine
      - Volume du disque d'identité
      - Carte d'interface réseau

6. Si vous supprimez le catalogue de machines, vérifiez que le catalogue est supprimé du Delivery Controller.

   a) Exécutez `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`. Cela doit renvoyer une erreur.

   b) Vérifiez dans la console EC2 d'AWS que les ressources suivantes sont supprimées.

      - Image du disque racine (AMI)
      - Modèle de lancement
      - Capture d'écran de l'AMI ou du disque racine

### Identifier les ressources créées par MCS

Voici les balises que MCS ajoute aux ressources. Les balises du tableau sont représentées au format “clé”:”valeur”.

| Nom de la ressource | Balise |
| --- | --- |
| Disque d’identification | “Name”: “machine virtuelleName_IdentityDisk” |
| | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Image | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Carte d’interface réseau | “Description”: “XD NIC” |
| | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Disque OS | “Name”: “machine virtuelleName_rootDisk” |
| | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| | [when AwsCaptureInstanceProperties = true] “Citrix Resource”: “” |
| | [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| Machine virtuelle de préparation | “Name”: “Preparation - CatalogName - xxxxxxxxxx” |
| | “XdConfig”: “XdProvisioned=true” |
| | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| | [when AwsCaptureInstanceProperties = true] “Citrix Resource”: “” |
| | [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| Instantané publié | “XdConfig”: “XdProvisioned=true” |

| Nom de la ressource | Balise |
| --- | --- |
| Modèle | S'il ne s'agit pas d'un instantané pour AMI travailleur de volume, alors "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" [when AwsCaptureInstanceProperties = true] "XdConfig": "XdProvisioned=true" [when AwsCaptureInstanceProperties = true] "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" [when AwsCaptureInstanceProperties = true] "CitrixResource": "" [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": "" |
| machine virtuelle dans le catalogue | "XdConfig": "XdProvisioned=true" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" [when AwsCaptureInstanceProperties = true] "CitrixResource": "" [when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:id":"lt-xxxx" [when AwsCaptureInstanceProperties = true] "aws:ec2launchtemplate:version": "n" [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixOperationalResource": "" |
| AMI travailleur de volume | "XdConfig": "XdProvisioned=true" |
| Bootstraper travailleur de volume | "Name": "XenDesktop Temp" "XdConfig": "XdProvisioned=true" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" [when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] "CitrixVolumeWorkerBootstrapper": "" |
| Instance travailleur de volume | "Name": "Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx" |

| Nom de la ressource | Balise |
| --- | --- |
| | “XdConfig”: “XdProvisioned=true” |

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à AWS
- Créer des catalogues de machines
- Créer un catalogue AWS
- Gérer des catalogues de machines

## Gérer un catalogue XenServer

June 27, 2024

Gérer les catalogues de machines décrit les assistants qui permettent de gérer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements de virtualisation XenServer.

> **Remarque :**
>
> Avant de gérer un catalogue XenServer, vous devez terminer la création d’un catalogue XenServer. Voir Créer un catalogue XenServer.

### Identifier les ressources créées par MCS

Voici les balises que MCS ajoute aux ressources. Les balises du tableau sont représentées au format “clé”:”valeur”.

| Nom de la ressource | Balise |
| --- | --- |
| Disque de base publié et sa copie sur chaque réseau ou stockage local | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Disque d’identification | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Disque OS | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |

| Nom de la ressource | Balise |
| --- | --- |
| machine virtuelle de préparation | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| machine virtuelle dans le catalogue | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Disque WBC | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à XenServer
- Créer des catalogues de machines
- Créer un catalogue XenServer
- Gérer des catalogues de machines

## Gérer un catalogue Google Cloud Platform

June 27, 2024

Gérer les catalogues de machines décrit les assistants qui permettent de gérer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements Google Cloud.

> **Remarque :**
>
> Avant de gérer un catalogue Google Cloud Platform, vous devez terminer de créer un catalogue Google Cloud Platform. Voir Créer un catalogue Google Cloud Platform.

### Gérer un catalogue de machines

Pour ajouter des machines à un catalogue, mettre à jour des machines et restaurer une mise à jour, consultez Gérer des catalogues de machines.

### Gestion de l’alimentation

Citrix DaaS vous permet de gérer l’alimentation des machines Google Cloud. Utilisez le nœud **Rechercher** dans le volet de gauche pour localiser la machine dont vous souhaitez gérer l’alimenta-

tion. Les actions de gestion de l'alimentation suivantes sont disponibles :

- Supprimer
- Démarrer
- Redémarrer
- Forcer le redémarrage
- Arrêter
- Forcer l'arrêt
- Ajouter au groupe de mise à disposition
- Gérer les balises
- Activer le mode de maintenance

Vous pouvez également gérer l'alimentation des machines Google Cloud à l'aide de la fonctionnalité Autoscale. Pour ce faire, ajoutez les machines Google Cloud à un groupe de mise à disposition, puis activez la fonctionnalité Autoscale pour ce groupe de mise à disposition. Pour plus d'informations sur la fonctionnalité Autoscale, consultez la section Autoscale.

#### Mettre à jour les machines provisionnées à l'aide de PowerShell

La commande `Set-ProvScheme` modifie le schéma de provisioning. Toutefois, ce script n'affecte pas les machines existantes. À l'aide de la commande PowerShell `Set-ProvVMUpdateTimeWindow`, vous pouvez désormais appliquer le schéma de provisioning actuel à une machine ou à un ensemble de machines persistant ou non persistant existant. Actuellement, dans GCP, la mise à jour des propriétés prise en charge par cette fonctionnalité est le profil de machine.

Vous pouvez mettre à jour :

- une seule machine virtuelle ;
- une liste des machines virtuelles spécifiques ou toutes les machines virtuelles existantes associées à un ID de schéma de provisioning ;
- une liste des machines virtuelles spécifiques ou toutes les machines virtuelles existantes associées à un nom de schéma de provisioning.

Pour mettre à jour les machines virtuelles existantes :

1. Vérifiez la configuration des machines existantes. Par exemple,

```
Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Mettez à jour le schéma de provisioning. Par exemple,

```
`Set-ProvScheme –ProvisioningSchemeName "my-catalog" –
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofileinstance.vm"
<!--NeedCopy-->
```

3. Vérifiez si la propriété actuelle de la machine virtuelle correspond au schéma de provisioning actuel et s'il existe une action de mise à jour en attente sur la machine virtuelle. Par exemple,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

   Vous pouvez également rechercher les machines avec une version particulière. Par exemple,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Mettez à jour les machines existantes.

   - Pour mettre à jour toutes les machines existantes :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

   - Pour mettre à jour une liste de machines spécifiques :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
    -1
<!--NeedCopy-->
```

   - Pour mettre à jour les machines en fonction de la sortie de `Get-ProvVM` :

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
    ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

5. Recherchez les machines pour lesquelles une mise à jour est planifiée. Par exemple,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

6. Redémarrez les machines. Lors de la prochaine mise sous tension, les modifications de propriétés sont appliquées aux machines existantes. Vous pouvez vérifier l'état actualisé à l'aide de la commande suivante :

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
```

```
<!--NeedCopy-->
```

### Modifier les propriétés personnalisées liées au disque d'un catalogue existant

Vous pouvez modifier les propriétés personnalisées suivantes liées au disque d'un catalogue existant et des machines virtuelles existantes du catalogue :

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

> **Remarque :**
>
> - La propriété `StorageType` est liée au disque du système d'exploitation.
> - La propriété `PersistOsDisk` ne peut être définie que pour le catalogue non persistant avec le cache en écriture différée activé.

Cette mise en œuvre vous permet de sélectionner différents types de stockage pour différents disques, même après la création d'un catalogue, et ainsi d'équilibrer les prix associés aux différents types de stockage.

Pour procéder, utilisez les commandes PowerShell `Set-ProvScheme` et `Set-ProvVMUpdateTimeWindow` .

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*`.
3. Exécutez `Get-ProvVM -VMName <VM name>` pour obtenir les propriétés personnalisées.
4. Modifiez la chaîne de propriétés personnalisées :
   a) Copiez les propriétés personnalisées dans un bloc-notes et modifiez-les.
   b) Dans la fenêtre **PowerShell**, collez les propriétés personnalisées modifiées à partir du bloc-notes et attribuez-leur une variable. Par exemple :

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com
   /2014/xd/machinecreation xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="CatalogZones" Value
   ="" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="
   true" />
<Property xsi:type="StringProperty" Name="PersistOSDisk" Value
   ="true" />
```

```
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
    Value="pd-standard" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    pd-standard" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Mettez à jour le catalogue existant. Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
    CustomProperties $cp
<!--NeedCopy-->
```

6. Mettez à jour les machines virtuelles existantes. Par exemple :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Redémarrez les machines virtuelles. Lors de la prochaine mise sous tension, les modifications des propriétés personnalisées sont appliquées aux machines existantes.

### Protection contre la suppression accidentelle de machine

Citrix DaaS vous permet de protéger les ressources MCS sur Google Cloud pour empêcher toute suppression accidentelle. Configurez la machine virtuelle provisionnée en définissant l'indicateur `deletionProtection` sur TRUE.

Par défaut, les machines virtuelles provisionnées via le plug-in MCS ou Google Cloud sont créées avec InstanceProtection activé. La mise en œuvre est applicable aux catalogues persistants et non persistants. Les catalogues non persistants sont mis à jour lorsque les instances sont recréées à partir du modèle. Pour les machines persistantes existantes, vous pouvez définir l'indicateur dans la console Google Cloud. Pour plus d'informations sur la définition de l'indicateur, consultez le site de documentation Google. Les nouvelles machines ajoutées aux catalogues persistants sont créées avec `deletionProtection` activé.

Si vous tentez de supprimer une instance de machine virtuelle pour laquelle vous avez défini l'indicateur `deletionProtection`, la demande échoue. Toutefois, si l'autorisation `compute.instances.setDeletionProtection` vous est accordée ou si le rôle IAM **Administrateur de Compute** vous est attribué, vous pouvez réinitialiser l'indicateur pour autoriser la suppression de la ressource.

### Identifier les ressources créées par MCS

Voici les balises que MCS ajoute aux ressources. Les balises du tableau sont représentées au format “clé”:”valeur”.

| Nom de la ressource | Balise |
| --- | --- |
| Disque d’identification | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Image | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Disque OS | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Machine virtuelle de préparation | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Instantané publié | “CitrixResource”: “internal” |
| Bucket de stockage | “Citrixresource”: “internal” |
| Modèle | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| machine virtuelle dans le catalogue | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”. Le plugin ajoute également cette étiquette pour les machines virtuelles provisionnées par MCS : “citrix-provisioning-scheme-id”: “provSchemeId”. Vous pouvez utiliser cette étiquette pour filtrer par catalogue dans la console GCP. |
| Disque WBC | “CitrixResource”: “internal”<br>CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |

> **Remarque :**
>
> Une machine virtuelle n'est pas visible dans l'inventaire Citrix si une balise **CitrixResource** est ajoutée pour l'identifier en tant que ressource créée par MCS. Vous pouvez supprimer ou renommer la balise pour la rendre visible.

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à des environnements Google Cloud
- Créer des catalogues de machines
- Créer un catalogue Google Cloud Platform
- Gérer des catalogues de machines

## Gérer un catalogue HPE Moonshot

June 27, 2024

Gérer les catalogues de machines décrit les assistants qui permettent de gérer un catalogue de machines. Les informations suivantes concernent les détails spécifiques à HPE Moonshot.

> **Remarque :**
>
> Avant de gérer un catalogue HPE Moonshot, vous devez terminer la création d'un catalogue HPE Moonshot.

### Gestion de l'alimentation

Citrix Virtual Apps and Desktops vous permet de gérer l'alimentation des machines HPE Moonshot. Utilisez le nœud **Rechercher** dans le volet de navigation pour localiser la machine dont vous souhaitez gérer l'alimentation. Les actions de gestion de l'alimentation suivantes sont disponibles :

- Démarrer
- Arrêter
- Forcer l'arrêt
- Redémarrer
- Reset

> **Remarque :**
>
> Les actions d'alimentation **Suspendre** et **Reprendre** ne sont pas prises en charge.

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à HPE Moonshot
- Créer des catalogues de machines
- Créer un catalogue de machines HPE Moonshot
- Gérer des catalogues de machines

## Gérer un catalogue Microsoft Azure

June 27, 2024

> **Remarque :**
>
> Depuis juillet 2023, Microsoft a renommé Azure Active Directory (Azure AD) Microsoft Entra ID. Dans ce document, toute occurrence de l'appellation Azure Active Directory, Azure AD ou de l'acronyme AAD fait désormais référence à Microsoft Entra ID.

Gérer les catalogues de machines décrit les assistants qui permettent de gérer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements de cloud Microsoft Azure Resource Manager.

> **Remarque :**
>
> Avant de gérer un catalogue Microsoft Azure, vous devez terminer de créer un catalogue Microsoft Azure. Voir Créer un catalogue Microsoft Azure.

### Changer le type de stockage vers un niveau inférieur lorsqu'une machine virtuelle est arrêtée

Vous pouvez réduire les coûts de stockage en changeant le type de stockage d'un disque géré vers un niveau inférieur lorsque vous arrêtez une machine virtuelle. Pour ce faire, utilisez la propriété personnalisée `StorageTypeAtShutdown`.

Le type de stockage du disque passe à un niveau inférieur (comme spécifié dans la propriété personnalisée `StorageTypeAtShutdown`) lorsque vous arrêtez la machine virtuelle. Une fois la machine

virtuelle sous tension, l'état d'origine du type de stockage est rétabli (comme spécifié dans la propriété personnalisée `StorageType` ou la propriété personnalisée `WBCDiskStorageType`).

> **Important :**
>
> Le disque n'existe pas tant que la machine virtuelle n'a pas été pas mise sous tension au moins une fois. Par conséquent, vous ne pouvez pas modifier le type de stockage lors de la première mise sous tension de la machine virtuelle.

#### Exigences

- Applicable à un disque géré. Cela implique que vous définissiez la propriété personnalisée `UseManagedDisks` sur true.
- Applicable à un catalogue persistant et non persistant avec un disque de système d'exploitation persistant. Cela implique que vous définissiez la propriété personnalisée `persistOsDisk` sur true.
- Applicable à un catalogue non persistant avec un disque WBC persistant. Cela implique que vous définissiez la propriété personnalisée `persistWBC` sur true.

#### Restriction

- Microsoft ne vous permet de modifier le type de disque que deux fois par jour. Consultez le document Microsoft. Avec Citrix, la mise à jour de `StorageType` est effectuée chaque fois qu'une action de démarrage ou de désallocation est effectuée pour la machine virtuelle. Par conséquent, limitez le nombre d'actions d'alimentation par machine virtuelle à deux fois par jour. Par exemple, une action d'alimentation le matin pour démarrer la machine virtuelle et une autre le soir pour la désallouer.

#### Modifier le type de stockage vers un niveau inférieur

Avant de suivre les étapes, consultez les exigences et restrictions.

1. Ajoutez la propriété personnalisée `StorageTypeAtShutdown`, définissez la valeur sur Standard_LRS (HDD) et créez un catalogue à l'aide de `New-ProvScheme`. Pour plus d'informations sur la création d'un catalogue à l'aide de PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

   > **Remarque :**
   >
   > Si la valeur de `StorageTypeAtShutdown` est autre que vide ou Standard_LRS (HDD), l'opération échoue.

Exemple de définition de propriétés personnalisées lors de la création d'un catalogue persistant :

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

Exemple de définition de propriétés personnalisées lors de la création d'un catalogue non persistant :

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

> **Remarque :**
>
> Lorsque vous utilisez un profil de machine, la propriété personnalisée prévaut sur la propriété définie dans `MachineProfile`.

2. Arrêtez la machine virtuelle et vérifiez le type de stockage de la machine virtuelle sur le portail Azure. Le type de stockage du disque passe à un niveau inférieur, comme spécifié dans la propriété personnalisée `StorageTypeAtShutdown`.
3. Allumez la machine virtuelle. Le type de stockage du disque revient au type de stockage mentionné dans :
   - `StorageType` propriété personnalisée pour le disque du système d'exploitation
   - `WBCDiskStorageType` propriété personnalisée pour le disque WBC uniquement si vous la spécifiez dans `CustomProperties`. Dans le cas contraire, il revient au type de stockage mentionné dans `StorageType`.

### Appliquer `StorageTypeAtShutdown` à un catalogue existant

Avant de suivre les étapes, consultez les exigences et restrictions.

Utilisez `Set-ProvScheme` pour ajouter une machine virtuelle à un catalogue existant. La fonctionnalité s'applique aux nouvelles machines virtuelles ajoutées après l'exécution de `Set-ProvScheme`. Les machines existantes ne sont pas affectées.

Exemple de définition de propriétés personnalisées lors de l'ajout d'une machine virtuelle à un catalogue existant :

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com
   /2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="
   Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value
   ="Standard_LRS" />
</CustomProperties>'

```

```
15 $ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName
16
17 Set-ProvScheme -ProvisioningSchemeName $ProvScheme.
       ProvisioningSchemeName -CustomProperties $customProperties
18 <!--NeedCopy-->
```

### Définir le type de stockage des machines virtuelles existantes sur un niveau inférieur lors de l'arrêt

Avant de suivre les étapes, consultez les exigences et restrictions.

Vous pouvez réduire les coûts de stockage en définissant le type de stockage des machines virtuelles existantes sur un niveau inférieur lorsque les machines virtuelles sont arrêtées. Pour ce faire, utilisez la propriété personnalisée `StorageTypeAtShutdown`.

Pour définir le type de stockage des machines existantes dans un catalogue sur un niveau inférieur lorsque les machines virtuelles sont arrêtées, procédez comme suit :

1. Ouvrez une fenêtre PowerShell.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Exécutez `Get-Provscheme -ProvisioningSchemeName $CatalogName`.
4. Modifiez la chaîne de propriétés personnalisées.

```
1 $customProperties = '<CustomProperties xmlns="http://schemas.
      citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
      org/2001/XMLSchema-instance">
2 <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
      Value="Standard_LRS" />
3 </CustomProperties>'
4 <!--NeedCopy-->
```

5. Mettez à jour le schéma de provisioning du catalogue existant. La mise à jour s'applique aux nouvelles machines virtuelles ajoutées après l'exécution de `Set-ProvScheme`.

```
1 Set-ProvScheme -ProvisioningSchemeName $CatalogName -
      CustomProperties $customProperties
2 <!--NeedCopy-->
```

6. Mettez à jour les machines virtuelles existantes pour activer `StorageTypeAtShutdown`.

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName -
      StartsNow -DurationInMinutes -1
2 <!--NeedCopy-->
```

7. La prochaine fois que vous allumez les machines, la propriété `StorageTypeAtShutdown` des machines est mise à jour. Le type de stockage change lors du prochain arrêt.

8. Exécutez la commande suivante pour afficher la valeur `StorageTypeAtShutdown` de chaque machine virtuelle d'un catalogue :

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {
  $vmName = $_.VMName; $storageTypeAtShutdown = ($_.CustomVmData |
       ConvertFrom-Json).StorageTypeAtShutdown.
      DiskStorageAccountType; return New-Object psobject -Property
      @{
  "VMName" = $vmName; "StorageTypeAtShutdown" =
      $storageTypeAtShutdown  }
   }

<!--NeedCopy-->
```

### Mettre à jour les machines provisionnées vers l'état du schéma de provisioning actuel

La commande `Set-ProvScheme` modifie le schéma de provisioning. Toutefois, ce script n'affecte pas les machines existantes. À l'aide de la commande PowerShell `Set-ProvVMUpdateTimeWindow`, vous pouvez appliquer le schéma de provisioning actuel à une machine ou à un ensemble de machines persistant ou non persistant existant. Vous pouvez également planifier un créneau horaire pour les mises à jour de la configuration des machines provisionnées par MCS existantes. Toute mise sous tension ou redémarrage pendant le créneau horaire prévu applique une mise à jour planifiée du schéma de provisioning à une machine. Actuellement, dans Azure, vous pouvez mettre à jour `ServiceOffering`, `MachineProfile` et les propriétés personnalisées suivantes :

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

> **Remarque :**
>
> - Vous pouvez uniquement mettre à jour les propriétés personnalisées `StorageType`, `WBCDiskStorageType` et `IdentityDiskStorageType` d'un catalogue à l'aide d'un disque géré dans les environnements Azure.
> - Si vous exécutez `Set-ProvVMUpdateTimeWindow` deux fois, la commande la plus récente prend effet.

Vous pouvez mettre à jour :

- une seule machine virtuelle ;
- une liste des machines virtuelles spécifiques ou toutes les machines virtuelles existantes associées à un ID de schéma de provisioning ;
- une liste des machines virtuelles spécifiques ou toutes les machines virtuelles existantes associées à un nom de schéma de provisioning (nom du catalogue de machines).

Après avoir apporté les modifications suivantes au schéma de provisioning, l'instance de machine virtuelle est recréée pour les catalogues persistants dans Azure :

- Remplacez la valeur `MachineProfile`
- Supprimer `LicenseType`
- Supprimer `DedicatedHostGroupId`

> **Remarque :**
>
> Le disque d'OS des machines existantes ainsi que toutes ses données restent tels quels et une nouvelle machine virtuelle est connectée au disque.

Avant de mettre à jour les machines virtuelles existantes :

1. Vérifiez la configuration des machines existantes. Par exemple,

```
Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Mettez à jour le schéma de provisioning. Par exemple,

   - Avec la machine virtuelle comme entrée de profil de machine :

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
   MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofile.folder<resource-group>.resourcegroup<
   virtual-machine>.vm"
<!--NeedCopy-->
```

   - Avec la spécification de modèle comme entrée du profil de la machine :

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"
-MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofile.folder<resource-group>.resourcegroup<
   template-spec>.templatespec<template-spec-version>.
   templatespecversion"
-ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
   serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```

   - Avec juste une offre de service :

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
<!--NeedCopy-->
```

3. Vérifiez si la propriété actuelle de la machine virtuelle correspond au schéma de provisioning actuel et s'il existe une action de mise à jour en attente sur la machine virtuelle. Par exemple,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

Vous pouvez également rechercher les machines avec une version particulière. Par exemple,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

Pour demander des mises à jour pour les machines existantes à appliquer au prochain redémarrage :

1. Exécutez les commandes suivantes pour mettre à jour les machines existantes et faire en sorte que les mises à jour s'appliquent au prochain redémarrage.

   - Pour mettre à jour toutes les machines existantes. Par exemple,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

   - Pour mettre à jour une liste de machines spécifiques. Par exemple,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
    -1
<!--NeedCopy-->
```

   - Pour mettre à jour les machines en fonction de la sortie de Get-Provmachine virtuelle. Par exemple,

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
    ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

> **Remarque :**
>
> - `StartsNow` indique que l'heure de démarrage planifiée est l'heure actuelle.
> - `DurationInMinutes` avec un nombre négatif (par exemple, —1) indique qu'il n'y

> a pas de limite supérieure dans le créneau planifié.

2. Recherchez les machines pour lesquelles une mise à jour est planifiée. Par exemple,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

3. Redémarrez les machines. Lors de la prochaine mise sous tension, les modifications de propriétés sont appliquées aux machines existantes. Vous pouvez vérifier l'état actualisé à l'aide de la commande suivante. Par exemple,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

Pour planifier la mise à jour d'une machine virtuelle avec les derniers paramètres de provisioning lors de son prochain démarrage dans le créneau planifié :

1. Exécutez les commandes suivantes :

   - Pour planifier une mise à jour avec l'heure actuelle comme heure de début

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName vm1 -StartsNow -DurationInMinutes 120
<!--NeedCopy-->
```

   - Pour planifier une mise à jour un week-end

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
    catalog" -VMName "vm1" -StartTimeInUTC "10/15/2022
    9:00am" -DurationInMinutes (New-TimeSpan -Days 2).
    TotalMinutes
<!--NeedCopy-->
```

> **Remarque :**
>
> - `VMName` est facultatif. Sans spécification, la mise à jour est planifiée pour l'ensemble du catalogue.
> - Au lieu de `StartTimeInUTC`, utilisez `StartsNow` pour indiquer que l'heure de démarrage est l'heure actuelle.
> - `DurationInMinutes` est facultatif. La valeur par défaut est de 120 minutes. Un nombre négatif (par exemple, —1) indique qu'il n'y a pas de limite supérieure dans le créneau planifié.

2. Vérifiez l'état de la mise à jour.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

```
<!--NeedCopy-->
```

3. Allumez la machine virtuelle. Si vous allumez la machine après le créneau horaire prévu, la mise à jour de la configuration n'est pas appliquée. Si vous allumez la machine dans le créneau horaire prévu,

   - Si la machine est éteinte, et
     - vous n'allumez pas la machine, la mise à jour de la configuration n'est pas appliquée
     - vous allumez la machine, la mise à jour de la configuration est appliquée
   - Si la machine est allumée, et
     - vous ne redémarrez pas la machine, la mise à jour de la configuration n'est pas appliquée
     - vous redémarrez la machine, la mise à jour de la configuration est appliquée

Pour annuler la mise à jour de la configuration :

Vous pouvez également annuler une mise à jour de la configuration d'une seule machine virtuelle, de plusieurs machines virtuelles ou d'un catalogue entier. Pour annuler une mise à jour de la configuration :

1. Exécutez `Clear-ProvVMUpdateTimeWindow`. Par exemple :

   - Pour annuler la mise à jour de la configuration prévue pour une seule machine virtuelle :

     ```
     Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName " my-catalog " -VMName " vm1 "
     <!--NeedCopy-->
     ```

   - Pour annuler la mise à jour de la configuration prévue pour plusieurs machines virtuelles :

     ```
     Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog" -VMName "vm1","vm2"
     <!--NeedCopy-->
     ```

     > **Remarque :**
     >
     > Les machines virtuelles doivent provenir du même catalogue.

### Mettre à jour les propriétés des machines virtuelles individuelles

Vous pouvez mettre à jour les propriétés de machines virtuelles individuelles dans un catalogue de machines MCS persistant à l'aide de la commande PowerShell `Set-ProvVM`. Toutefois, les mises à jour ne sont pas appliquées immédiatement. Vous devez définir la fenêtre horaire à l'aide de la commande PowerShell `Set-ProvVMUpdateTimeWindow` pour que les mises à jour s'appliquent.

Cette implémentation vous permet de gérer efficacement les machines virtuelles individuelles sans mettre à jour l'intégralité du catalogue de machines. Actuellement, cette fonctionnalité s'applique uniquement à l'environnement Azure.

Actuellement, les propriétés que vous pouvez mettre à jour sont les suivantes :

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

Grâce à cette fonctionnalité, vous pouvez :

- Mettre à jour les propriétés d'une machine virtuelle
- Conserver les propriétés mises à jour sur une machine virtuelle après la mise à jour du catalogue de machines
- Annuler les mises à jour de configuration appliquées à une machine virtuelle

Avant de mettre à jour les propriétés d'une machine virtuelle :

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Vérifiez la configuration du catalogue de machines existant. Par exemple :

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

4. Vérifiez la configuration de la machine virtuelle sur laquelle vous souhaitez appliquer les mises à jour. Par exemple :

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

### Mettre à jour les propriétés d'une machine virtuelle

Procédez comme suit pour mettre à jour les propriétés d'une machine virtuelle :

1. Éteignez la machine virtuelle sur laquelle vous souhaitez appliquer les mises à jour.
2. Mettez à jour les propriétés de la machine virtuelle. Par exemple, si vous souhaitez mettre à jour la propriété personnalisée du type de stockage (`StorageType`) de la machine virtuelle, exécutez ce qui suit :

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

Vous pouvez mettre à jour simultanément les propriétés de deux machines virtuelles d'un catalogue de machines. Par exemple :

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
    CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
<!--NeedCopy-->
```

> **Remarque :**
>
> Les mises à jour ne sont pas appliquées immédiatement.

3. Obtenez la liste des propriétés spécifiées pour la mise à jour ainsi que la version de configuration. Par exemple :

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    VMName machine1
<!--NeedCopy-->
```

Vérifiez la valeur de propriété `Version` et les propriétés à mettre à jour (dans ce cas, `StorageType`).

4. Vérifiez la version de configuration. Par exemple :

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Vérifiez la valeur de propriété de `ProvVMConfigurationVersion`. La mise à jour n'est pas encore appliquée. La machine virtuelle est toujours dans l'ancienne configuration.

5. Demandez une mise à jour planifiée. Par exemple :

```
 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    StartsNow -DurationInMinutes -1
 <!--NeedCopy-->
```

Pour plus d'informations, consultez Mettre à jour les machines provisionnées vers l'état du schéma de provisioning actuel.

> **Remarque :**
>
> Toute mise à jour du schéma de provisioning en attente est également appliquée.

6. Redémarrez la machine virtuelle. Par exemple :

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

7. Vérifiez la version de configuration. Par exemple :

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Vérifiez la valeur de propriété de `ProvVMConfigurationVersion`. La mise à jour est maintenant appliquée. La machine virtuelle présente désormais la nouvelle configuration.

8. Pour appliquer d'autres mises à jour de configuration sur la machine virtuelle, éteignez-la et répétez les étapes.

### Conserver les propriétés mises à jour sur une machine virtuelle après la mise à jour du catalogue de machines

Procédez comme suit pour conserver les propriétés mises à jour sur une machine virtuelle :

1. Éteignez la machine virtuelle sur laquelle vous souhaitez appliquer les mises à jour.
2. Mettez le catalogue de machines à jour. Par exemple, si vous souhaitez modifier la taille de la machine virtuelle (`ServiceOffering`) et le type de stockage (`StorageType`), exécutez ce qui suit :

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -
    ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
    Name='StorageType' Value='StandardSSD_LRS' />..."
<!--NeedCopy-->
```

3. Obtenez les détails de configuration du catalogue de machines. Par exemple :

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

La `ProvisioningSchemeVersion` est maintenant incrémentée d'une unité. La taille de la machine virtuelle et le type de stockage sont également mis à jour.

4. Mettez à jour les propriétés de la machine virtuelle. Par exemple, appliquez un profil de machine à la machine virtuelle.

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<template-
    spec>.templatespec<template-spec-version>.templatespecversion"
<!--NeedCopy-->
```

> **Remarque :**
>
> L'entrée du profil de machine comporte une balise et une taille de machine virtuelle différente (`ServiceOffering`) spécifiée.

5. Obtenez la liste des propriétés que la machine virtuelle aura après avoir fusionné les mises à jour de configuration sur la machine virtuelle avec les mises à jour du catalogue de machines. Par exemple :

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
    AzureCatalog -VMName machine1
<!--NeedCopy-->
```

> **Remarque :**
>
> Toute mise à jour sur la machine virtuelle remplacera les mises à jour effectuées sur le catalogue de machines.

6. Demandez une mise à jour planifiée pour la machine virtuelle. Par exemple :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Redémarrez la machine virtuelle. Par exemple :

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

   La machine virtuelle conserve sa taille de machine virtuelle mise à jour telle que dérivée du profil de la machine. Les valeurs de balise spécifiées dans le profil de la machine sont également appliquées à la machine virtuelle. Toutefois, le type de stockage est dérivé du dernier schéma de provisioning.

8. Obtenez la version de configuration de la machine virtuelle. Par exemple :

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   La `ProvisioningSchemeVersion` et la `ProvVMConfigurationVersion` affichent désormais la dernière version.

#### Annuler les mises à jour de configuration appliquées à une machine virtuelle

1. Après avoir appliqué les mises à jour à une machine virtuelle, éteignez-la.
2. Exécutez la commande suivante pour supprimer les mises à jour appliquées à la machine virtuelle. Par exemple :

```
Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

3. Demandez une mise à jour planifiée pour la machine virtuelle. Par exemple :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. Redémarrez la machine virtuelle. Par exemple :

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

5. Vérifiez la version de configuration de la machine virtuelle. Par exemple :

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

   La valeur `ProvVMConfigurationVersion` est désormais la version de configuration du catalogue de machines.

### Récupérer des informations sur les machines virtuelles Azure, les instantanés, le disque du système d'exploitation et la définition d'image de la galerie

Vous pouvez afficher des informations sur une machine virtuelle Azure, notamment le disque et le type de système d'exploitation, l'instantané et la définition de l'image de la galerie. Ces informations sont affichées pour les ressources de l'image principale lorsqu'un catalogue de machines est affecté. Utilisez cette fonctionnalité pour afficher et sélectionner une image Linux ou Windows. Une propriété PowerShell, `TemplateIsWindowsTemplate`, a été ajoutée au paramètre `AdditionDatafield`. Ce champ contient des informations spécifiques à Azure : type de machine virtuelle, disque du système d'exploitation, informations sur l'image de la galerie et informations sur le type de système d'exploitation. Si `TemplateIsWindowsTemplate` est défini sur **True**, cela indique que le type de système d'exploitation est Windows ; si `TemplateIsWindowsTemplate` est défini sur **False**, cela indique que le type de système d'exploitation est Linux.

> **Conseil :**
>
> Les informations affichées par la propriété PowerShell `TemplateIsWindowsTemplate` sont dérivées de l'API Azure. Ce champ peut parfois être vide. Par exemple, un instantané d'un disque de données ne contient pas le champ `TemplateIsWindowsTemplate`, car le type de système d'exploitation ne peut pas être récupéré à partir d'un instantané.

Par exemple, définissez le paramètre Azure machine virtuelle `AdditionData` sur **True** pour le type

de système d'exploitation Windows à l'aide de PowerShell :

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.
    folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).
    AdditionalData
Key Value
ServiceOfferingDescription Standard_B2ms
HardDiskSizeGB 127
ResourceGroupName FENGHUAJ-DEV-TESTING-RG
ServiceOfferingMemory 8192
ServiceOfferingCores 2
TemplateIsWindowsTemplate True
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SupportedMachineGenerations Gen1,Gen2
<!--NeedCopy-->
```

### Identifier les ressources créées par MCS

Voici les balises que MCS ajoute aux ressources. Les balises du tableau sont représentées au format "clé":"valeur".

| Nom de la ressource | Balise |
| --- | --- |
| Disque d'identification | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Image | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Carte d'interface réseau | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Disque OS | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Machine virtuelle de préparation | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Instantané publié | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal" |
| Groupe de ressources | "CitrixResource": "Internal" |

| Nom de la ressource | Balise |
| --- | --- |
| Compte de stockage | CitrixSchemaVersion: 2.0<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“CitrixResource”: “Internal” |
| machine virtuelle dans le catalogue | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“CitrixResource”: “Internal” |
| Disque WBC | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“CitrixResource”: “Internal” |

> **Remarque :**
>
> Une machine virtuelle n’est pas visible dans l’inventaire Citrix si une balise **CitrixResource** est ajoutée pour l’identifier en tant que ressource créée par MCS. Vous pouvez supprimer ou renommer la balise pour la rendre visible.

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à Microsoft Azure
- Créer des catalogues de machines
- Créer un catalogue Microsoft Azure
- Gérer des catalogues de machines

## Gérer un catalogue Microsoft System Center Virtual Machine Manager

June 27, 2024

Gérer les catalogues de machines décrit les assistants qui permettent de gérer un catalogue de machines. Les informations suivantes fournissent des informations spécifiques aux environnements de virtualisation Microsoft System Center Virtual Machine Manager (machine virtuelleM).

> **Remarque :**
>
> Avant de gérer un catalogue VMM, vous devez terminer la création d'un catalogue VMM. Voir Créer un catalogue Microsoft System Center Virtual Machine Manager.

### Identifier les ressources créées par MCS

Voici les balises que MCS ajoute aux ressources. Les balises du tableau sont représentées au format "clé":"valeur".

| Nom de la ressource | Balise |
|---|---|
| machine virtuelle de préparation | Chaîne de balise : "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>Entrée de propriété personnalisée : "XdConfig:" XdProvisioned=True" |
| machine virtuelle dans le catalogue | Chaîne de balise : "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>Entrée de propriété personnalisée : "XdConfig:" XdProvisioned=True" |

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à Microsoft System Center Virtual Machine Manager
- Créer des catalogues de machines
- Créer un catalogue Microsoft System Center Virtual Machine Manager
- Gérer des catalogues de machines

## Gérer un catalogue VMware

June 27, 2024

Gérer les catalogues de machines décrit les assistants qui permettent de gérer un catalogue de machines. Les informations suivantes couvrent les détails spécifiques aux environnements de virtualisation VMware.

> **Remarque :**
>
> Avant de gérer un catalogue VMware, vous devez terminer la création d'un catalogue VMware. Voir Créer un catalogue VMware.

### Mettre à jour l'ID de dossier d'un catalogue de machines

Vous pouvez mettre à jour l'ID de dossier d'un catalogue de machines MCS en spécifiant `FolderId` dans les propriétés personnalisées de la commande `Set-ProvScheme`. Les machines virtuelles créées après la mise à jour de l'ID de dossier sont créées sous ce nouvel ID de dossier. Si cette propriété n'est pas spécifiée dans `CustomProperties`, les machines virtuelles sont créées dans le dossier où se trouve l'image principale.

Effectuez les étapes suivantes pour mettre à jour l'ID de dossier d'un catalogue de machines.

1. Ouvrez un navigateur Web et entrez l'URL de **vSphere Web Client**.
2. Entrez les informations d'identification et cliquez sur **Login**.
3. Créez un dossier d'emplacement de machine virtuelle dans **vSphere Web Client**.
4. Ouvrez une fenêtre PowerShell.
5. Exécutez **asnp citrix*** pour charger des modules PowerShell spécifiques à Citrix.
6. Spécifiez `FolderID` dans les `CustomProperties` de `Set-ProvScheme`. Dans cet exemple, la valeur de l'ID de dossier est `group-v2406`.

```
1 Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
    f630687372" -CustomProperties "<CustomProperties xmlns=""http
    ://schemas.citrix.com/2014/xd/machinecreation"" xmlns:xsi=""
    http://www.w3.org/2001/XMLSchema-instance""><Property xsi:type=
    ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
    CustomProperties>"
2 <!--NeedCopy-->
```

7. Ajoutez une machine virtuelle au catalogue de machines à l'aide de Studio.
8. Vérifiez la nouvelle machine virtuelle sur vSphere Web Client. La nouvelle machine virtuelle est créée dans le nouveau dossier.

#### Trouver l'ID de dossier dans vSphere

Accédez à Managed Object Browser (MOB) sur n'importe quel système ESXi ou vCenter Server pour trouver l'ID de dossier des machines virtuelles.

Le MOB est une application serveur Web disponible dans tous les systèmes ESX/ESXi et vCenter Server. Cet utilitaire vSphere vous permet d'afficher des informations détaillées sur des objets tels que les machines virtuelles, les magasins de données et les pools de ressources.

1. Ouvrez un navigateur Web et entrez `http://x.x.x.x/mob`, où x.x.x.x est l'adresse IP de l'hôte vCenter Server ou ESX/ESXi. Par exemple, https://10.60.4.70/mob.
2. Sur la **page d'accueil** de MOB, cliquez sur la valeur **content** du contenu de la propriété.
3. Cliquez sur la valeur de **rootFolder**.
4. Cliquez sur la valeur de **childEntity**.
5. Cliquez sur la valeur de **vmFolder**.
6. Vous pouvez trouver l'ID de dossier dans la valeur de **childEntity**.

### Migration du stockage de machines virtuelles

Vous pouvez déplacer le stockage sur disque des machines virtuelles existantes d'un ancien stockage vers un nouveau stockage. Pendant la migration, MCS conserve les fonctionnalités de la machine virtuelle, telles que la gestion de l'alimentation, la réinitialisation du disque du système d'exploitation, etc. Vous pouvez également ajouter de nouvelles machines virtuelles au catalogue de machines à l'aide du nouveau stockage sur disque. Pour cela, utilisez la commande PowerShell `Move-ProvVMDisk`.

Actuellement, vous ne pouvez migrer que des machines virtuelles persistantes à clone complet.

Le nouveau stockage doit satisfaire aux conditions suivantes :

- Il doit se trouver dans le même cluster que l'ancien stockage.
- L'hôte sur lequel s'exécute la machine virtuelle doit avoir accès à l'ancienne et à la nouvelle banque de données.

Vous pouvez effectuer les tâches suivantes :

- Migrer le stockage sur disque
- Marquer l'ancien stockage comme obsolète

#### Migrer le stockage sur disque

Pour migrer le stockage sur disque :

1. Ajoutez un nouvel espace de stockage à une unité d'hébergement existante. Modifiez l'ancien stockage en le définissant sur **Remplacé**. Vous pouvez le faire à l'aide de Web Studio ou des commandes PowerShell.
    - Si vous utilisez Web Studio, consultez la section Modifier le stockage.

- Si vous utilisez les commandes PowerShell :
  - Exécutez `Add-Hyphostingunitstorage` pour ajouter le nouveau stockage à l'unité d'hébergement existante.
  - Exécutez `Set-Hyphostingunitstorage` avec **Superseded** défini sur Vrai pour désactiver la création de nouvelles machines virtuelles dans l'ancien stockage.

2. Éteignez les machines virtuelles et activez le **mode maintenance**.
3. Déplacez le stockage sur disque des machines virtuelles vers le nouveau stockage et mettez à jour les informations de stockage. Par exemple :

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -
    VMName ("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,
    Identity -DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

4. Obtenez l'ID de tâche de la migration. Par exemple :

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk -
    ProvisioningSchemeName xxxxx -DiskType OS,Identity -
    DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

5. Vérifiez l'état de la migration.

   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines` : fournit la liste des machines virtuelles dont la migration de disque a réussi, y compris les machines virtuelles déjà migrées vers le nouveau stockage.
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines` : fournit la liste des machines virtuelles dont la migration a échoué.
   - `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines` : fournit la liste des machines virtuelles dont la migration n'a pas encore commencé.
   - `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01` : fournit les propriétés de machine virtuelle mises à jour après la migration. Vérifiez les propriétés telles que `StorageId`, `AssignedImage`, `BootedImage`, `IdentityDiskId`, `IdentityDiskStorage` et `LastBootTime`.

Après avoir migré les disques des machines virtuelles créées par MCS avec instantané, l'avertissement **Consolidation requise dans le client VSphere** peut s'afficher. Pour consolider et éviter les pertes de données :

1. Effectuez une sauvegarde de la machine virtuelle VMware. Par exemple, transférez tous les fichiers de machine virtuelle dans un autre dossier d'une banque de données.
2. Lorsque l'avertissement s'affiche, cliquez sur **Consolider**, puis sur **OK** pour confirmer la consolidation.

#### Marquer l'ancien stockage comme obsolète

Pour rendre obsolète l'ancien stockage après la migration du disque des machines virtuelles :

1. Obtenez des informations sur les disques de base et le nombre de machines dans chaque espace de stockage sur disque de l'unité d'hébergement. Par exemple :

   ```
   $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
       xxxxx
   $result
   $result.ProvResourceInStorage | Format-List -Property *
   <!--NeedCopy-->
   ```

   Une fois la migration réussie, MCS supprime automatiquement le disque de base obsolète et aucune machine ne se trouve dans l'ancien stockage. Après avoir exécuté la commande, assurez-vous donc qu'il n'y a pas de machines ni de disque de base dans l'ancien stockage.

2. Exécutez `Remove-Hyphostingunitstorage` pour supprimer complètement l'ancien stockage de l'unité d'hébergement. Vous pouvez également utiliser Web Studio pour supprimer l'ancien espace de stockage.

### Identifier les ressources créées par MCS

Voici les balises que MCS ajoute aux ressources. Les balises du tableau sont représentées au format "clé":"valeur".

| Nom de la ressource | Balise |
|---|---|
| machine virtuelle de préparation | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True" |
| machine virtuelle dans le catalogue | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True" |

### Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à VMware
- Créer des catalogues de machines
- Créer un catalogue VMware
- Gérer des catalogues de machines

## Gestion de l'alimentation

June 27, 2024

Avec Citrix Virtual Apps and Desktops, vous pouvez gérer l'alimentation de machines virtuelles provisionnées par MCS sur différents hyperviseurs et services cloud pris en charge. Bénéfices de l'opération de gestion de l'alimentation :

- Une expérience utilisateur optimale
- Gestion des coûts et économies d'énergie

Les actions d'alimentation disponibles sont les suivantes :

- Démarrer
- Arrêter
- Redémarrer
- Suspendre
- Reprendre
- Forcer le redémarrage
- Forcer l'arrêt

> **Remarque :**
>
> - Pour une machine virtuelle non persistante, le cycle d'alimentation (arrêt/démarrage et redémarrage) entraîne la réinitialisation du disque du système d'exploitation.
> - Les capacités et les comportements des actions d'alimentation varient en fonction des hyperviseurs ou des services cloud.

L'article décrit les principales fonctionnalités de gestion de l'alimentation associées à certains hyperviseurs pris en charge.

- Gérer l'alimentation des machines virtuelles AWS
- Gérer l'alimentation des machines virtuelles Azure

## Gérer l'alimentation des machines virtuelles AWS

June 27, 2024

Pour en savoir plus sur les autorisations requises, voir Autorisations Azure requises.

### Mise en veille prolongée d'instances

Le processus de mise en veille prolongée enregistre l'état en mémoire de l'instance, ainsi que ses adresses IP privées et élastiques, ce qui lui permet de reprendre exactement là où elle s'était arrêtée.

Lorsqu'une instance reçoit l'ordre de mise en veille prolongée, elle écrit l'état en mémoire dans un fichier du volume EBS racine, puis s'arrête d'elle-même. Un volume Amazon EBS est un périphérique de stockage durable au niveau bloc que vous pouvez associer à vos instances. Après avoir attaché un volume à une instance, vous pouvez l'utiliser comme vous le feriez pour un disque dur physique. Chiffrez le volume EBS racine de l'instance. Le chiffrement garantit une protection adéquate des données sensibles lorsqu'elles sont copiées de la mémoire vers le volume EBS. Pour plus d'informations sur le chiffrement EBS, consultez Chiffrement Amazon EBS.

Les limites de la mise en veille prolongée d'instances prises en charge sont les suivantes :

- La mémoire d'instance (RAM) n'est prise en charge que jusqu'à 150 Go
- Le mode de démarrage UEFI n'est pas pris en charge
- Le SSD à usage général et le SSD IOPS provisionné ne sont pris en charge qu'en tant que types de volumes EBS.

#### Créer des machines virtuelles compatibles avec la mise en veille prolongée

Pour créer des machines virtuelles compatibles avec la mise en veille prolongée :

1. Créez une connexion hôte. Voir Connexion à AWS.
2. Lancez une instance avec la racine EBS chiffrée et la propriété **Stop-Hibernate** activée. Pour plus d'informations sur le lancement de l'instance, le chiffrement du volume EBS racine et l'activation de la mise en veille prolongée, consultez https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/. Utilisez cette instance comme image principale pour créer une AMI.
3. Préparez l'image principale :
    a) Installez un VDA sur l'image principale. Citrix recommande d'installer la version la plus récente pour autoriser l'accès aux dernières fonctionnalités. Si vous ne parvenez pas à installer un VDA sur l'image principale, la création du catalogue échoue. Pour plus d'informations sur l'installation d'un VDA, consultez la section Installer des VDA.
    b) Joignez l'image principale au domaine dont les ordinateurs de bureau et les applications sont membres. Assurez-vous que l'image principale est disponible sur l'hôte sur lequel les machines sont créées.

4. Créez une AMI à partir de cette instance. Pour plus d'informations sur la création d'une AMI à partir d'une instance, consultez Créer une AMI à partir d'une instance Amazon EC2.
5. Créez un catalogue de machines à l'aide de la commande `New-ProvScheme`. Définissez la propriété personnalisée `AwsCaptureInstanceProperties` sur **True**. Pour plus d'informations sur l'activation des propriétés d'instance AWS dans l'interface Configuration complète, consultez Application des propriétés d'instance AWS et balisage des ressources opérationnelles dans l'interface Configuration complète.

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot
-CustomProperties "AwsCaptureInstanceProperties,true;"
-HostingUnitName "xxx" -IdentityPoolName $catalog_name -
   InitialBatchSizeHint 1
-MasterImageVM "xyz.template" -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\MyConn\us-east-2a.availabilityzone
    \10.0.0.0``/24 (vpc-0f1771e45671aedcd).network" }

-ProvisioningSchemeName $catalog_name
-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -
   ServiceOffering "xxx"
<!--NeedCopy-->
```

   Pour plus d'informations sur la création d'un catalogue de machines à l'aide de commandes PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/.

Des machines virtuelles pouvant être mises en veille prolongée sont créées si :

- Vous sélectionnez une AMI créée à partir d'une image principale sur laquelle la propriété **Stop-Hibernate** est activée.
- La machine virtuelle principale est jointe au domaine et le VDA est installé.
- Vous sélectionnez la taille de machine virtuelle appropriée (offre de services) capable de gérer la mise en veille prolongée.

La commande **New-ProvScheme** échoue avec un message d'erreur approprié si :

- La machine virtuelle principale est compatible avec la mise en veille prolongée, mais l'offre de services n'est pas capable de gérer la mise en veille prolongée.
- Si la machine virtuelle principale n'est pas jointe au domaine et qu'aucun VDA n'est installé.

#### État de mise en veille prolongée des offres de service et de l'AMI

Pour obtenir l'état de mise en veille prolongée des offres de service et des AMI (modèles), exécutez les commandes suivantes :

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

#### Mettre à jour l'offre de service d'un schéma de provisioning existant compatible avec la mise en veille prolongée

1. Exécutez la commande `Set-ProvScheme`. Par exemple,

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <
    String>
<!--NeedCopy-->
```

Le système affiche un message d'exception si l'offre de service n'est pas compatible.

#### Mettre à jour un catalogue de machines compatible avec la mise en veille prolongée

Si vous essayez de mettre à jour un catalogue de machines existant avec un catalogue de machines non compatible avec la mise en veille prolongée, la mise à jour échoue avec un message d'erreur approprié.

#### Gestion de l'alimentation des machines virtuelles en veille prolongée

Vous pouvez effectuer les opérations de gestion de l'alimentation suivantes sur les machines virtuelles en veille prolongée :

1. Suspendre la machine virtuelle de son état d'exécution.
2. Reprendre la machine virtuelle à partir de l'état suspendu.
3. Redémarrer la machine virtuelle à partir de l'état suspendu.

## Gérer l'alimentation des machines virtuelles Azure

June 27, 2024

Pour plus d'informations sur les autorisations requises, consultez Autorisations Azure requises.

### Provisioning à la demande d'Azure

Avec le provisioning à la demande d'Azure, les machine virtuelle sont créées uniquement lorsque Citrix Virtual Apps and Desktops initie une action d'alimentation, une fois que le provisioning est terminé.

Lorsque vous utilisez MCS pour créer des catalogues de machines dans Azure Resource Manager, la fonctionnalité de provisioning à la demande d'Azure :

- Réduit vos coûts de stockage
- Accélère la création de catalogues

Lorsque vous créez un catalogue MCS, le portail Azure affiche les groupes de sécurité réseau, les interfaces réseau, les images de base et les disques d'identité dans les groupes de ressources.

Le portail Azure n'affiche pas la machine virtuelle tant que Citrix Virtual Apps and Desktops n'a pas initié une action d'alimentation pour celle-ci. Il existe deux types de machines présentant les différences suivantes :

- Pour une machine regroupée, le disque du système d'exploitation et le cache en écriture différée existent uniquement lorsque la machine virtuelle existe. Lorsque vous arrêtez une machine groupée dans la console, la machine virtuelle n'est pas visible dans le portail Azure. Cela peut entraîner des économies de stockage importantes si vous arrêtez régulièrement les machines (par exemple, en dehors des heures de travail).
- Pour une machine dédiée, le disque du système d'exploitation est créé la première fois que la machine virtuelle est démarrée. La machine virtuelle du portail Azure reste dans le stockage jusqu'à ce que l'identité de la machine soit supprimée. Lorsque vous arrêtez une machine dédiée dans la console, la machine virtuelle reste visible dans le portail Azure.

> **Remarque :**
>
> La prise en charge des catalogues Azure créés avant la fonctionnalité de provisioning à la demande (catalogues « d'ancienne génération ») est obsolète. Par conséquent, recréez les machines virtuelles du catalogue Azure d'ancienne génération. Les catalogues sont ensuite provisionnés à la demande, ce qui permet de réduire les coûts de stockage.

### Conserver une machine virtuelle provisionnée lors des cycles d'alimentation

Indiquez si vous souhaitez conserver une machine virtuelle provisionnée lors des cycles d'alimentation. Utilisez le paramètre PowerShell `New-ProvScheme CustomProperties`. Ce paramètre prend en charge une propriété supplémentaire `PersistVm`, utilisée pour déterminer si une machine virtuelle provisionnée persiste en cas de cycle d'alimentation. Définissez la propriété `PersistVm` sur **Vrai** pour conserver une machine virtuelle lorsqu'elle est mise hors tension ou définissez la propriété sur **Faux** pour garantir que la machine virtuelle n'est pas conservée lorsqu'elle est mise hors tension.

> **Remarque :**
>
> La propriété `PersistVm` s'applique uniquement à un schéma de provisioning dont les pro-

> priétés `CleanOnBoot` et `UseWriteBackCache` sont activées. Si la propriété `PersistVm` n'est pas spécifiée pour les machines virtuelles non persistantes, elles sont supprimées de l'environnement Azure lorsqu'elles sont mises hors tension.

Dans l'exemple suivant, le paramètre `New-ProvScheme CustomProperties` définit la propriété `PersistVm` sur **true** :

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Standard_LRS" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-resourcegroup" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
</CustomProperties>
<!--NeedCopy-->
```

Dans l'exemple suivant, le paramètre `New-ProvScheme CustomProperties` préserve le cache en écriture différée en définissant `PersistVM` sur **true** :

```
New-ProvScheme
-AzureAdJoinType "None"
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"Standard_LRS`" /><Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"false`" /><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
-HostingUnitName "demo"
-IdentityPoolName "NonPersistent-MCSIO-PersistVM"
-MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.resourcegroup\demo-snapshot.snapshot"
-NetworkMapping @ {
"0"="XDHyp:\HostingUnits\demo\virtualprivatecloud.folder\East US.region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet.virtualprivatecloud\default.network" }

```

```
-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
 -ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
    Standard_B2ms.serviceoffering" -UseWriteBackCache
 -WriteBackCacheDiskSize 127
 -WriteBackCacheMemorySize 256
 <!--NeedCopy-->
```

> **Conseil :**
>
> La propriété `PersistVm` détermine si une machine virtuelle provisionnée doit être conservée. La propriété `PersistOsdisk` détermine si le disque du système d'exploitation doit être conservé. Pour conserver une machine virtuelle provisionnée, conservez d'abord le disque du système d'exploitation. Ne supprimez pas le disque du système d'exploitation sans supprimer au préalable la machine virtuelle. Vous pouvez utiliser la propriété `PersistOsdisk` sans spécifier le paramètre `PersistVm`.

### Personnaliser le comportement de mise sous tension en cas d'échec du changement de type de stockage

Lors de la mise sous tension, le type de stockage d'un disque géré peut ne pas passer au type souhaité en raison d'une panne sur Azure. Dans ces scénarios, la machine virtuelle reste éteinte et un message d'échec vous est envoyé. Vous pouvez toutefois choisir de mettre la machine virtuelle sous tension même si le stockage ne peut pas être restauré à son type configuré ou de la laisser hors tension.

- Si vous configurez la propriété personnalisée `FailSafeStorageType` sur **true** (paramètre par défaut) ou si vous ne la spécifiez pas dans les commandes `New-ProvScheme` ou `Set-ProvScheme` :
  - Lors de la mise sous tension, la machine virtuelle s'allume avec un type de stockage incorrect.
  - À l'arrêt, la machine virtuelle reste éteinte avec un type de stockage incorrect.
- Si vous configurez la propriété personnalisée `FailSafeStorageType` sur **false** dans les commandes `New-ProvScheme` ou `Set-ProvScheme` :
  - Si elle est sous tension, la machine virtuelle reste éteinte avec un type de stockage incorrect.
  - À l'arrêt, la machine virtuelle reste éteinte avec un type de stockage incorrect.

Pour créer un catalogue de machines :

1. Ouvrez une fenêtre PowerShell.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Créez un pool d'identités s'il n'a pas déjà été créé.

4. Ajoutez la propriété personnalisée dans `New-ProvScheme`. Par exemple :

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
    \abc.resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
     resourcegroup\abc-vnet.virtualprivatecloud\default.network" }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
    serviceoffering.folder\Standard_DS2_v2.serviceoffering"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix
    .com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`
    "Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown
    `" Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
     Value=`"true`" />
</CustomProperties>"
<!--NeedCopy-->
```

5. Créez le catalogue de machines. Pour plus d'informations sur la création d'un catalogue à l'aide du SDK Remote PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Mettez à jour un catalogue de machines existant afin d'inclure la propriété personnalisée `FailSafeStorageType`. Cette mise à jour n'affecte pas les machines virtuelles existantes.

1. Mettez à jour la propriété personnalisée dans la commande `Set-ProvScheme`. Par exemple :

```
    Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
    <CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
        machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
        instance`">
    <Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"
        Premium_LRS`" />
    <Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType
        `" Value=`"Premium_LRS`" />
    <Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
        Value=`"false`" />
    </CustomProperties>"
    <!--NeedCopy-->
```

Pour appliquer la modification effectuée dans Set-ProvScheme aux machines virtuelles existantes, exécutez la commande `Set-ProvVMUpdateTimeWindow` avec les paramètres `-StartsNow` et `-DurationInMinutes -1`.

1. Exécutez la commande `Set-ProvVMUpdateTimeWindow` avec les paramètres `-StartsNow` et `-DurationInMinutes -1`. Par exemple :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

2. Redémarrez les machines virtuelles.

### Créer des machines virtuelles compatibles avec la mise en veille prolongée

Dans les environnements Azure, vous pouvez créer un catalogue de machines MCS qui est compatible avec la mise en veille prolongée. Grâce à cette fonctionnalité, vous pouvez suspendre une machine virtuelle, puis vous reconnecter à l'état précédent de la machine virtuelle lorsqu'un utilisateur se connecte à nouveau.

La fonctionnalité de mise en veille prolongée s'applique aux éléments suivants :

- OS mono-session
- Machines virtuelles persistantes et non persistantes
- Bureaux VDI statiques et aléatoires (groupés)

Vous pouvez revenir à la même session après avoir mis une machine virtuelle en veille prolongée, que le bureau VDI soit statique ou aléatoire.

Dans cette section, consultez les rubriques suivantes :

- Logiciel requis
- Limitations
- Créer et gérer un catalogue de machines virtuelles compatibles avec la mise en veille prolongée
- Créer un catalogue pour des machines virtuelles existantes compatibles avec la mise en veille prolongée
- Activer la mise en veille prolongée sur des machines virtuelles existantes provisionnées par MCS
- Vérifier la propriété de mise en veille prolongée
- Gestion de l'alimentation des machines virtuelles (manuelle et automatisée)

#### Conditions préalables à l'utilisation de la mise en veille prolongée

Pour utiliser la mise en veille prolongée, effectuez les tâches suivantes :

- Installez Azure machine virtuelle Agent sur l'image principale pour Windows et Linux. Le fichier de page de l'image Windows peut se trouver sur le disque temporaire. MCS définit l'emplacement du fichier de page sur le lecteur C : du disque de base lorsque la mise en veille prolongée est activée sur le catalogue de machines.

- MCS définit automatiquement la propriété de mise en veille prolongée pour les ressources générées. Il n'est pas nécessaire de configurer les propriétés des ressources principales pour prendre en charge la mise en veille prolongée.
- Utilisez une taille de machine virtuelle compatible avec la mise en veille prolongée dans votre abonnement.
- Créez un profil de machine compatible avec la mise en veille prolongée (machine virtuelle ou spécification de modèle) afin que les machines virtuelles héritent de cette capacité. Pour créer la machine virtuelle, consultez Bien démarrer avec la mise en veille prolongée.

  > **Remarque :**
  >
  > Selon Microsoft, vous pouvez déployer des machines virtuelles compatibles avec la mise en veille prolongée à partir d'un disque du système d'exploitation. Cette fonctionnalité est actuellement prise en charge dans certaines régions et sera bientôt disponible pour toutes les régions. Pour plus d'informations, consultez Déployer des machines virtuelles sur lesquelles est activée la mise en veille prolongée à partir du disque du système d'exploitation.

  Pour créer la spécification de modèle, procédez comme suit :

  1. Ouvrez le portail Azure. Choisissez une machine virtuelle dont vous souhaitez utiliser la configuration dans le modèle. Sélectionnez **Exporter le modèle** dans le volet de gauche.
  2. Décochez la case **Inclure les paramètres**. Copiez le contexte et enregistrez-le sous forme de fichier JSON, par exemple `VMExportTemplate.json`.
  3. Assurez-vous que le paramètre `hibernationEnabled` est **`true`** dans le modèle. Si le paramètre n'est pas **`true`**, vérifiez la configuration de la machine virtuelle que vous avez utilisée. Vous pouvez spécifier une taille de machine virtuelle prise en charge dans le fichier modèle. Toutefois, vous pouvez également spécifier la taille de la machine lors de la création du catalogue.
  4. Ajoutez le modèle de la ressource d'interface réseau au fichier JSON `VMExportTemplate.json`. Vous disposez alors d'un fichier modèle ARM contenant deux ressources.
  5. Sélectionnez **Portail Azure > Spécifications du modèle > Importer le modèle > Choisissez un fichier de modèle local** pour importer ce fichier de modèle en tant que spécification de modèle ARM.
  6. Une fois la spécification de modèle ARM créée, vous pouvez l'utiliser comme profil de machine.

  > **Remarque :**
  >
  > La synchronisation avec Citrix Studio peut prendre quelques minutes.

Pour plus d'informations, consultez le document Microsoft Prérequis à l'utilisation de la mise en veille prolongée.

#### Limitations

- Seuls les catalogues de machines avec OS mono-session (persistants et non persistants) sont pris en charge.
- Les fonctionnalités de disque de système d'exploitation éphémères et d'E/S MCS ne prennent pas en charge la mise en veille prolongée Azure.
- La mise en veille prolongée peut échouer lors des mises à jour automatiques de Windows.

Pour plus d'informations, veuillez consulter la documentation Microsoft.

### Créer et gérer un catalogue de machines virtuelles compatibles avec la mise en veille prolongée

Pour créer des machines virtuelles compatibles avec la mise en veille prolongée, vous pouvez créer et gérer un catalogue de machines compatibles avec la veille prolongée en utilisant les outils suivants :

- Studio Web ou
- Commandes PowerShell

#### Créer un catalogue à l'aide de Web Studio

1. Sélectionnez **Créer un catalogue de machines**. L'assistant de création de catalogues s'ouvre.
2. Sur la page **Type de machine**, sélectionnez le type de machine avec **OS mono-session** pour ce catalogue.
3. Sur la page **Gestion des machines**, sélectionnez les paramètres comme suit :
    a) Sélectionnez **Machines dont l'alimentation est gérée (par exemple, machines virtuelles ou PC lames)**.
    b) Sélectionnez **Citrix Machine Creation Services (MCS)**.
4. Sur la page **Expérience de bureau**, sélectionnez l'expérience de bureau aléatoire ou statique selon vos besoins.
5. Sur la page **Image**, sélectionnez une image principale. Cochez la case **Utiliser un profil de machine** et sélectionnez un profil de machine compatible avec la mise en veille prolongée. Cliquez sur l'infobulle pour savoir si un profil de machine est compatible avec la mise en veille prolongée.
6. Sur la page **Types de stockage et de licence**, sélectionnez le stockage et la licence à utiliser pour ce catalogue.
7. Sur la page **Machines virtuelles**, sélectionnez le nombre de machines virtuelles, la taille des machines virtuelles et la zone de disponibilité.

> **Remarque :**
>
> Les tailles de machine compatibles avec la mise en veille prolongée ne sont affichées que pour votre sélection.

8. Sur la page **Cartes d'interface réseau**, ajoutez les cartes d'interface réseau que vous souhaitez que les machines virtuelles utilisent.
9. Sur la page **Paramètres du disque**, sélectionnez le type de stockage et la taille du disque de cache en écriture différée.
10. Sur la page **Groupe de ressources**, sélectionnez le groupe de ressources pour provisionner les machines virtuelles.
11. Sur la page **Identités des machines**, sélectionnez **Créer de nouveaux comptes Active Directory**. Spécifiez ensuite un schéma d'affectation de nom de compte.
12. Sur la page **Informations d'identification du domaine**, cliquez sur **Entrez les informations d'identification**. Entrez les informations d'identification de votre domaine pour effectuer la création de compte dans le domaine Active Directory cible.
13. Sur la page **Résumé**, entrez un nom pour le catalogue de machines, puis cliquez sur **Terminer**.

Lorsque la création du catalogue de machines MCS est terminée, localisez le catalogue dans la liste des catalogues, puis cliquez sur l'onglet **Propriétés du modèle**. La valeur du paramètre **Veille prolongée** doit être **Pris en charge**.

Si vous souhaitez modifier un catalogue de machines, tenez compte des restrictions suivantes :

- Si le catalogue de machines actuel prend en charge la mise en veille prolongée, vous ne pouvez pas :
  - Modifier la taille de la machine virtuelle en taille qui ne prend pas en charge la mise en veille prolongée.
  - Modifier le profil de machine en profil qui ne prend pas en charge la mise en veille prolongée.
- Si le catalogue de machines actuel ne prend pas en charge la mise en veille prolongée, vous ne pouvez pas :
  - remplacer pour le moment le profil de la machine par un profil compatible avec la mise en veille prolongée à l'aide du Web Studio. Vous pouvez toutefois le faire à l'aide des commandes PowerShell. Reportez-vous à la section Activer la mise en veille prolongée sur des machines virtuelles existantes provisionnées par MCS.

**Créer un catalogue pour gérer des machines virtuelles existantes compatibles avec la mise en veille prolongée** Si vous possédez déjà des machines virtuelles compatibles avec la mise en veille

prolongée et que vous souhaitez les suspendre et les reprendre, créez un catalogue de machines pour importer ces machines virtuelles à des fins de gestion de l'alimentation.

> **Remarque :**
>
> Vous pouvez créer un catalogue de machines contenant à la fois des machines virtuelles compatibles avec la mise en veille prolongée et des machines virtuelles non compatibles. Toutefois, si vous souhaitez bénéficier de fonctionnalités de mise en veille prolongée, vous devez créer le catalogue de machines avec uniquement des machines virtuelles compatibles avec la mise en veille prolongée.

Pour créer un catalogue de machines virtuelles existantes compatibles avec la mise en veille prolongée à l'aide de Web Studio, suivez les instructions à l'écran pour terminer les étapes et faites attention aux paramètres clés suivants :

1. Sur la page **Gestion des machines**, sélectionnez **Machines dont l'alimentation est gérée** et **Autre service ou technologie**.
2. Sur la page **Machines virtuelles**, ajoutez ou importez uniquement les machines virtuelles compatibles avec la mise en veille prolongée.

**Créer un catalogue de machines à l'aide de commandes PowerShell** Une fois que vous avez satisfait à toutes les exigences relatives à l'utilisation de la mise en veille prolongée, vous pouvez créer un catalogue de machines compatibles avec la mise en veille prolongée à l'aide de la commande `New-ProvScheme`. Pour plus d'informations sur la création d'un catalogue à l'aide de Remote PowerShell SDK, consultez New-ProvScheme.

Lors de la création du catalogue, vous pouvez vérifier si la taille d'une machine virtuelle et le profil de machine prennent en charge la mise en veille prolongée ou non à l'aide des commandes PowerShell suivantes :

- Pour la taille de machine virtuelle, exécutez la commande suivante et vérifiez si la propriété `supportsHibernation` est **True**. Par exemple,

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath @
    ("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.
    folder") | select Name, AdditionalData | ConvertTo-Json
<!--NeedCopy-->
```

- Pour le profil de machine, exécutez la commande suivante et vérifiez si la propriété `supportsHibernation` est **True**. Par exemple,

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath @
    ("XDHyp:\HostingUnits\ <VirtualNetwork> \machineprofile.folder
    \abc.resourcegroup")|select Name, AdditionalData|ConvertTo-
    Json
<!--NeedCopy-->
```

Si vous souhaitez modifier un catalogue de machines, tenez compte des restrictions suivantes :

- Si le catalogue de machines actuel prend en charge la mise en veille prolongée, vous ne pouvez pas :
  - Modifier la taille de machine virtuelle en taille qui ne prend pas en charge la mise en veille prolongée
  - Modifier le profil de machine en profil qui ne prend pas en charge la mise en veille prolongée
- Si le catalogue de machines actuel ne prend pas en charge la mise en veille prolongée, vous ne pouvez pas :
  - remplacer pour le moment le profil de la machine par un profil compatible avec la mise en veille prolongée à l'aide de Web Studio. Vous pouvez toutefois le faire à l'aide des commandes PowerShell. Reportez-vous à la section Activer la mise en veille prolongée sur des machines virtuelles existantes provisionnées par MCS.

Pour plus d'informations sur la manière de modifier la taille de machine virtuelle et le profil de machine d'un catalogue à l'aide du SDK Remote PowerShell, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/.

#### Activer la mise en veille prolongée sur des machines virtuelles existantes provisionnées par MCS

Vous pouvez activer la mise en veille prolongée Azure pour les machines suivantes :

- machines virtuelles provisionnées par Windows MCS d'un catalogue de machines créées sans disque temporaire.
- machines virtuelles provisionnées par Linux MCS d'un catalogue de machines créées avec et sans disque temporaire.

> **Remarque :**
>
> - Un agent Azure machine virtuelle doit être installé sur les machines virtuelles provisionnées par MCS existantes.
> - Actuellement, vous pouvez uniquement utiliser la commande PowerShell pour activer cette fonctionnalité.

Pour ce faire :

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell spécifiques à Citrix.

3. Vérifiez la configuration des machines existantes. Par exemple :

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Activez la mise en veille prolongée sur ce catalogue de machines à l'aide de la commande `Set-ProvScheme`. Par exemple :

```
Set-ProvScheme -provisioningSchemeName xxxx
-machineprofile <path-to-machineprofile-with-hibernation-enabled>
-serviceoffering "XDHyp:\HostingUnits\msc-dev\serviceoffering.
    folder\Standard_D4as_v5.serviceoffering"
<!--NeedCopy-->
```

5. Demandez une mise à jour sur les machines virtuelles existantes dans un catalogue de machines.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeUid xxxx -VMName <
    String[]
<!--NeedCopy-->
```

6. Redémarrez les machines virtuelles pour déclencher des mises à jour sur les machines virtuelles existantes. Par exemple :

```
New-BrokerHostingPowerAction -machinename "<name>" -Action Restart
<!--NeedCopy-->
```

#### Vérifier la propriété de mise en veille prolongée

Vous pouvez vérifier la propriété de mise en veille prolongée d'un catalogue de machines, d'une machine virtuelle et d'une machine broker à l'aide des commandes PowerShell :

- Pour vérifier la propriété de mise en veille prolongée d'un schéma de provisioning, exécutez les commandes PowerShell suivantes. Le paramètre `HibernationEnabled` doit être `True`.

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).
    VMMetadata -join "" |  ConvertFrom-Json | Select
    HibernationEnabled
<!--NeedCopy-->
```

- Pour vérifier la propriété de mise en veille prolongée d'une machine virtuelle de provisioning, exécutez les commandes PowerShell suivantes. Le paramètre `SupportsHibernation` doit être `True`.

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json
    | Select SupportsHibernation
<!--NeedCopy-->
```

- Pour vérifier la capacité de mise en veille prolongée d'une machine broker, exécutez les commandes PowerShell suivantes. Les actions d'alimentation **Suspendre** et **Reprendre** indiquent la capacité de mise en veille prolongée.

```
(Get-BrokerMachine -MachineName <YourMachineName>).
   SupportedPowerActions
<!--NeedCopy-->
```

### Gestion de l'alimentation des machines virtuelles compatibles avec la mise en veille prolongée

Vous pouvez effectuer les opérations de gestion de l'alimentation suivantes sur les machines virtuelles compatibles avec la mise en veille prolongée :

- **Suspendre** une machine virtuelle de son état d'exécution
- **Reprendre** une machine virtuelle à partir de l'état suspendu
- **Forcer l'arrêt** d'une machine virtuelle à partir d'un état suspendu
- **Forcer le redémarrage** d'une machine virtuelle à partir de l'état suspendu

Consultez les informations suivantes pour obtenir plus d'informations :

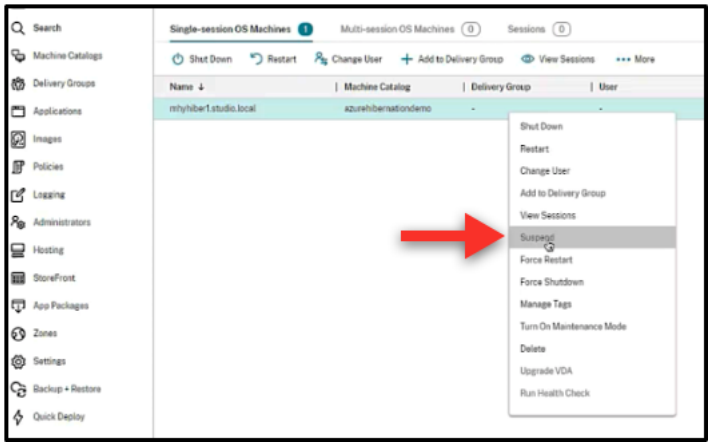
- Suspendre
- Reprendre

**Suspendre** Vous pouvez suspendre une machine virtuelle de l'une des manières suivantes :

- Utilisation **manuelle** de Web Studio
- **Automatiquement** à l'aide de la stratégie de délai d'expiration : pour plus d'informations, voir Paramètres divers.

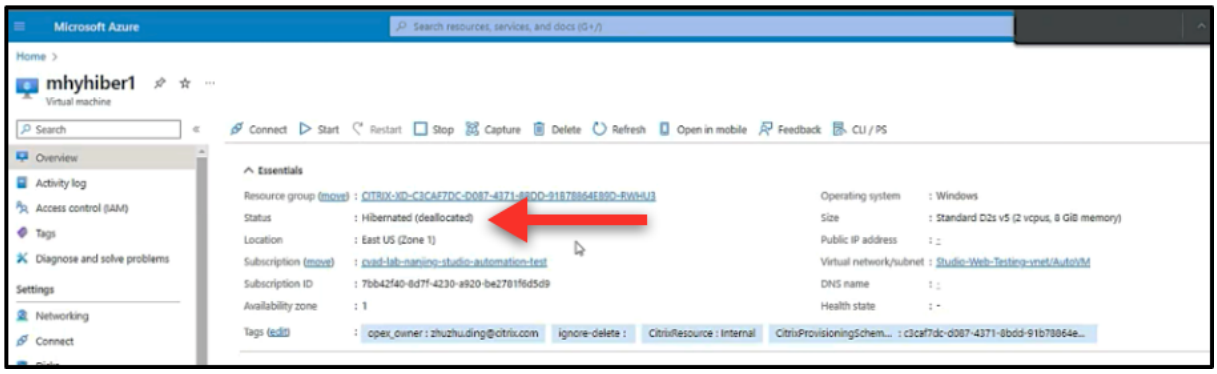
Pour suspendre manuellement une machine virtuelle :

1. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Suspendre**. Cliquez sur **Oui** pour confirmer l'action. L'**état d'alimentation** passe de **Suspension en cours** à **Suspendu**.



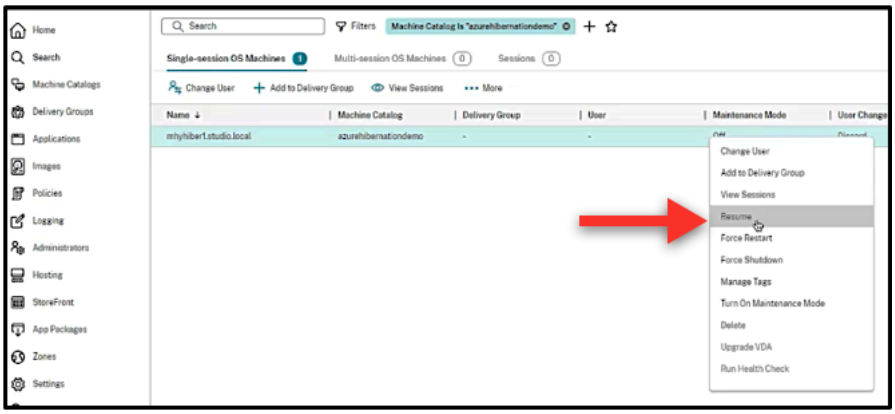

 

Vous pouvez vérifier l'état de la machine virtuelle sur le portail Azure.

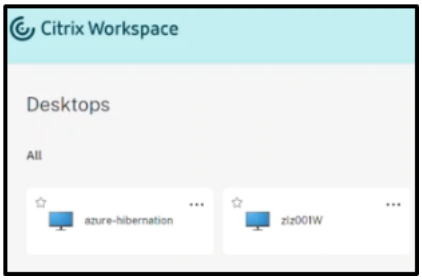



**Reprendre** Pour reprendre une machine virtuelle mise en veille prolongée, utilisez l'une des méthodes suivantes :

- **Manuellement** :
  - Les administrateurs peuvent reprendre la machine virtuelle à l'aide de Web Studio.




  - Les utilisateurs finaux peuvent démarrer la machine virtuelle à l'aide du menu Citrix Workspace une fois qu'ils ont cliqué sur l'icône du bureau.

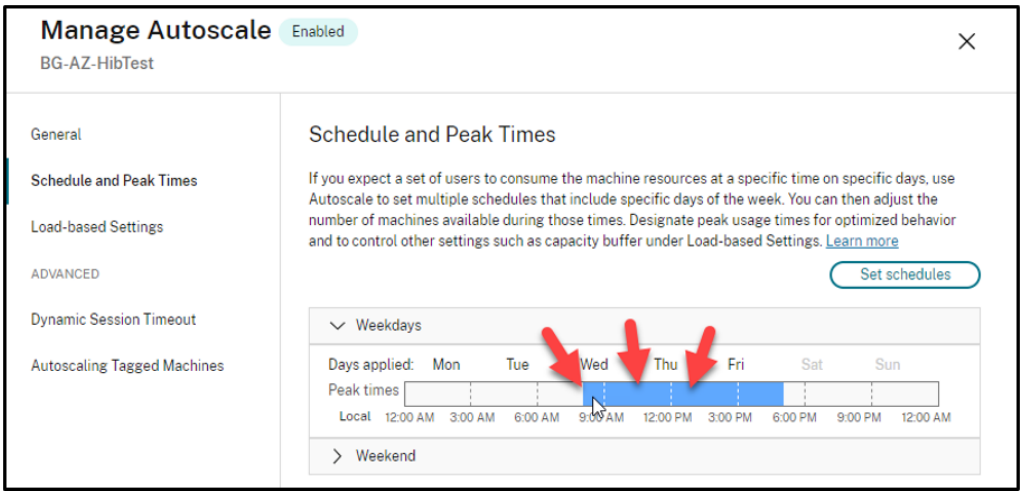



- **Automatiquement** :
  - Autoscale peut automatiquement allumer les machines mises en veille prolongée si vous configurez correctement les heures de pointe. Vous pouvez définir les heures de pointe par

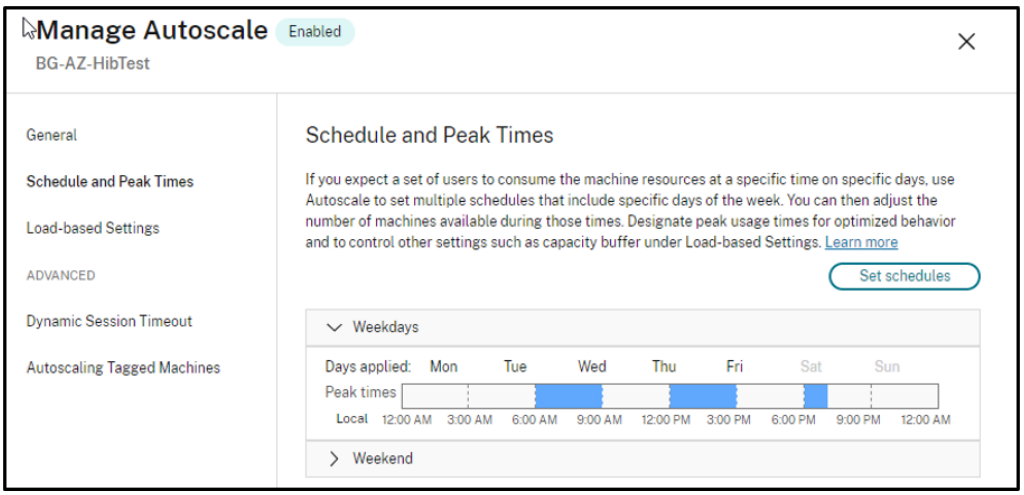
 

intervalles de 30 minutes en cliquant sur le calendrier. Chaque cadre bleu représente une plage horaire marquée comme heure de pointe. Les heures de pointe peuvent comporter des plages horaires consécutives et non consécutives.

* Plages horaires consécutives

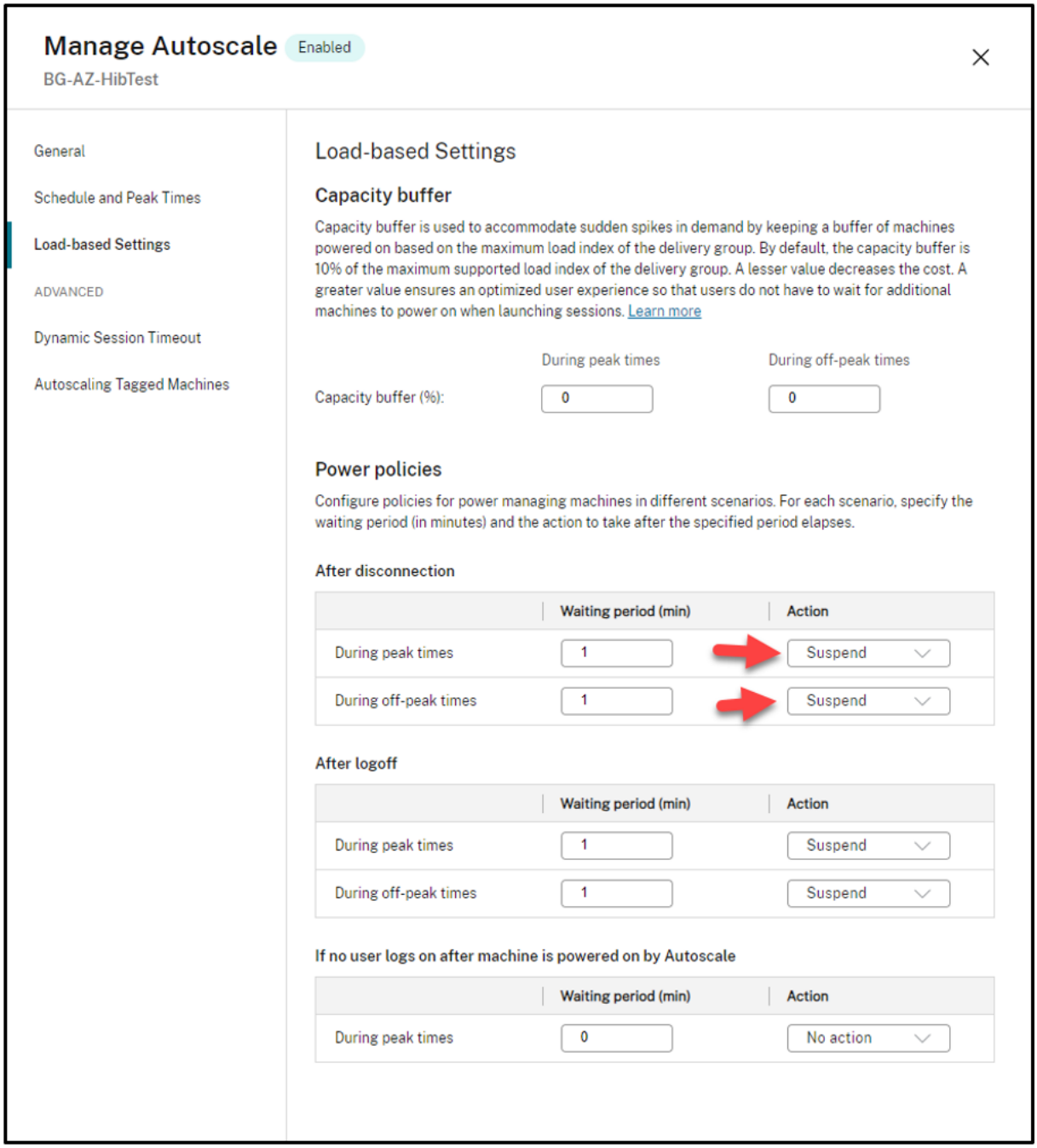



* Plages horaires non consécutives




> **Remarque :**
>
> Dans **Gérer Autoscale > Paramètres basés sur la charge**, si l'**action** est configurée sur **Suspendre**, assurez-vous que toutes les machines virtuelles de ce groupe de mise à disposition disposent d'une fonctionnalité de mise en veille prolongée. Dans le cas contraire, les machines virtuelles qui ne peuvent pas passer en veille prolongée continuent de fonctionner.




## Informations supplémentaires

Pour plus d'informations sur la mise en veille prolongée de Citrix Azure, consultez l'article Tech Zone de Citrix.

# Stratégies de sécurité

June 27, 2024

Cet article décrit les fonctionnalités de sécurité des différents services cloud pris en charge. Les fonctionnalités de sécurité incluent :

- Groupes de sécurité
- Démarrage sécurisé
- Fonctionnalités de chiffrement

# Groupes de sécurité

June 27, 2024

Le groupe de sécurité est un groupe de règles de sécurité permettant de filtrer le trafic réseau entre les ressources d'un réseau virtuel. Les règles de sécurité autorisent ou interdisent le trafic réseau entrant ou sortant pour plusieurs types de ressources. Chaque règle définit les propriétés suivantes :

- Nom : nom unique au sein du groupe de sécurité réseau
- Priorité : les règles sont traitées par ordre de priorité, les numéros les plus petits étant traités avant les plus élevés, car les plus petits numéros ont une priorité plus élevée
- Source ou destination : n'importe quelle adresse IP ou une adresse IP individuelle, un bloc de routage CIDR (10.0.0.0/24, par exemple), une étiquette de service ou un groupe de sécurité d'applications
- Protocole : protocoles sur la base desquels vous ajoutez des règles pour chaque groupe de sécurité
- Sens : si la règle s'applique au trafic entrant ou sortant
- Plage de ports : vous pouvez spécifier un port individuel ou une série de ports
- Action : autoriser ou refuser

Consultez les informations suivantes pour en savoir plus sur les hyperviseurs pris en charge :

- Groupes de sécurité dans AWS
- Groupes de sécurité dans Microsoft Azure
- Groupes de sécurité dans Google Cloud Platform

### Groupes de sécurité dans AWS

Les groupes de sécurité agissent en tant que pare-feu virtuels qui contrôlent le trafic pour les instances dans votre VPC. Vous devez ajouter des règles à vos groupes de sécurité permettant aux instances de votre sous-réseau public de communiquer avec les instances de votre sous-réseau privé. Vous pouvez également associer ces groupes de sécurité avec chaque instance dans votre VPC. Les règles entrantes contrôlent le trafic entrant dans votre instance, et les règles sortantes contrôlent le trafic sortant de votre instance.

Pour plus d'informations sur les paramètres réseau lors de la préparation de l'image, consultez la section Paramètres réseau lors de la préparation de l'image.

Lorsque vous lancez une instance, vous pouvez spécifier un ou plusieurs groupes de sécurité. Pour configurer des groupes de sécurité, consultez la section Configurer des groupes de sécurité.

### Groupes de sécurité dans Microsoft Azure

Citrix Virtual Apps and Desktops prend en charge les groupes de sécurité réseau dans Azure. Les groupes de sécurité réseau doivent être associés à des sous-réseaux. Pour plus d'informations, consultez la section Groupes de sécurité réseau.

Pour plus d'informations sur le groupe de sécurité réseau créé lors de la préparation de l'image, consultez la sectionCréer un catalogue de machines à l'aide d'une image Azure Resource Manager.

### Groupes de sécurité dans Google Cloud Platform

Lors de la préparation d'un catalogue de machines, une image de machine est préparée pour servir de disque système d'image principale pour le catalogue. Lors de ce processus, le disque est temporairement attaché à une machine virtuelle. Cette machine virtuelle doit s'exécuter dans un environnement isolé qui empêche tout le trafic réseau entrant et sortant. Pour cela, une paire de règles de pare-feu deny-all est utilisée. Pour plus d'informations, consultez la section Règles de pare-feu.

## Démarrage sécurisé

June 27, 2024

Le démarrage sécurisé est conçu pour garantir que seul un logiciel fiable est utilisé pour démarrer le système. Le microprogramme dispose d'une base de données de certificats sécurisés et vérifie que l'image qu'il charge est signée par l'un des certificats sécurisés. Si cette image charge d'autres images, cette image doit également être vérifiée de la même manière. vTPM est une instance logicielle

virtualisée d'un module TPM physique traditionnel. vTPM permet de vérifier la fiabilité en mesurant l'ensemble de la chaîne de démarrage de votre machine virtuelle (UEFI, système d'exploitation, système et pilotes).

Pour plus d'informations sur les services cloud pris en charge, consultez les rubriques suivantes :

- Démarrage sécurisé dans Google Cloud Platform
- Démarrage sécurisé dans Microsoft Azure
- Démarrage sécurisé dans VMware

### Démarrage sécurisé dans Google Cloud Platform

Vous pouvez provisionner des machines virtuelles protégées sur GCP. Une machine virtuelle protégée est renforcée par un ensemble de contrôles de sécurité qui fournissent une intégrité vérifiable de vos instances Compute Engine, en utilisant des fonctionnalités avancées de sécurité de plate-forme telles que le démarrage sécurisé, un module de plate-forme virtuelle de confiance, un microprogramme UEFI et la surveillance de l'intégrité.

Pour plus d'informations sur l'utilisation de PowerShell pour créer un catalogue avec machine virtuelle protégée, consultez la section Utiliser PowerShell pour créer un catalogue avec machine virtuelle protégée.

> **Remarque :**
>
> Si vous installez Windows 11 sur l'image principale, vous devez activer vTPM pendant le processus de création de l'image principale. Vous devez également activer vTPM sur la source du profil de la machine (machine virtuelle ou modèle d'instance). Pour plus d'informations sur la création de machines virtuelles Windows 11 sur le nœud à locataire unique, consultez Créer des machines virtuelles Windows 11 sur le nœud à locataire unique.

### Démarrage sécurisé dans Microsoft Azure

Dans les environnements Azure, vous pouvez créer des catalogues de machines avec lancement fiable. Azure propose le lancement fiable comme moyen transparent d'améliorer la sécurité des machines virtuelles de deuxième génération. Un lancement fiable protège contre les techniques d'attaque avancées et persistantes. Le démarrage sécurisé de votre machine virtuelle est à la base du lancement fiable. Le lancement fiable utilise également vTPM pour effectuer une vérification à distance par le cloud. Il est utilisé pour les vérifications de l'intégrité de la plate-forme et pour prendre des décisions basées sur la confiance. Vous pouvez activer individuellement le démarrage sécurisé et vTPM. Pour plus d'informations sur la création d'un catalogue de machines avec lancement fiable, consultez Catalogues de machines avec lancement fiable.

### Démarrage sécurisé dans VMware

MCS prend en charge la création d'un catalogue de machines avec le modèle VMware associé au vTPM comme source pour l'entrée de profil de machine. Si Windows 11 est installé sur l'image principale, le vTPM doit être activé pour l'image principale. Par conséquent, le modèle VMware, qui est une source de profil de machine, doit être associé au vTPM. Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'un profil de machine.

## Fonctionnalités de chiffrement

June 27, 2024

Les fonctionnalités de chiffrement protègent le contenu des machines virtuelles contre les attaques d'invités malveillants sur un hôte de machine virtuelle partagé et contre les attaques lancées par le logiciel de contrôle de l'hyperviseur qui gère toutes les machines virtuelles de l'hôte.

Pour plus d'informations sur les services cloud pris en charge, consultez les rubriques suivantes :

- Fonctionnalités de chiffrement dans AWS
- Fonctionnalités de chiffrement dans Google Cloud Platform
- Fonctionnalités de chiffrement dans Microsoft Azure

### Fonctionnalités de chiffrement dans AWS

Cette section décrit les fonctionnalités de chiffrement des environnements de virtualisation AWS.

#### Chiffrement automatique

Vous pouvez activer le chiffrement automatique des nouveaux volumes Amazon EBS et des copies instantanées créées sur votre compte. Pour plus d'informations, consultez la section Chiffrement automatique.

### Fonctionnalités de chiffrement dans Google Cloud Platform

Cette section décrit les fonctionnalités de chiffrement des environnements de virtualisation Google Cloud Platform (GCP).

Si vous avez besoin de plus de contrôle sur les opérations liées aux clés que ne le permettent les clés de chiffrement gérées par Google, vous pouvez utiliser des clés de chiffrement gérées par le client.

Lorsque vous utilisez une clé de chiffrement gérée par le client, un objet est chiffré avec cette clé par Cloud Storage au moment où il est stocké dans un bucket, et l'objet est automatiquement déchiffré par Cloud Storage lorsqu'il est communiqué aux demandeurs. Pour plus d'informations, consultez Clés de chiffrement gérées par le client.

Vous pouvez utiliser des clés de chiffrement gérées par le client (CMEK) pour les catalogues MCS. Pour plus d'informations, consultez la section Utilisation de clés de chiffrement gérées par le client (CMEK).

## Fonctionnalités de chiffrement dans Microsoft Azure

Cette section décrit les fonctionnalités de chiffrement des environnements de virtualisation Azure.

### Chiffrement Azure côté serveur

La plupart des disques gérés par Azure sont chiffrés à l'aide du chiffrement de stockage Azure, qui utilise le chiffrement côté serveur (SSE) pour protéger vos données et vous aider à respecter vos engagements en matière de sécurité et de conformité. Citrix Virtual Apps and Desktops prend en charge les clés de cryptage gérées par le client pour les disques gérés Azure via Azure Key Vault. Pour plus d'informations, consultez Chiffrement Azure côté serveur.

### Cryptage de disque sur l'hôte Azure

Vous pouvez créer un catalogue de machines MCS avec fonctionnalité de cryptage sur l'hôte.

Cette méthode de chiffrement ne chiffre pas les données via le stockage Azure. Le serveur hébergeant la machine virtuelle chiffre les données, puis les données chiffrées circulent via le serveur de stockage Azure. Par conséquent, cette méthode de chiffrement chiffre les données de bout en bout.

Pour plus d'informations sur la création d'un catalogue de machines MCS avec fonctionnalité de cryptage sur l'hôte, consultez Cryptage de disque sur l'hôte Azure.

### Chiffrement double Azure

Le chiffrement double est un chiffrement côté plate-forme (par défaut) et un chiffrement géré par le client (CMEK). Par conséquent, si vous êtes un client gérant des données sensibles en termes de sécurité et que vous êtes préoccupé par le risque associé à un algorithme de cryptage, à une mise en œuvre ou à une clé compromise, vous pouvez opter pour ce cryptage double. Les disques du système d'exploitation et de données persistants, ainsi que les instantanés et les images sont chiffrés au repos à l'aide du chiffrement double. Pour plus d'informations, consultez la section Chiffrement double sur disque géré.

**Machines virtuelles confidentielles Azure**

Les machines virtuelles informatiques confidentielles Azure garantissent que votre bureau virtuel est chiffré en mémoire et protégé lors de son utilisation.

Vous pouvez utiliser MCS pour créer un catalogue avec des machines virtuelles confidentielles Azure. Vous devez utiliser le workflow du profil de machine pour créer un tel catalogue. Vous pouvez utiliser les spécifications de modèle VM et ARM comme entrée de profil de machine.

Pour plus d'informations, consultez la section Machines virtuelles confidentielles Azure.

## Créer des groupes de mise à disposition

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Un groupe de mise à disposition est une collection de machines sélectionnées à partir d'un ou de plusieurs catalogues de machines. Le groupe de mise à disposition indique quels utilisateurs peuvent utiliser ces machines et les applications et les bureaux à la disposition des utilisateurs.

La création d'un groupe de mise à disposition est la prochaine étape de la configuration de votre déploiement après la création d'un site et la création d'un catalogue de machines. Plus tard, vous pourrez modifier les paramètres initiaux dans le premier groupe de mise à disposition et créer d'autres groupes de mise à disposition. Il existe également des fonctionnalités et paramètres que vous pouvez configurer uniquement lors de la modification d'un groupe de mise à disposition, et non lors de sa création.

Pour Remote PC Access, lorsque vous créez un site, un groupe de mise à disposition appelé Bureaux Remote PC Access est automatiquement créé.

Pour créer un groupe de mise à disposition :

1. Si vous avez créé un site et un catalogue de machines sans groupe de mise à disposition, Web Studio vous guide vers le bon point de départ pour en créer un.
2. Si vous avez déjà créé un groupe de mise à disposition et que vous souhaitez en créer un autre, procédez comme suit :

a) Sélectionnez **Groupes de mise à disposition**. Sélectionnez **Créer un groupe de mise à disposition** dans le volet Actions.
b) Pour organiser les groupes de mise à disposition sous forme de dossiers, créez des dossiers dans le dossier **Groupes de mise à disposition** par défaut. Pour plus d'informations, voir Créer un dossier.
c) Sélectionnez le dossier dans lequel vous souhaitez créer le groupe, puis cliquez sur **Créer un groupe de mise à disposition**. L'assistant de création de groupe s'ouvre.

3. L'assistant s'ouvre avec une page **Introduction**, que vous pouvez supprimer des lancements ultérieurs de cet assistant.
4. L'assistant vous guide ensuite à travers les pages décrites dans la section suivante. Lorsque vous avez terminé chaque page, cliquez sur **Suivant** jusqu'à la page finale.

### Étape 1. Machines

Sur la page **Machines**, sélectionnez un catalogue et sélectionnez le nombre de machines que vous souhaitez utiliser dans ce catalogue.

À savoir :

- Au moins une machine doit rester non utilisée dans un catalogue sélectionné.
- Un catalogue peut être spécifié dans plusieurs groupes de mise à disposition. Une machine ne peut être utilisée que dans un seul groupe de mise à disposition.
- Un groupe de mise à disposition peut utiliser des machines de plus d'un catalogue, cependant ces catalogues doivent contenir les mêmes types de machines (OS multi-session, OS mono-session ou Remote PC Access). En d'autres termes, vous ne pouvez pas combiner des types de machines dans un groupe de mise à disposition. De même, si votre déploiement possède des catalogues de machines Windows et des catalogues de machines Linux, un groupe de mise à disposition peut contenir des machines d'un des types de système d'exploitation, mais pas les deux.
- Citrix vous recommande d'installer ou de mettre à niveau toutes les machines avec la version de VDA la plus récente. Mettez à niveau les catalogues et les groupes de mise à disposition au besoin. Lors de la création d'un groupe de mise à disposition, si vous sélectionnez des machines sur lesquelles sont installées différentes versions de VDA, le groupe de mise à disposition est compatible avec la version de VDA la plus ancienne Cela s'appelle le *niveau fonctionnel* du groupe. Par exemple, si l'une des machines dispose d'un VDA version 7.1 et que d'autres machines disposent de la version actuelle, toutes les machines du groupe peuvent uniquement utiliser les fonctionnalités qui étaient prises en charge dans le VDA 7.1. Cela signifie que certaines fonctionnalités qui nécessitent des versions de VDA ultérieures risquent de ne pas être disponibles dans ce groupe de mise à disposition.

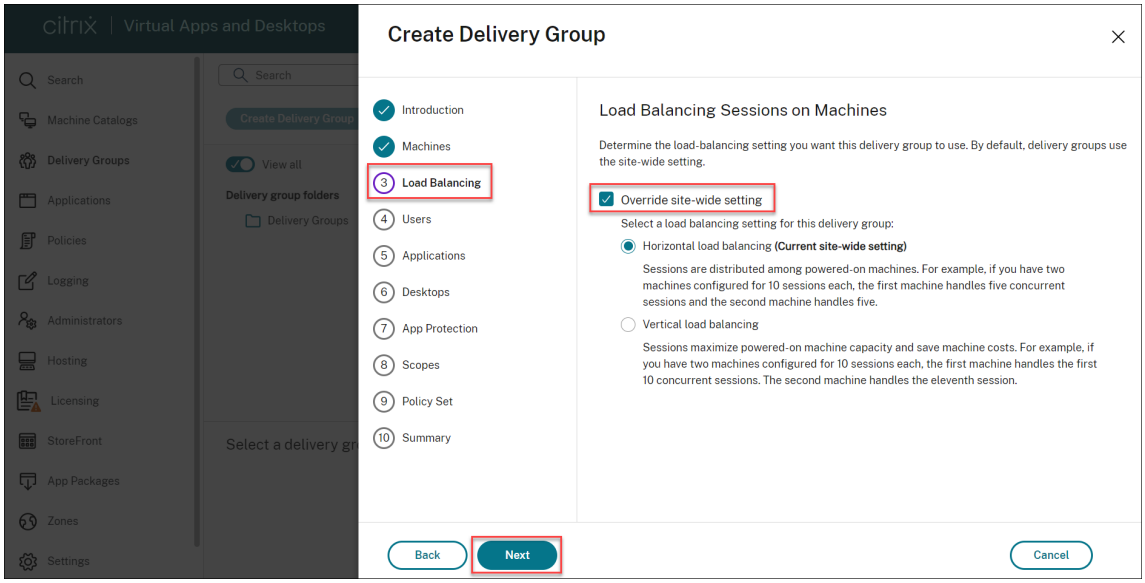
- Chaque machine d'un catalogue Remote PC Access est automatiquement associée à un groupe de mise à disposition. Lorsque vous créez un site Remote PC Access, un catalogue nommé Machines Remote PC Access et un groupe de mise à disposition appelé Bureaux Remote PC Access sont créés automatiquement.
- Les vérifications de compatibilité suivantes sont effectuées :
  - MinimumFunctionalLevel doit être compatible
  - SessionSupport doit être compatible
  - AllocationType doit être compatible avec SingleSession
  - ProvisioningType doit être compatible
  - PersistChanges doit être compatible avec MCS et Citrix Provisioning
  - Le catalogue RemotePC est uniquement compatible avec le catalogue RemotePC Access
  - Vérification associée à AppDisk

### Étape 2. Équilibrage de charge

Pour configurer les paramètres d'équilibrage de charge lors de la création d'un groupe de mise à disposition :

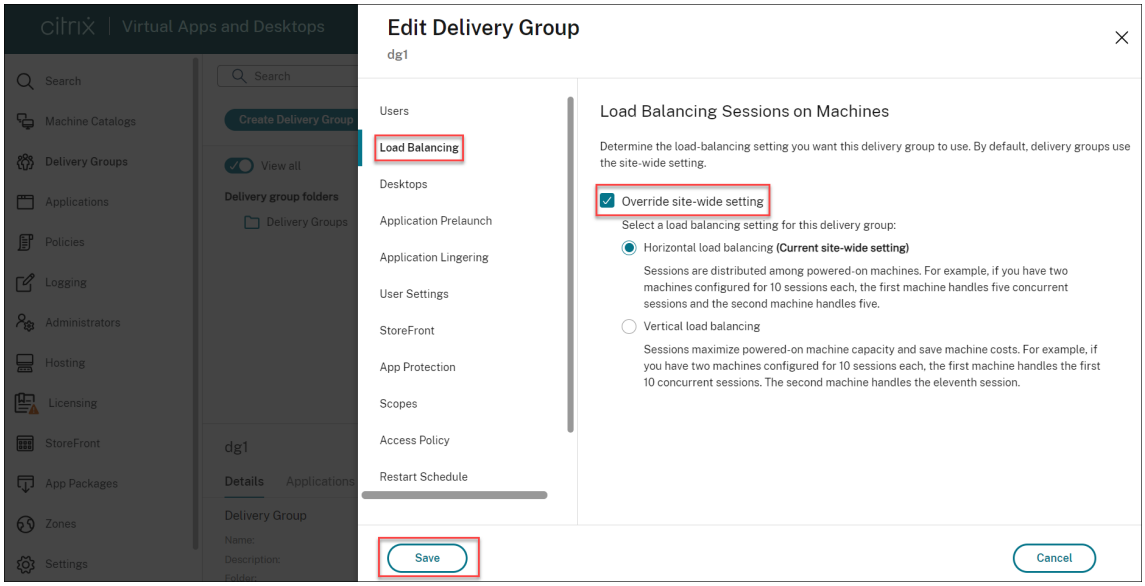
1. Connectez-vous à Web Studio.
2. Dans le menu de navigation de gauche, cliquez sur **Groupes de mise à disposition**.
3. Sur la page **Groupes de mise à disposition**, cliquez sur **Créer un groupe de mise à disposition**.
4. Dans l'assistant **Créer un groupe de mise à disposition**, cliquez sur **Suivant**. L'assistant **Machine** s'ouvre.
5. Dans l'assistant **Machines**, sélectionnez le catalogue de machines requis et cliquez sur **Suivant**. L'assistant **Équilibrage de charge** s'ouvre.
6. Dans l'assistant **Équilibrage de charge**, cochez la case **Remplacer paramètre à l'échelle du site**.
7. Sélectionnez l'option **Équilibrage de charge horizontal** ou l'option **Équilibrage de charge vertical** selon vos besoins et cliquez sur **Suivant**.



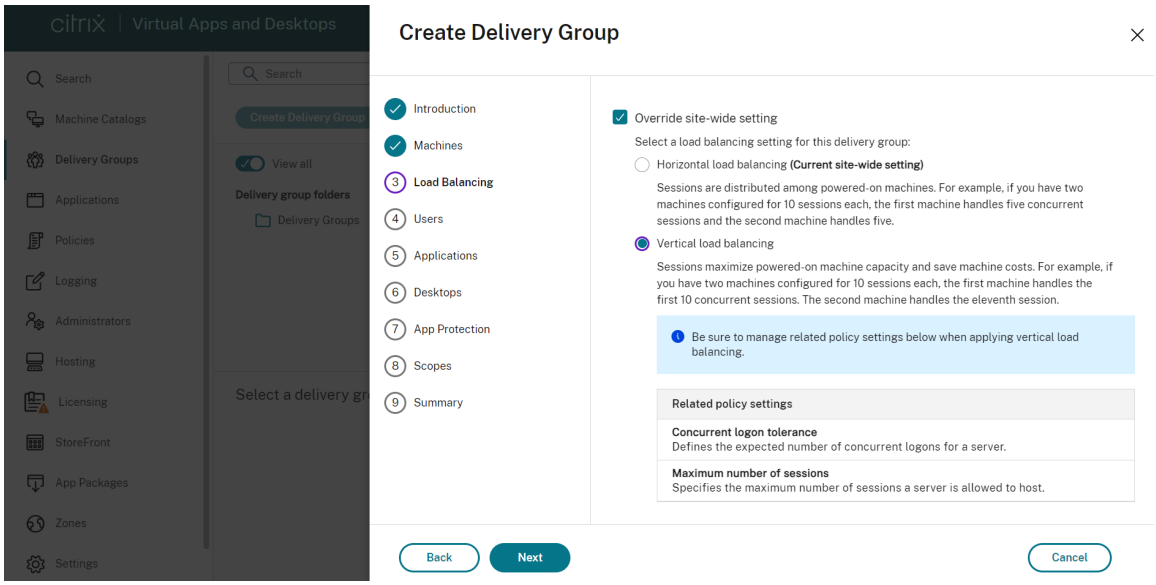

Pour configurer les paramètres d'équilibrage de charge lors de la modification d'un groupe de mise à disposition existant :

1. Connectez-vous à Web Studio.
2. Dans le panneau de gauche, cliquez sur **Groupes de mise à disposition**.
3. Sélectionnez un **groupe de mise à disposition** dans la liste et cliquez sur **Modifier**. L'assistant **Modifier le groupe de mise à disposition** s'ouvre.
4. Sur la page **Modifier le groupe de mise à disposition**, cliquez sur **Équilibrage de charge**.
5. Cochez la case **Remplacer paramètre à l'échelle du site**.
6. Sélectionnez l'option **Équilibrage de charge horizontal** ou **Équilibrage de charge vertical** selon vos besoins et cliquez sur **Enregistrer**.



> **Remarque :**
>
> Lorsque le paramètre d'équilibrage de charge vertical est appliqué, assurez-vous que les stratégies **Tolérance d'ouvertures de session simultanées** et **Nombre maximum de sessions** sont correctement configurées.




Pour en savoir plus sur l'équilibrage de charge au niveau du site et au niveau du groupe de mise à disposition, consulter l'article Équilibrer la charge des machines

### Étape 3. Type de mise à disposition

Cette page s'affiche uniquement si vous avez choisi un catalogue contenant des machines avec OS mono-session statiques (attribuées).

Sur la page **Type de mise à disposition**, choisissez **Applications** ou **Bureaux**. Vous ne pouvez pas activer les deux.

Si vous avez sélectionné des machines à partir d'un catalogue d'OS multi-session ou OS mono-session aléatoires (regroupés), le type de mise à disposition est applications et bureaux par défaut : vous pouvez mettre à disposition des applications, des bureaux, ou les deux.

### Étape 4. Utilisateurs

Spécifiez les utilisateurs et les groupes d'utilisateurs qui peuvent utiliser les applications et les bureaux dans le groupe de mise à disposition.

### Où les listes d'utilisateurs sont spécifiées

Les listes d'utilisateurs Active Directory sont spécifiées lorsque vous créez ou modifiez les informations suivantes :

- La liste d'accès utilisateur d'un site, qui n'est pas configurée dans Web Studio. Par défaut, la règle de stratégie d'admissibilité d'application inclut tout le monde. Consultez les applets de commande `BrokerAppEntitlementPolicyRule` du SDK PowerShell pour plus de détails.
- Les groupes d'applications (s'ils ont été configurés).
- Groupes de mise à disposition.
- Applications.

La liste des utilisateurs qui peuvent accéder à une application via StoreFront est constituée à partir de l'intersection des listes utilisateur ci-dessus. Par exemple, pour configurer l'utilisation d'une application A pour un département particulier, sans pour autant limiter l'accès à d'autres groupes :

- utiliser la règle de stratégie d'admissibilité d'application par défaut qui inclut tout le monde ;
- Configurez la liste des utilisateurs du groupe de mise à disposition pour autoriser les utilisateurs du siège social à utiliser toutes les applications spécifiées dans le groupe de mise à disposition.
- (Si des groupes d'applications sont configurés) Configurez la liste des utilisateurs du groupe d'applications pour permettre aux membres du département Administration et Finances d'accéder aux applications A à L.
- Configurez les propriétés de l'application A pour limiter sa visibilité uniquement au personnel des comptes clients du département Administration et Finances.

### Utilisateurs authentifiés et non authentifiés

Il existe deux types d'utilisateurs : authentifiées et non authentifiés (les utilisateurs non authentifiés sont également appelés anonymes). Vous pouvez configurer un ou deux types dans un groupe de mise à disposition.

- **Authentifiés :** pour accéder aux applications et aux bureaux, les utilisateurs et les membres du groupe que vous spécifiez par nom doivent présenter des informations d'identification comme une carte à puce ou un nom d'utilisateur et mot de passe à StoreFront ou l'application Citrix Workspace. Pour les groupes de mise à disposition contenant des machines avec OS de bureau, vous pouvez importer les données utilisateur (une liste des utilisateurs) plus tard en modifiant le groupe de mise à disposition.
- **Non authentifiés (anonymes) :** pour les groupes de mise à disposition contenant les machines avec OS multi-session, vous pouvez autoriser les utilisateurs à accéder à des applications et des bureaux sans présenter d'informations d'identification à StoreFront ou à l'application Citrix

Workspace. Par exemple, l'application peut nécessiter des informations d'identification, mais ce n'est pas le cas pour le portail et les outils d'accès Citrix. Un groupe d'utilisateurs anonymes est créé lorsque vous installez le premier Delivery Controller.

Pour accorder l'accès à des utilisateurs non authentifiés, chaque machine du groupe de mise à disposition doit posséder un VDA pour OS Windows Server (version minimum 7.6) installé. Lorsque des utilisateurs non authentifiés sont activés, vous devez disposer d'un magasin StoreFront non authentifié.

Des comptes d'utilisateurs non authentifiés sont créés sur demande lorsqu'une session est lancée et nommée Anon*XYZ*, dans lequel *XYZ* est une valeur unique à trois chiffres.

Les sessions d'utilisateur non authentifié possèdent un délai d'inactivité par défaut de 10 minutes ; de plus, les sessions sont automatiquement fermées lorsque le client se déconnecte. La reconnexion, l'itinérance entre les clients et le contrôle de l'espace de travail ne sont pas pris en charge.

Le tableau suivant décrit les choix disponibles sur la page **Utilisateurs** :

| Activer l'accès pour | Ajouter/affecter des utilisateurs et des groupes d'utilisateurs ? | Cocher la case « Autoriser les utilisateurs non authentifiés » ? |
|---|---|---|
| Seuls les utilisateurs authentifiés | Oui | Non |
| Seuls les utilisateurs non authentifiés | Non | Oui |
| À la fois les utilisateurs authentifiées et non authentifiés | Oui | Oui |

### Étape 5. Applications

À savoir :

- vous ne pouvez pas ajouter d'applications aux groupes de mise à disposition Remote PC Access.
- Par défaut, les applications que vous ajoutez sont placées dans un dossier nommé Applications. Vous pouvez spécifier un dossier différent. Pour de plus amples informations, veuillez consulter l'article Gérer les applications.
- Vous pouvez modifier les propriétés d'une application lorsque vous l'ajoutez à un groupe de mise à disposition ou ultérieurement. Pour de plus amples informations, veuillez consulter l'article Gérer les applications.

- Si vous essayez d'ajouter une application et qu'une application avec le même nom existe dans ce dossier, vous êtes invité à renommer l'application que vous ajoutez. Si vous refusez, l'application est ajoutée avec un suffixe qui la rend unique dans ce dossier d'application.
- Lorsque vous ajoutez une application à plusieurs groupes de mise à disposition, vous risquez de rencontrer un problème de visibilité si vous ne disposez pas d'autorisations suffisantes pour afficher l'application dans tous les groupes de mise à disposition. Dans ce cas, consultez un administrateur disposant des autorisations appropriées ou demandez une extension de vos autorisations à tous les groupes de mise à disposition auxquels l'application a été ajoutée.
- Si vous publiez deux applications du même nom vers les mêmes utilisateurs, modifiez la propriété Nom de l'application (pour l'utilisateur) dans Web Studio ; sinon, les utilisateurs voient des noms en double s'afficher dans l'application Citrix Workspace.

Cliquez sur **Ajouter** pour afficher les sources des applications.

- **À partir du menu Démarrer :** applications qui sont découvertes sur une machine créée à partir de l'image principale du catalogue sélectionné. Lorsque vous sélectionnez cette source, une nouvelle page s'ouvre avec une liste d'applications découvertes ; sélectionnez les applications que vous souhaitez ajouter, puis cliquez sur **OK**.
- **Manuellement :** applications situées sur un VDA dans le groupe de mise à disposition ou à un autre endroit de votre réseau. La sélection de cette source ouvre une nouvelle page dans laquelle vous pouvez spécifier l'application à ajouter de la manière suivante :
  - Saisissez le chemin d'accès de l'exécutable, le répertoire de travail, les arguments de la ligne de commande (facultatifs), et les noms affichés des administrateurs et des utilisateurs.
  - Sélectionnez une application à partir d'un VDA dans le groupe de mise à disposition. Pour ce faire, cliquez sur **Parcourir**, entrez les informations d'identification pour accéder au VDA, attendez d'être connecté au VDA, puis sélectionnez une application depuis le VDA. Les propriétés de l'application sélectionnée renseignent automatiquement les champs de la page.
- **Existantes :** applications déjà ajoutées au site, peut-être dans un autre groupe de mise à disposition. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Ajoutez les applications et cliquez sur **OK**.
- **App-V :** applications dans des packages App-V. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez sélectionner le serveur App-V ou la bibliothèque d'applications. Sélectionnez les applications que vous souhaitez ajouter à partir de l'écran des résultats et cliquez sur **OK**. Pour plus d'informations, consultez la section Déployer et fournir des applications App-V.

Si une source d'applications ou une application n'est pas disponible ou valide, elle n'est pas visible ou ne peut pas être sélectionnée. Par exemple, la source **existante** n'est pas disponible si aucune

application n'a été ajoutée au site. Ou une application peut ne pas être compatible avec les types de session pris en charge sur des machines du catalogue sélectionné.

### Étape 6. Bureaux

Le titre de cette page dépend du catalogue de machines que vous avez choisi sur la page **Machines** :

- Si vous avez choisi un catalogue contenant des machines regroupées, cette page est appelée **Bureaux**.
- Si vous avez choisi un catalogue contenant des machines attribuées et spécifié « Bureaux » sur la page **Type de mise à disposition**, cette page est appelée **Desktop User Assignments** (Attributions utilisateur bureau).
- Si vous avez choisi un catalogue contenant des machines attribuées et spécifié « Applications » sur la page **Type de mise à disposition**, cette page est appelée **Application Machine User Assignments** (Attributions utilisateur machine application).

Cliquez sur **Ajouter**. Effectuez les opérations suivantes dans cette boîte de dialogue :

- Dans les champs Nom d'affichage et Description, entrez les informations à afficher dans l'application Citrix Workspace.
- Pour ajouter une restriction de balise à un bureau, sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise dans la liste déroulante. Pour plus d'informations, veuillez consulter la section Balises.
- Utilisez les boutons radio pour lancer un bureau ou pour affecter une machine lors du lancement du bureau. Les utilisateurs peuvent être tout utilisateur pouvant accéder à ce groupe de mise à disposition, ou des utilisateurs et groupes d'utilisateurs spécifiques.
- Si le groupe contient des machines attribuées, spécifiez le nombre maximal de bureaux par utilisateur. Cette valeur doit être de 1 au minimum.
- Activez ou désactivez le bureau (pour les machines regroupées) ou la règle d'attribution de bureau (pour les machines attribuées). La désactivation d'un bureau arrête la mise à disposition du bureau. La désactivation d'une règle d'attribution de bureau arrête l'attribution automatique de bureaux aux utilisateurs.
- Lorsque vous avez terminé avec la boîte de dialogue, cliquez sur **OK**.

#### Nombre maximal d'instances d'un bureau dans un site (PowerShell uniquement)

Pour configurer le nombre maximal d'instances d'un bureau sur le site (PowerShell uniquement) :

- Dans PowerShell, utilisez l'applet de commande BrokerEntitlementPolicyRule appropriée avec le paramètre MaxPerEntitlementInstances. Par exemple, l'applet de commande suivante modi-

fie la règle `tsvda-desktop` pour définir le nombre maximal autorisé d'instances simultanées d'un bureau sur le site à deux. Lorsque deux instances de bureau sont en cours d'exécution, une erreur se produit si un troisième abonné tente de démarrer un bureau.

```
Set-BrokerEntitlementPolicyRule -Name tsvda-desktop -MaxPerEntitlementInst
 2
```

- Pour plus d'informations, utilisez l'applet de commande Get-Help. Par exemple, `Get-Help Set-BrokerEntitlementPolicyRule-Parameter MaxPerEntitlementInstances`.

### Étape 7. Résumé

Entrez un nom pour le groupe de mise à disposition. Vous pouvez également entrer une description (facultatif), qui s'affiche dans l'application Citrix Workspace et dans Web Studio.

Consultez les informations récapitulatives, puis cliquez sur **Terminer**.

## Gérer des groupes de mise à disposition

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

### Introduction

Cet article décrit les procédures permettant de gérer des groupes de mise à disposition depuis la console de gestion. En plus de la modification des paramètres spécifiés lors de la création du groupe, vous pouvez configurer d'autres paramètres qui ne sont pas disponibles lorsque vous créez un groupe de mise à disposition.

Les catégories de procédures sont les suivantes : général, utilisateurs, machines et sessions. Certaines tâches couvrent plusieurs catégories. Par exemple, « Empêcher les utilisateurs de se connecter aux machines » est décrit dans la catégorie Machines, mais affecte également les utilisateurs. Si vous ne trouvez pas une tâche dans une catégorie, vérifiez une catégorie associée.

D'autres articles contiennent également des informations connexes :

- La section Applications contient des informations sur la gestion des applications dans les groupes de mise à disposition.
- La gestion des groupes de mise à disposition nécessite les autorisations du rôle intégré d'administrateur de groupe de mise à disposition. Pour de plus amples informations, veuillez consulter la section Administration déléguée.

## General

- Afficher les détails du groupe
- Modifier le type de mise à disposition
- Modifier les adresses de StoreFront
- Modifier le niveau fonctionnel
- Gérer les groupes de mise à disposition Remote PC Access
- Organiser les groupes de mise à disposition sous forme de dossiers
- Gérer App Protection

### Afficher les détails du groupe

1. Utilisez la fonction de recherche pour localiser un groupe de mise à disposition spécifique. Pour obtenir des instructions, reportez-vous à la section Rechercher des instances.
2. Dans les résultats de la recherche, sélectionnez un groupe selon vos besoins.
3. Pour obtenir la description des colonnes du groupe, reportez-vous au tableau suivant.
4. Pour plus d'informations sur ce groupe, cliquez sur un onglet dans le volet d'informations inférieur.

| Colonne | Description |
|---|---|
| Groupe de mise à disposition | Nom du groupe et type de session. Les types de session incluent OS monosession et OS multisession. |
| Mise à disposition | Type de ressources fournies par ce groupe. Les valeurs possibles incluent Applications, Bureaux et Applications et bureaux. « Attribution de machine statique » s'affiche si le groupe de mise à disposition est composé de machines dédiées. |
| Sessions en cours d'utilisation | Nombre de machines configurées et nombre de machines dont l'état est Déconnecté. |
| Nombre alloué | Nombre de machines du catalogue attribuées à un groupe de mise à disposition. |

| Colonne | Description |
| --- | --- |
| Folder | Emplacement du groupe dans l'arborescence **Groupes de mise à disposition**. Affiche le nom du dossier dans lequel se trouve le groupe (y compris la barre oblique inverse de fin) ou indique − si le groupe se trouve au niveau racine. |

#### Modifier le type de mise à disposition d'un groupe de mise à disposition

Le type indique ce que le groupe de mise à disposition peut mettre à disposition : des applications, des bureaux, ou les deux.

Avant de changer un type **application uniquement** ou **bureaux et applications** en type **bureaux uniquement**, supprimez toutes les applications du groupe de mise à disposition.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **Type de mise à disposition**, sélectionnez le type de mise à disposition que vous voulez.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

#### Modifier les adresses de StoreFront

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **StoreFront**, sélectionnez ou ajoutez des URL StoreFront. Ces URL sont utilisées par l'application Citrix Workspace qui est installée sur chaque machine dans le groupe de mise à disposition.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

Vous pouvez également spécifier les adresses du serveur StoreFront en sélectionnant **StoreFront** dans le volet de gauche.

### Modifier le niveau fonctionnel

Modifiez le niveau fonctionnel pour le groupe de mise à disposition après avoir mis à niveau les VDA sur les machines et les catalogues de machines contenant les machines utilisées dans le groupe de mise à disposition.

Avant de commencer :

- Si vous utilisez Citrix Provisioning (anciennement Provisioning Services), vous devez mettre à niveau la version du VDA dans la console Citrix Provisioning.
- Démarrez les machines contenant le VDA mis à niveau afin qu'elles puissent s'enregistrer avec le Delivery Controller. Ce processus informe la console de la nature des éléments nécessitant une mise à niveau dans le groupe de mise à disposition.
- Si vous devez continuer à utiliser des versions antérieures du VDA, les fonctionnalités plus récentes ne sont pas disponibles. Pour de plus amples informations, consultez la documentation de mise à niveau.

Pour mettre à niveau un groupe de mise à disposition :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe de mise à disposition, puis cliquez sur **Mettre à niveau le groupe de mise à disposition** dans la barre d'actions. L'action **Modifier le niveau fonctionnel** s'affiche uniquement si des VDA mis à niveau sont détectés.

L'écran indique pour quelles machines, le cas échéant, le niveau fonctionnel ne peut pas être modifié et pourquoi. Vous pouvez ensuite annuler l'action de modification, résoudre les problèmes des machines, puis recommencer l'action de modification.

Une fois la modification terminée, vous pouvez rétablir les machines à leur état précédent. Sélectionnez le groupe de mise à disposition, puis sélectionnez **Annuler la modification du niveau fonctionnel** dans la barre d'actions.

### Gérer les groupes de mise à disposition Remote PC Access

Si une machine dans un catalogue de machines Remote PC Access n'est pas affectée, la machine est attribuée temporairement à un groupe de mise à disposition associé à ce catalogue de machines. Cette attribution temporaire permet à la machine d'être affectée à un utilisateur ultérieurement.

L'association du groupe de mise à disposition avec le catalogue de machines a une valeur de priorité. La priorité détermine le groupe de mise à disposition attribué de cette machine lorsque celui-ci s'enregistre auprès du système ou lorsqu'un utilisateur a besoin d'une machine. Plus la valeur est basse, plus la priorité est élevée. Si un catalogue de machine Remote PC Access possède plusieurs attributions de groupe de mise à disposition, le logiciel sélectionne la correspondance avec la priorité la plus élevée. Utilisez le SDK du PowerShell pour définir cette valeur de priorité.

Lors de leur création, les catalogues de machines Remote PC Access sont associés à un groupe de mise à disposition. Les comptes de machines ou unités d'organisation ajoutés au catalogue ultérieurement peuvent être ajoutés au groupe de mise à disposition. Cette association peut être désactivée ou activée.

Pour ajouter ou supprimer une association de catalogue de machines Remote PC Access avec un groupe de mise à disposition :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe Remote PC Access.
3. Dans la section **Détails**, cliquez sur l'onglet **Catalogues de machines**, puis sélectionnez un catalogue Remote PC Access.
4. Pour ajouter ou restaurer une association, cliquez sur **Ajouter des bureaux**. Pour supprimer une association, cliquez sur **Supprimer l'association**.

### Organiser les groupes de mise à disposition sous forme de dossiers

Vous pouvez créer des dossiers pour organiser les groupes de mise à disposition afin d'en faciliter l'accès.

**Rôles requis** Pour créer et gérer des dossiers de groupes de mise à disposition, vous devez disposer de l'un des rôles intégrés par défaut suivants : Administrateur cloud, Administrateur complet ou Administrateur du groupe de mise à disposition. Si nécessaire, vous pouvez personnaliser les rôles pour la création et la gestion des dossiers de groupe de mise à disposition. Pour plus d'informations, consultez la section Autorisations requises.

**Créer un dossier de groupes de mise à disposition** Avant de commencer, planifiez comment organiser vos groupes de mise à disposition. Tenez compte des considérations suivantes :

- Vous pouvez imbriquer des dossiers sur un maximum de cinq niveaux (à l'exception du dossier racine par défaut).
- Un dossier peut contenir des groupes de mise à disposition et des sous-dossiers.
- Tous les nœuds (tels que les nœuds **Catalogues de machines**, **Applications** et **Groupes de mise à disposition**) partagent une arborescence de dossiers dans le back-end. Pour éviter les conflits de nom avec d'autres nœuds lorsque vous renommez ou déplacez des dossiers, nous vous recommandons de donner des noms différents aux dossiers de premier niveau dans différents nœuds.

Pour créer un dossier de groupes de mise à disposition, procédez comme suit :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.

2. Dans la hiérarchie des dossiers, sélectionnez un dossier, puis sélectionnez **Créer un dossier** dans la barre **d'actions**.
3. Entrez un nom pour le nouveau dossier, puis cliquez sur **Terminé**.

> **Conseil :**
>
> Si vous créez un dossier dans le mauvais emplacement, vous pouvez le faire glisser vers l'emplacement approprié.

### Déplacer un groupe de mise à disposition

Vous pouvez déplacer un groupe de mise à disposition entre des dossiers. Les étapes détaillées sont les suivantes :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Affichez les groupes par dossier. Vous pouvez également activer **Afficher tout** au-dessus de la hiérarchie des dossiers pour afficher tous les groupes à la fois.
3. Cliquez avec le bouton droit sur un groupe, puis sélectionnez **Déplacer le groupe de mise à disposition**.
4. Sélectionnez le dossier vers lequel vous souhaitez déplacer le groupe, puis cliquez sur **Terminé**.

> **Conseil :**
>
> Vous pouvez faire glisser un groupe vers un dossier.

### Gérer les dossiers de groupes de mise à disposition

Vous pouvez supprimer, renommer et déplacer des dossiers de groupes de mise à disposition.

Notez que vous ne pouvez supprimer un dossier que si celui-ci et ses sous-dossiers ne contiennent pas de groupes de mise à disposition.

Pour gérer un dossier, procédez comme suit :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Dans la hiérarchie des dossiers, sélectionnez un dossier, puis sélectionnez une action dans la barre **d'actions** selon vos besoins :
   - Pour renommer le dossier, sélectionnez **Renommer le dossier**.
   - Pour supprimer le dossier, sélectionnez **Supprimer le dossier**.
   - Pour déplacer le dossier, sélectionnez **Déplacer le dossier**.
3. Suivez les instructions à l'écran pour effectuer les étapes restantes.

**Autorisations requises** Le tableau suivant répertorie les autorisations requises pour effectuer des actions sur les dossiers de groupes de mise à disposition.

| Action | Autorisations requises |
|---|---|
| Créer des dossiers de groupes de mise à disposition | Créer un dossier de groupes de mise à disposition |
| Supprimer des dossiers de groupes de mise à disposition | Supprimer un dossier de groupes de mise à disposition |
| Déplacer des dossiers de groupes de mise à disposition | Déplacer un dossier de groupes de mise à disposition |
| Renommer des dossiers de groupes de mise à disposition | Modifier un dossier de groupes de mise à disposition |
| Déplacer des groupes de mise à disposition vers des dossiers | Modifier un dossier de groupes de mise à disposition et modifier les propriétés d'un groupe de mise à disposition |

#### Gérer App Protection

Les informations suivantes complètent la protection des applications. Tenez compte des détails suivants :

- Vous devez disposer d'un droit App Protection valide. Pour acheter la fonctionnalité App Protection, contactez votre représentant commercial Citrix.
- App Protection nécessite une approbation XML. Pour activer l'approbation XML, accédez à **Paramètres > Activer l'approbation XML**.
- Remarques sur la protection contre la capture d'écran :
  - Sous Windows et macOS, seule la fenêtre du contenu protégé est vide. La fonctionnalité App Protection est active lorsqu'une fenêtre protégée n'est pas réduite.
  - Sur Linux, l'intégralité de la capture est vide. La fonctionnalité App Protection est active, qu'une fenêtre protégée soit réduite ou non.

Pour choisir une méthode de protection des applications pour un groupe de mise à disposition, procédez comme suit :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier** dans la barre d'actions.
3. Sur la page **Protection des applications**, vous pouvez activer la protection contre **l'enregistrement de frappe** et la **capture d'écran**.

## Utilisateurs

- Modifier les paramètres utilisateur
- Ajouter ou supprimer des utilisateurs

### Modifier les paramètres utilisateur dans un groupe de mise à disposition

Le nom de cette page apparaît sous **Paramètres utilisateur** ou **Paramètres de base**.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **Paramètres utilisateur** (ou **Paramètres de base**), modifiez les paramètres dans le tableau suivant.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

| Paramètre | Description |
|---|---|
| Description | Le texte que Citrix Workspace (ou StoreFront) utilise et que les utilisateurs voient. |
| Activer le groupe de mise à disposition | Indique si le groupe de mise à disposition est activé. |
| Fuseau horaire | Fuseau horaire dans lequel les machines de ce groupe de mise à disposition doivent résider. L'option répertorie les fuseaux horaires pris en charge par le site. **Remarque :** la modification du fuseau horaire d'un groupe de mise à disposition peut redémarrer les machines de ce groupe de mise à disposition. Pour éviter cela, veillez à modifier les paramètres de fuseau horaire en dehors des heures de production. |

| Paramètre | Description |
| --- | --- |
| Activer Secure ICA | Sécurise toutes les communications en provenance et à destination de machines dans le groupe de mise à disposition à l'aide de SecureICA, qui crypte le protocole ICA. Le niveau par défaut est 128 bits. Le niveau peut être modifié en utilisant le SDK. Citrix vous recommande d'utiliser des méthodes de cryptage supplémentaires telles que le cryptage TLS lorsque d'un passage au travers de réseaux publics. SecureICA n'effectue pas non plus de contrôle d'intégrité des données. |

#### Ajouter ou supprimer des utilisateurs dans un groupe de mise à disposition

Pour de plus amples informations sur les utilisateurs, consultez la section Utilisateurs.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **Utilisateurs** :
   - Pour ajouter des utilisateurs, cliquez sur **Ajouter**, puis spécifiez les utilisateurs que vous souhaitez ajouter.
   - Pour supprimer des utilisateurs, sélectionnez un ou plusieurs utilisateurs, puis cliquez sur **Supprimer**.
   - Cochez ou décochez la case pour autoriser l'accès aux utilisateurs non authentifiés.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

**Importer ou exporter des listes d'utilisateurs** Pour les groupes de mise à disposition contenant des machines avec OS mono-session physique, vous pouvez importer les informations de l'utilisateur à partir d'un fichier .csv après la création du groupe de mise à disposition. Vous pouvez également exporter des informations utilisateur vers un fichier .csv. Le fichier .csv peut contenir des données provenant d'une version antérieure du produit.

La première ligne du fichier CSV doit contenir deux en-têtes de colonne séparés par une virgule. Assurez-vous que le premier en-tête est `Machine Account` et que le second est `User Names`.

(Vous pouvez inclure des en-têtes supplémentaires mais ils ne sont pas pris en charge.) Les lignes suivantes du fichier contiennent des données séparées par des virgules. Les entrées `Machine Account` peuvent être un SID d'ordinateur, un nom de domaine complet, un domaine et des paires de nom d'ordinateur.

Pour importer ou exporter des informations sur l'utilisateur :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **Allocation de machine**, sélectionnez **Importer** la liste ou **Exporter** la liste, puis accédez à l'emplacement du fichier.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

## Machines

- Modifier les attributions de machines des utilisateurs
- Modifier le nombre maximal de machines par utilisateur
- Mettre à jour une machine
- Ajouter, modifier ou retirer une restriction de balise pour un bureau
- Supprimer une machine
- Restreindre l'accès aux machines
- Empêcher les utilisateurs de se connecter à une machine (mode de maintenance)
- Arrêter et redémarrer les machines
- Créer et gérer des programmes de redémarrage pour les machines
- Charger des machines gérées
- Alimenter des machines gérées

### Modifier les attributions de machines des utilisateurs d'un groupe de mise à disposition

Vous pouvez modifier les attributions des machines avec OS monosession configurées avec MCS. Vous ne pouvez pas modifier les attributions pour les machines avec OS multi-session ou les machines configurées avec Citrix Provisioning.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **Bureaux** ou **Règles d'attribution de bureau** (le titre de la page dépend du type de catalogue de machines que le groupe de mise à disposition utilise), spécifiez les nouveaux utilisateurs.

4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

#### Modifier le nombre maximal de machines par utilisateur dans un groupe de mise à disposition

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **Règles d'attribution de bureau**, définissez le nombre maximal de bureaux par utilisateur.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

#### Mettre à jour une machine dans un groupe de mise à disposition

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Afficher les machines** dans la barre d'actions.
3. Sélectionnez une machine, puis cliquez sur **Mettre à jour les machines** dans la barre d'actions.

Pour sélectionner une autre image, sélectionnez **Image**, puis sélectionnez un instantané.

Pour appliquer les modifications et notifier les utilisateurs de la machine, sélectionnez **Envoyer une notification aux utilisateurs**. Ensuite, spécifiez :

- Lors de la mise à jour de l'image principale : maintenant ou lors du prochain redémarrage.
- Le temps de distribution du redémarrage (le temps total pour commencer la mise à jour de toutes les machines du groupe)
- Indiquer si les utilisateurs sont informés du redémarrage
- Le message que les utilisateurs reçoivent

#### Ajouter, modifier ou retirer une restriction de balise pour un bureau

L'ajout, la modification et la suppression de restrictions de balise peut avoir des effets inattendus sur les bureaux qui sont pris en compte pour le démarrage. Consultez les informations et précautions dans la section Balises.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **Bureaux**, sélectionnez le bureau, puis cliquez sur **Modifier**.

4. Pour ajouter une restriction de balise, sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise.
5. Pour modifier ou supprimer une restriction de balise, vous pouvez soit :
    - Sélectionner une autre balise.
    - Supprimer la restriction de balise en désélectionnant **Restreindre les lancements aux machines dotées de balises**.
6. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

#### Supprimer une machine d'un groupe de mise à disposition

La suppression d'une machine la supprime d'un groupe de mise à disposition. Elle ne la supprime pas dans le catalogue de machines que le groupe de mise à disposition utilise. Par conséquent, cette machine est disponible pour l'attribution à un autre groupe de mise à disposition.

Les machines doivent être arrêtées avant de pouvoir être supprimées. Pour empêcher temporairement les utilisateurs de se connecter à une machine pendant que vous la supprimez, placez-la en mode maintenance avant de l'arrêter.

Les machines peuvent contenir des données personnelles, soyez donc prudent avant d'allouer la machine à un autre utilisateur. Il est recommandé de réimager la machine.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Afficher les machines** dans la barre d'actions.
3. Vérifiez que la machine est arrêtée.
4. Sélectionnez la machine, puis cliquez sur **Supprimer du groupe de mise à disposition** dans la barre d'actions.

Vous pouvez également supprimer une machine d'un groupe de mise à disposition au travers de la connexion utilisée par la machine.

#### Restreindre l'accès aux machines dans un groupe de mise à disposition

Toute modification que vous apportez pour restreindre l'accès aux machines dans un groupe de mise à disposition remplace les paramètres précédents, quelle que soit la méthode que vous utilisez. Vous pouvez :

- **Limiter l'accès des administrateurs à l'aide d'étendues d'administration déléguée :** créez et allouez une étendue qui permet aux administrateurs d'accéder à toutes les applications, et

une autre qui ne leur donne accès qu'à certaines applications. Pour de plus amples informations, veuillez consulter la section Administration déléguée.

- **Limiter l'accès des utilisateurs via des expressions de stratégie SmartAccess :**utilisez des expressions de stratégie pour filtrer les connexions utilisateur effectuées via Citrix Gateway.

  1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
  2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
  3. Dans la page **Stratégie d'accès**, sélectionnez **Connexions transitant par NetScaler Gateway**.
  4. Pour choisir un sous-ensemble de ces connexions, sélectionnez **Connexions remplissant l'un des critères de filtre suivants**. Ensuite, définissez le site Citrix Gateway, et ajoutez, modifiez ou supprimez les expressions de la stratégie SmartAccess pour les scénarios d'accès des utilisateurs autorisés. Pour plus d'informations, consultez la documentation relative à Citrix Gateway.
  5. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

- **Limiter l'accès des utilisateurs via des filtres d'exclusion :** utilisez des filtres d'exclusion sur les stratégies d'accès que vous définissez dans le kit de développement. Des stratégies d'accès sont appliquées aux groupes de mise à disposition pour affiner les connexions. Par exemple, vous pouvez restreindre l'accès aux machines à un sous-ensemble d'utilisateurs, vous pouvez spécifier les machines utilisateur autorisées. Les filtres d'exclusion affinent davantage les stratégies d'accès. Vous pouvez, par exemple, refuser l'accès à un sous-ensemble d'utilisateurs ou de machines pour des raisons de sécurité. Par défaut, les filtres d'exclusion sont désactivés.

  Par exemple, un laboratoire d'enseignement sur un sous-réseau de réseau d'entreprise qui empêche l'accès de ce laboratoire à un groupe de mise à disposition particulier. Peu importe qui utilise les machines dans le laboratoire, utilisez la commande : `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`.

  Utilisez également un astérisque (*) en tant que caractère générique afin de faire correspondre toutes les balises qui commencent par la même expression de stratégie. À titre d'exemple, si vous avez ajouté la balise `VPDesktops_Direct` à une machine et `VPDesktops_Test` à une autre machine, la définition de la balise dans le script `Set-BrokerAccessPolicy` sur `VPDesktops_*` applique le filtre aux deux machines.

  Si vous êtes connecté à l'aide d'un navigateur Web ou avec la fonctionnalité d'expérience de l'application Citrix Workspace activée dans le magasin, vous ne pouvez pas utiliser un filtre d'exclusion du nom de client.

### Empêcher les utilisateurs de se connecter à une machine (mode de maintenance) dans un groupe de mise à disposition

Lorsque vous devez arrêter temporairement les nouvelles connexions aux machines, vous pouvez activer le mode de maintenance pour une ou toutes les machines dans un groupe de mise à disposition. Vous pouvez effectuer cette opération avant d'appliquer des correctifs ou à l'aide d'outils de gestion.

- Lorsqu'une machine avec OS multi-session se trouve en mode de maintenance, les utilisateurs peuvent se connecter à des sessions existantes mais ne peuvent pas démarrer de nouvelles sessions.
- Lorsqu'une machine avec OS monosession (ou un ordinateur utilisant Remote PC Access) est en mode de maintenance, les utilisateurs ne peuvent pas se connecter ou se reconnecter. Les connexions courantes restent connectées jusqu'à ce qu'elles se déconnectent ou ferment leur session.

Pour activer ou désactiver le mode de maintenance :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe.
3. Pour activer le mode de maintenance pour toutes les machines dans le groupe de mise à disposition, cliquez sur **Activer le mode de maintenance** dans la barre d'actions.

   Pour activer le mode de maintenance pour une machine, cliquez sur **Afficher les machines** dans la barre d'actions. Sélectionnez une machine, puis cliquez sur **Activer le mode de maintenance** dans la barre d'actions.
4. Pour désactiver le mode de maintenance pour une ou toutes les machines dans un groupe de mise à disposition, suivez les instructions précédentes, cliquez sur **Désactiver le mode de maintenance** dans la barre d'actions.

Les paramètres Windows RDC (Remote Desktop Connection) affectent également le fait qu'une machine avec OS multi-session est en mode de maintenance. Le mode de maintenance est activé dans l'un des cas suivants :

- Le mode de maintenance est activé, comme décrit précédemment.
- RDC est défini sur **Ne pas autoriser les connexions à cet ordinateur**.
- RDC n'est pas défini sur **Ne pas autoriser les connexions à cet ordinateur**. Le paramètre de **mode d'ouverture de session utilisateur de la configuration à distance d'hôte** est **Autoriser les reconnexions mais refuser les nouvelles ouvertures de session** ou **Autoriser les reconnexions mais refuser les nouvelles ouvertures de session jusqu'au redémarrage du serveur**.

Vous pouvez également activer ou désactiver le mode de maintenance pour :

- Une connexion, ce qui affecte les machines qui utilisent cette connexion.
- Un catalogue de machines, ce qui affecte les machines de ce catalogue.

### Arrêter et redémarrer les machines d'un groupe de mise à disposition

Cette procédure n'est pas prise en charge par les machines Remote PC Access.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Afficher les machines** dans la barre d'actions.
3. Sélectionnez la machine et cliquez sur l'une des options suivantes dans la barre d'actions :

    - **Forcer l'arrêt :** force l'arrêt de la machine et actualise la liste des machines.
    - **Redémarrer :** requiert la fermeture du système d'exploitation de la machine, puis redémarrage de la machine. Si le système d'exploitation ne peut pas s'y conformer, la machine reste dans son état actuel.
    - **Forcer le redémarrage :** force l'arrêt du système d'exploitation, puis redémarre la machine.
    - **Suspendre :** pause la machine sans la fermer et actualise la liste de machines.
    - **Arrêter :** requiert la fermeture du système d'exploitation.

Pour les actions qui ne sont pas forcées, si la machine ne se ferme pas dans les 10 minutes, elle est mise hors tension. Si Windows tente d'installer des mises à jour durant la fermeture, il y a un risque que la machine soit mise hors tension avant la fin des mises à jour.

Citrix vous recommande d'empêcher les utilisateurs des machines avec OS mono-session de sélectionner **Arrêter** dans une session. Consultez la documentation des stratégies Microsoft pour plus de détails.

Vous pouvez également arrêter et redémarrer des machines sur une connexion.

### Créer et gérer des programmes de redémarrage pour les machines d'un groupe de mise à disposition

> **Remarque :**
>
> - Lorsqu'un programme de redémarrage est appliqué à un groupe de mise à disposition avec Autoscale activé, ses machines sont juste mises hors tension et le restent jusqu'à ce que Autoscale les mette sous tension.
> - Lorsque des programmes de redémarrage sont appliqués à des machines mono-session aléatoires, ces machines sont mises hors tension plutôt que redémarrées, afin de réduire

> les coûts. Nous vous recommandons d'utiliser Autoscale pour mettre les machines sous tension.
> • La modification du fuseau horaire d'un groupe de mise à disposition peut redémarrer les machines de ce groupe de mise à disposition. Pour éviter cela, veillez à modifier les paramètres de fuseau horaire en dehors des heures de production.

Un programme de redémarrage spécifie quand redémarrer périodiquement toutes les machines d'un groupe de mise à disposition. Vous pouvez créer un ou plusieurs programmes pour un groupe de mise à disposition. Un programme peut affecter :

- Toutes les machines du groupe.
- Une ou plusieurs machines du groupe (mais pas toutes). Les machines sont identifiées par une balise que vous appliquez à la machine. Cela s'appelle une restriction de balise, car la balise restreint une action aux seuls éléments qui en ont.

Par exemple, supposons que toutes vos machines appartiennent à un même groupe de mise à disposition. Vous voulez que chaque machine soit redémarrée une fois par semaine et que les machines utilisées par l'équipe de comptabilité soient redémarrées quotidiennement. Pour ce faire, configurez un programme pour toutes les machines et un autre programme uniquement pour les machines de la comptabilité.

Un programme comprend le jour et l'heure de début du redémarrage, ainsi que la durée.

Vous pouvez activer ou désactiver un programme. La désactivation d'un programme peut être utile lors de tests, à des intervalles particuliers ou lors de la préparation de programmes avant leur activation.

Vous ne pouvez pas utiliser de programmes pour la mise sous tension ou l'arrêt automatique à partir de la console de gestion, uniquement pour redémarrer.

**Chevauchement de programmes** Plusieurs programmes peuvent se chevaucher. Dans l'exemple ci-dessus, les deux programmes affectent les machines utilisées par la comptabilité. Ces machines pourraient être redémarrées deux fois dimanche. Le code de programmation est conçu pour éviter le redémarrage d'une même machine plus souvent que nécessaire, mais cela ne peut pas être garanti.

- Si l'heure de début et la durée des programmes coïncident précisément, il est plus probable que les machines seront redémarrées une seule fois.
- Plus l'heure de début et la durée diffèrent, plus il est probable que plusieurs redémarrages seront effectués.
- Le nombre de machines affectées par un programme peut aussi influencer les risques de chevauchement. Dans cet exemple, le programme hebdomadaire qui affecte toutes les machines peut initier des redémarrages plus rapidement que le programme quotidien des machines de la comptabilité, en fonction de la durée spécifiée pour chacun d'eux.

Pour un aperçu détaillé des programmes de redémarrage, voir Programmes de redémarrage.

#### Afficher les programmes de redémarrage

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sélectionnez la page **Programme de redémarrage**.

La page **Programme de redémarrage** contient les informations suivantes pour chaque programme configuré :

- Nom du calendrier.
- Restriction de balise utilisée, le cas échéant.
- Fréquence à laquelle la machine redémarre.
- Si les utilisateurs de la machine reçoivent une notification.
- Si le programme est activé.

**Ajouter (appliquer) des balises** Lorsque vous configurez un programme de redémarrage qui utilise une restriction de balise, assurez-vous que cette balise a été ajoutée aux machines que le programme affecte. Dans l'exemple ci-dessus, une balise serait appliquée à chacune des machines utilisées par l'équipe de comptabilité. Pour plus de détails, consultez la section Balises.

Bien que vous puissiez appliquer plusieurs balises à une machine, un programme de redémarrage ne peut spécifier qu'une seule balise.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez le groupe contenant les machines contrôlées par le programme.
3. Cliquez sur **Afficher les machines**, puis sélectionnez les machines auxquelles vous souhaitez ajouter une balise.
4. Cliquez sur **Gérer les balises** dans la barre d'actions.
5. Si la balise existe, activez la case à cocher en regard du nom de la balise. Si la balise n'existe pas, cliquez sur **Créer**, puis spécifiez le nom de la balise. Une fois que la balise est créée, activez la case à cocher en regard du nom de la balise créée.
6. Cliquez sur **Enregistrer** dans la boîte de dialogue **Gérer les balises**.

#### Créer un programme de redémarrage

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **Programme de redémarrage**, cliquez sur **Ajouter**.
4. Sur la page **Ajouter calendrier de redémarrage** :

- Pour activer le programme, sélectionnez **Oui**. Pour désactiver le programme, sélectionnez **Non**.
- Tapez un nom de programme et une description.
- Pour **Restreindre à la balise**, appliquez une restriction de balise.
- Pour **Inclure les machines en mode de maintenance**, indiquez si vous souhaitez inclure les machines qui sont en mode de maintenance dans ce programme. Pour utiliser PowerShell à la place, consultez Redémarrages planifiés pour les machines en mode de maintenance.
- Pour **Fréquence de redémarrage**, sélectionnez la fréquence du redémarrage : quotidienne, hebdomadaire, mensuelle, ponctuelle. Si vous sélectionnez **Hebdomadaire** ou **Mensuel**, vous pouvez spécifier un ou plusieurs jours spécifiques.
- Pour **Se répète chaque**, spécifiez la fréquence d'exécution du programme.
- Pour **Date de début**, spécifiez une date de début pour la première occurrence du programme.
- Pour **Commencer le redémarrage à**, spécifiez l'heure de la journée à laquelle le redémarrage commence au format d'horloge 24 heures.
- Pour **Durée du redémarrage** :
  - Si vous ne souhaitez pas utiliser le redémarrage naturel, sélectionnez **Redémarrer toutes les machines en même temps** ou **Redémarrer toutes les machines dans un délai donné**.
  - Si vous souhaitez utiliser le redémarrage naturel, sélectionnez **Redémarrer toutes les machines après le vidage des sessions**.

    Lorsque vous démarrez un programme de redémarrage configuré pour utiliser le redémarrage naturel :

    * Toutes les machines inactives appartenant au groupe de mise à disposition sont redémarrées immédiatement
    * Chaque machine appartenant à un groupe de mise à disposition ayant une ou plusieurs sessions actives est redémarrée lorsque toutes les sessions sont déconnectées.

    > **Remarque :**
    >
    > Vous pouvez utiliser cette option pour les machines dont l'alimentation est gérée et également pour les machines dont l'alimentation n'est pas gérée.

- Dans **Notifier les utilisateurs**, indiquez si un message de notification doit s'afficher sur les machines applicables avant qu'un redémarrage commence. Par défaut, aucun message n'apparaît.

- Si vous choisissez d'afficher un message 15 minutes avant que le redémarrage commence, vous pouvez choisir (dans **Fréquence de notification**) de répéter le message toutes les cinq minutes après le premier message. Par défaut, le message ne se répète pas.
- Entrez le titre et le texte de la notification. Il n'y a pas de texte par défaut.

  Si vous souhaitez que le message comprenne un compte à rebours avant le redémarrage, incluez la variable **%m%**. Si vous avez choisi de redémarrer toutes les machines en même temps, le message s'affiche sur chaque machine à l'heure appropriée avant que le redémarrage ne commence.

5. Cliquez sur **Terminé** pour appliquer les modifications et fermer la fenêtre **Ajouter calendrier de redémarrage**.
6. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

**Redémarrer après vidage** Une autre valeur de durée de redémarrage est disponible lors de l'utilisation de PowerShell pour créer ou mettre à jour un programme de redémarrage de machine (`New-BrokerRebootSchedulev2` ou `Set-BrokerRebootSchedulev2`).

Lorsque vous activez la fonction de redémarrage après vidage avec le paramètre `-UseNaturalReboot <Boolean>`, toutes les machines sont redémarrées après avoir vidé toutes les sessions. Lorsque l'heure de redémarrage est atteinte, les machines sont mises en état de vidage et redémarrées lorsque toutes les sessions sont déconnectées.

Cette fonctionnalité est prise en charge pour les groupes de mise à disposition contenant des machines mono-session ou multi-session. Vous pouvez utiliser cette option pour les machines dont l'alimentation est gérée et également pour les machines dont l'alimentation n'est pas gérée.

Dans un environnement local, cette fonction n'est prise en charge que lors de l'utilisation de PowerShell. Cette fonction n'est pas disponible dans Web Studio.

#### Modifier, supprimer, activer ou désactiver un programme de redémarrage

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **Programme de redémarrage**, cochez la case correspondant à un programme.
   - Pour modifier un programme, cliquez sur **Modifier**. Mettez à jour la configuration du programme en utilisant les instructions sous Créer un programme de redémarrage.
   - Pour activer ou désactiver un programme, cliquez sur **Modifier**. Sélectionnez ou désélectionnez la case **Activer calendrier de redémarrage**.

- Pour supprimer un programme, cliquez sur **Supprimer**. Confirmez la suppression. La suppression d'un programme n'affecte pas les balises appliquées aux machines dans les machines affectées.

#### Redémarrages programmés retardés en raison d'une panne de base de données

> **Remarque :**
>
> Cette fonctionnalité est disponible uniquement dans PowerShell.

Si une panne de base de données de site se produit avant le début d'un redémarrage programmé pour les machines (VDA) d'un groupe de mise à disposition, les redémarrages commencent à la fin de la panne. Cela peut donner des résultats inattendus.

Par exemple, supposons que vous ayez planifié les redémarrages d'un groupe de mise à disposition pendant les heures hors production (à partir de 3h00). Une panne de base de données de site se produit une heure avant le début d'un redémarrage programmé (2h00). La panne dure six heures (jusqu'à 8h00). Le programme de redémarrage commence lorsque la connexion entre le Delivery Controller et la base de données du site est restaurée. Le VDA redémarre désormais cinq heures après son programme d'origine, ce qui entraîne le redémarrage des VDA pendant les heures de production.

Pour éviter cette situation, vous pouvez utiliser le paramètre `MaxOvertimeStartMins` pour les applets de commande `New-BrokerRebootScheduleV2` et `Set-BrokerRebootScheduleV2`. La valeur spécifie le nombre maximal de minutes au-delà de l'heure de début planifiée pendant lesquelles un programme de redémarrage peut commencer.

- Si la connexion à la base de données est restaurée dans ce délai (heure planifiée + `MaxOvertimeStartMins`), le VDA redémarre.
- Si la connexion à la base de données n'est pas restaurée dans ce délai, le VDA ne redémarre pas.
- Si ce paramètre est omis ou est réglé sur zéro, le redémarrage programmé commence lorsque la connexion à la base de données est restaurée, quelle que soit la durée de la panne.

Pour plus d'informations, consultez l'aide de l'applet de commande. Cette fonctionnalité est disponible uniquement dans PowerShell. Vous ne pouvez pas définir cette valeur lors de la configuration d'un programme de redémarrage dans Web Studio.

#### Redémarrages planifiés des machines en mode de maintenance

> **Remarque :**
>
> Cette fonctionnalité est disponible uniquement dans PowerShell. L'option `IgnoreMaintenanceMode` est prise en charge par Citrix Virtual Apps and Desktops 7 2006 et versions ultérieures.

Pour indiquer si une planification de redémarrage affecte les machines en mode de maintenance, utilisez l'option `IgnoreMaintenanceMode` avec les applets de commande `BrokerRebootScheduleV2` .

Par exemple, l'applet de commande suivante crée une planification qui redémarre les machines en mode de maintenance (en plus des machines qui ne sont pas en mode de maintenance).

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup
> -IgnoreMaintenanceMode $true
```

L'applet de commande suivante modifie une planification de redémarrage existante.

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode
$true
```

Pour plus d'informations, consultez l'aide de l'applet de commande. Cette fonctionnalité est disponible uniquement dans PowerShell.

#### Charger des machines gérées dans les groupes de mise à disposition

Vous pouvez gérer la charge des machines avec OS multi-session uniquement.

La gestion de la charge mesure la charge du serveur et détermine le serveur à sélectionner dans les conditions actuelles d'environnement. Cette sélection est basée sur :

- **État du mode de maintenance du serveur :** une machine avec OS multi-session est considérée pour l'équilibrage de charge uniquement lorsque le mode de maintenance est désactivé.
- **Indice de charge du serveur :** détermine la probabilité qu'un serveur qui met à disposition des machines avec OS multi-session a de recevoir des connexions. L'index est une combinaison de calculateurs de charge : le nombre de sessions et les paramètres des mesures de performances tels que l'UC, le disque et l'utilisation de la mémoire. Les calculateurs de charge sont spécifiés dans les paramètres de la stratégie de gestion de la charge.

  Un serveur d'index de charge de 10 000 indique que le serveur est complètement chargé. Si aucun des autres serveurs n'est disponible, il se peut que les utilisateurs reçoivent un message indiquant que le bureau ou l'application est indisponible lorsqu'ils lancent une session.

  Vous pouvez surveiller l'index de charge dans Director (Surveiller), la recherche Web Studio (Gérer) et le kit de développement.

  Dans les écrans de la console, pour afficher la colonne **Index de charge du serveur** (qui est masquée par défaut), sélectionnez une machine, cliquez avec le bouton droit sur un en-tête de colonne, puis sélectionnez **Sélectionner colonne**. Dans la catégorie **Machine**, sélectionnez **Index de charge**.

Dans le kit de développement, utilisez l'applet de commande `Get-BrokerMachine`. Pour de plus amples informations, consultez l'article CTX202150.

- **Paramètre de stratégie de tolérance d'ouvertures de session simultanées :** le nombre maximal de demandes simultanées pour ouvrir une session sur le serveur. (Ce paramètre est équivalent à l'optimisation de la charge dans les versions 6.x de XenApp.)

  Lorsque le nombre de demandes d'ouvertures de session que tous les serveurs reçoivent est égal ou supérieur au paramètre Tolérance d'ouvertures de session simultanées, la prochaine demande d'ouverture de session est attribuée au serveur avec le nombre d'ouvertures de session en attente le plus faible. Si plusieurs serveurs répondent à ces critères, le serveur ayant l'index de charge le plus faible est sélectionné.

#### Alimenter des machines gérées dans un groupe de mise à disposition

Vous pouvez gérer l'alimentation des machines avec OS mono-session virtuelles uniquement, pas celle des machines physiques (y compris les machines Remote PC Access). Les machines d'OS mono-session avec capacités GPU ne peuvent pas être suspendues, par conséquent les opérations de mise hors tension échouent. Pour les machines avec OS multi-session, vous pouvez créer un programme de redémarrage.

Dans des groupes de mise à disposition contenant des machines regroupées, les machines avec OS mono-session virtuelles peuvent être dans l'un des états suivants :

- Allouées de manière aléatoire et en cours d'utilisation.
- Non allouées et non connectées

Dans des groupes de mise à disposition contenant des machines statiques, les machines avec OS mono-session virtuelles peuvent être :

- allouées à titre permanent et en cours d'utilisation ;
- Allouées à titre permanent et non connectées (mais prêtes)
- Non allouées et non connectées

Lors d'une utilisation normale, les groupes de mise à disposition statiques contiennent toujours des machines allouées et non allouées à titre permanent. Initialement, aucune machine n'est allouée, sauf celles manuellement allouées lors de la création du groupe de mise à disposition. Lorsque les utilisateurs se connectent, les machines sont allouées à titre permanent. Vous pouvez gérer l'alimentation des machines non allouées complètement dans les groupes de mise à disposition, mais uniquement partiellement gérer les machines allouées à titre permanent.

- **Regroupements et tampons :** pour les groupes de mise à disposition regroupés et les groupes de mise à disposition statiques avec des machines non allouées, un regroupement (dans ce cas) est un ensemble de machines non allouées ou allouées temporairement qui sont conservées

à l'état sous tension, prêtes pour la connexion des utilisateurs. Un utilisateur reçoit une machine immédiatement après l'ouverture de session. La taille du regroupement (le nombre de machines conservées sous tension) est configurable par heure de la journée. Pour les groupes de mise à disposition statiques, utilisez le kit de développement pour configurer le regroupement.

Un tampon en veille est un ensemble de machines non allouées qui sont activées lorsque le nombre de machines du regroupement tombe en dessous d'un seuil. Ce seuil est un pourcentage de la taille du groupe de mise à disposition. Pour les grands groupes de mise à disposition, un nombre important de machines peut être activé lorsque le seuil est dépassé. Planifiez donc soigneusement les tailles des groupes de mise à disposition ou utilisez le SDK pour ajuster la taille de la mémoire tampon par défaut.

- **Horloges d'état d'alimentation :** vous pouvez utiliser les horloges d'état d'alimentation pour suspendre des machines une fois que les utilisateurs se sont déconnectés depuis un laps de temps spécifié. Par exemple, les machines sont suspendues automatiquement en dehors des heures ouvrables si les utilisateurs se sont déconnectés depuis au moins 10 minutes.

  Vous pouvez configurer des horloges pour les jours de la semaine et les week-ends et, pour les heures de pointe et les intervalles calmes.

- **Gestion partielle de l'alimentation des machines allouées à titre permanent :** pour des machines allouées à titre permanent, vous pouvez définir des horloges d'état d'alimentation, mais pas des regroupements ou des mémoires tampons. Les machines sont activées au début de chaque période de pointe et désactivées au début de chaque période creuse. Vous n'avez pas de contrôle précis comme avec les machines non allouées sur le nombre de machines qui deviennent disponibles pour compenser les machines qui sont utilisées.

#### Gérer la consommation des machines virtuelles avec OS mono-session

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier le groupe de mise à disposition** dans la barre d'actions.
3. Sur la page **Gestion de l'alimentation**, sélectionnez **Jours ouvrés** dans **Gestion de l'alimentation des machines**. Par défaut, les jours de la semaine vont du lundi au vendredi.
4. Pour les groupes de mise à disposition aléatoires, dans **Machines à allumer**, cliquez sur **Modifier** et spécifiez la taille du regroupement durant les jours ouvrés. Ensuite, sélectionnez le nombre de machines à mettre sous tension.
5. Dans **Heures de pointe**, définissez les heures de pointe et les heures creuses de chaque jour.
6. Définissez les horloges d'état d'alimentation pour les heures de pointe et les heures creuses des jours de la semaine : Dans **Durant les heures de pointe > Après déconnexion**, indiquez le délai (en minutes) avant la suspension des machines déconnectées dans le groupe de mise à

disposition, puis sélectionnez **Suspendre**. Dans **Durant les heures creuses > Après déconnexion**, indiquez le délai avant la suspension des machines déconnectées dans le groupe de mise à disposition, puis sélectionnez **Arrêter**. Cette horloge n'est pas disponible pour les groupes de mise à disposition avec des machines aléatoires.

7. Sélectionnez **Week-end** dans la liste **Gérer l'alimentation des machines**, puis configurez les heures de pointe et les horloges d'état d'alimentation pour les week-ends.
8. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

Utilisez le SDK pour :

- Arrêter, plutôt que suspendre, les machines en réponse aux horloges d'état d'alimentation ou si vous voulez que les horloges soient basées sur les fermetures de session et non sur les déconnexions.
- Modifier les définitions par défaut des jours de la semaine et du week-end.
- Désactivez la gestion de l'alimentation. Voir CTX217289.

**Gestion de l'alimentation des machines VDI qui passent à une période différente avec des sessions déconnectées**

> **Important :**
>
> Cette amélioration s'applique uniquement aux machines VDI avec sessions déconnectées. Elle ne s'applique pas aux machines VDI avec sessions fermées.

Dans les versions antérieures, une machine VDI en transition vers une période où une action (action de déconnexion = « **Suspend** » ou « **Shutdown** ») devait rester sous tension. Ce scénario se produisait si la machine était déconnectée pendant une période (heures de pointe ou heures creuses) pendant laquelle aucune action (action de déconnexion = « **Nothing** ») n'était requise.

À partir de Citrix Virtual Apps and Desktops 7 1909, la machine est suspendue ou mise hors tension lorsque le temps de déconnexion spécifié est écoulé, en fonction de l'action de déconnexion configurée pour la période suivante.

Par exemple, vous configurez les stratégies d'alimentation suivantes pour un groupe de mise à disposition VDI :

- Définissez `PeakDisconnectAction` sur « Nothing »
- Définissez `OffPeakDisconnectAction` sur « Shutdown »
- `OffPeakDisconnectTimeout` défini sur « 10 »

Pour plus d'informations sur l'action de déconnexion dans la stratégie d'alimentation, reportez-vous aux sections https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/a

bout_Broker_PowerManagement/#power-policy et https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Dans les versions antérieures, une machine VDI avec une session déconnectée pendant les heures de pointe restait sous tension lorsqu'elle passait des heures de pointe aux heures creuses. À partir de Citrix Virtual Apps and Desktops 7 1909, les actions de stratégie `OffPeakDisconnectAction` et `OffPeakDisconnectTimeout`sont appliquées à la machine VDI lors de la transition. Par conséquent, la machine est mise hors tension 10 minutes après sa transition vers les heures creuses.

Si vous souhaitez revenir au comportement précédent (autrement dit, n'effectuer aucune action sur les machines qui passent d'heures de pointe à heures creuses ou inversement avec des sessions déconnectées), effectuez l'une des opérations suivantes :

- Définissez la valeur de Registre `LegacyPeakTransitionDisconnectedBehaviour` sur `1`, l'équivalent de *true*, qui active le comportement précédent. Par défaut, la valeur est `0` ou *false*, qui déclenche la déconnexion des actions de stratégie d'alimentation lors de la transition.
  - Chemin : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer`
  - Nom :`LegacyPeakTransitionDisconnectedBehaviour`
  - Type : `REG_DWORD`
  - Données : `0x00000001 (1)`
- Configurez le paramètre à l'aide de la commande PowerShell `Set-BrokerServiceConfigurationDa` . Par exemple :
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Une machine doit répondre aux critères suivants avant que des actions de stratégie d'alimentation puissent lui être appliquées lors de la transition :

- A une session déconnectée.
- N'a aucune action d'alimentation en attente.
- Appartient à un groupe de mise à disposition VDI (mono-session) qui effectue une transition vers une période différente.
- A une session qui se déconnecte pendant une certaine période (heures de pointe ou heures creuses) et effectue une transition vers une période où une action d'alimentation est affectée.

#### Modifier le pourcentage de VDA dans un état alimenté pour les catalogues

1. Réglez les heures de pointe pour le groupe de mise à disposition dans la section **Gestion de l'alimentation** du groupe de mise à disposition.
2. Notez le nom du groupe de bureaux.

3. Avec des privilèges d'administrateur, démarrez PowerShell et exécutez les commandes suivantes. Remplacez "Nom du groupe de bureaux"par le nom de votre groupe de bureaux pour lequel le pourcentage de VDA en cours d'exécution a changé.

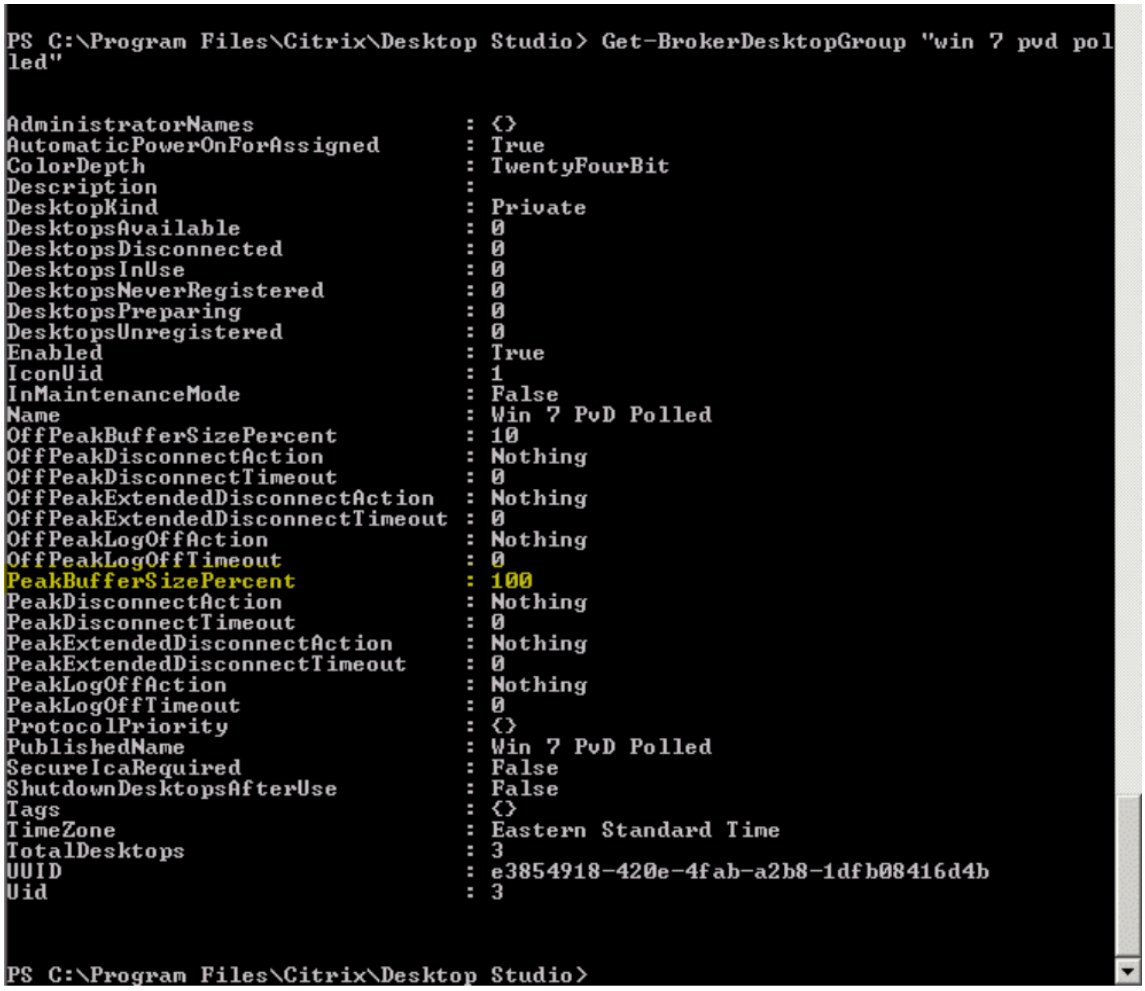
   ```
   asnp Citrix*

   # Set-BrokerDesktopGroup "Desktop Group Name"-PeakBufferSizePercent
    100
   ```

   Une valeur de 100 signifie que 100 % des VDA sont prêts.

4. Vérifiez la solution en exécutant :

   ```
   #Get-BrokerDesktopGroup "Desktop Group Name"
   ```




Cela peut prendre jusqu'à une heure pour que les modifications prennent effet.

Pour arrêter les VDA après la déconnexion de l'utilisateur, entrez :

```
# Set-BrokerDesktopGroup "Desktop Group Name"-ShutDownDesktopsAfterUse
 $True
```

Pour redémarrer les VDA aux heures de pointe, afin qu'ils soient prêts pour les utilisateurs après leur déconnexion, entrez :

```
# Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDurin
 $True
```

## Sessions

- Fermer ou déconnecter la session, ou envoyer un message aux utilisateurs
- Configurer le pré-lancement de session et la persistance de session
- Contrôler la reconnexion de session en cas de déconnexion d'une machine en mode de maintenance
- Configurer l'itinérance de session

### Fermer ou déconnecter une session

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe de mise à disposition, puis sélectionnez **Afficher les machines** dans la barre d'actions.
3. Dans le volet central, sélectionnez la machine, sélectionnez **Afficher les sessions** dans la barre d'actions, puis sélectionnez une session.
    - Sinon, dans le volet central, sélectionnez l'onglet **Session**, puis sélectionnez une session.
4. Pour fermer une session, sélectionnez **Fermer la session** dans la barre d'actions. La session se ferme et l'utilisateur est déconnecté. La machine devient disponible auprès des autres utilisateurs, à moins qu'elle ne soit attribuée à un utilisateur spécifique.
5. Pour déconnecter une session, sélectionnez **Déconnecter** dans la barre d'actions. Les applications continuent à être exécutées dans la session et la machine reste attribuée à cet utilisateur. L'utilisateur peut se reconnecter à la même machine.

Vous pouvez configurer les horloges d'état d'alimentation pour les machines avec OS mono-session pour gérer automatiquement les sessions non utilisées. Consultez la section Alimenter des machines gérées pour plus de détails.

### Envoyer un message à un groupe de mise à disposition

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe de mise à disposition, puis sélectionnez **Afficher les machines** dans la barre d'actions.
3. Dans le volet central, sélectionnez une machine à laquelle vous souhaitez envoyer un message.

4. Dans la barre d'actions, sélectionnez **Afficher les sessions**.
5. Dans le volet central, sélectionnez toutes les sessions, puis sélectionnez **Envoyer un message** dans la barre d'actions.
6. Tapez votre message et cliquez sur **OK**. Vous pouvez spécifier le niveau de gravité si nécessaire. Les options incluent **Critique**, **Question**, **Avertissement**et **Informations**.

Vous pouvez également envoyer un message à l'aide de Citrix Director. Pour plus d'informations, consultez Envoyer des messages aux utilisateurs.

### Configurer le pré-lancement de session et la persistance de session dans un groupe de mise à disposition

Ces fonctionnalités sont prises en charge sur les machines avec OS multi-session uniquement.

Les fonctionnalités de pré-lancement de session et de persistance de session aident les utilisateurs spécifiés à accéder aux applications rapidement, en démarrant des sessions avant qu'elles ne sont demandées (pré-lancement de session) et conserver les sessions d'applications actives après qu'un utilisateur ferme toutes les applications (persistance de session).

Par défaut, le pré-lancement de session et la persistance de session ne sont pas utilisés. Une session démarre (se lance) lorsqu'un utilisateur démarre une application et reste active jusqu'à ce que la dernière application ouverte dans la session se ferme.

Considérations :

- Le groupe de mise à disposition doit prendre en charge les applications, et les machines doivent être exécutées sur un VDA pour OS multi-session, version minimale 7.6.
- Ces fonctionnalités sont uniquement prises en charge lors de l'utilisation de l'application Citrix Workspace pour Windows, et requièrent également une configuration de l'application Citrix Workspace supplémentaire. Pour obtenir des instructions, recherchez pré-lancement de session dans la documentation produit pour votre version de l'application Citrix Workspace pour Windows.
- L'application Citrix Workspace pour HTML5 n'est pas prise en charge.
- Lorsque vous utilisez le pré-lancement de session, si une machine utilisateur est placée en mode « suspendue » ou « veille prolongée », le pré-lancement ne fonctionne pas (quels que soient les paramètres de pré-lancement de session). Les utilisateurs peuvent verrouiller leurs machines/sessions. Cependant, si un utilisateur ferme sa session sur l'application Citrix Workspace, la session est fermée et le pré-lancement ne s'applique plus.
- Lorsque vous utilisez le pré-lancement de session, les machines clientes physiques ne peuvent pas utiliser les fonctions de gestion de l'alimentation en veille ou veille prolongée. Les utilisateurs de la machine cliente peuvent verrouiller leurs sessions, mais ne doivent pas les fermer.

- Les sessions pré-lancées et persistantes utilisent une licence simultanée, mais uniquement lorsque vous êtes connecté. Si vous utilisez une licence d'utilisateur/de périphérique, la licence dure 90 jours. Toute session pré-lancée et persistante non utilisée se déconnecte après 15 minutes par défaut. Cette valeur peut être configurée dans PowerShell (applet de commande `New`/`Set-BrokerSessionPreLaunch`).
- Une planification et un contrôle attentif des modèles d'activité de vos utilisateurs sont essentiels pour personnaliser ces fonctionnalités afin qu'elles se complètent l'une avec l'autre. Une configuration optimale équilibre les avantages d'une disponibilité d'application antérieure pour les utilisateurs par rapport au coût de licences en cours d'utilisation et de ressources allouées.
- Vous pouvez également configurer le pré-lancement de session pour une heure de la journée planifiée dans l'application Citrix Workspace.

**Durée pendant laquelle les sessions pré-lancées et persistantes restent actives** Il existe plusieurs façons de spécifier la durée pendant laquelle une session non utilisée reste active si l'utilisateur ne démarre pas une application : un délai configuré et des seuils de charge du serveur. Vous pouvez tous les configurer. L'événement qui se produit en premier provoque la fin de la session non utilisée.

- **Expiration du délai :** une expiration de délai configurée spécifie le nombre de minutes, heures ou jours pendant lesquels une session pré-lancée inutilisée ou une session de persistance restent actives. Si vous configurez un délai d'expiration trop court, les sessions pré-lancées se terminent avant de permettre aux utilisateurs de bénéficier d'un accès aux applications plus rapide. Si vous configurez un délai d'expiration trop long, les connexions utilisateur entrantes peuvent être refusées car le serveur ne dispose pas de suffisamment de ressources.

  Vous pouvez activer ce délai à partir du SDK uniquement (applet de commande `New`/`Set-BrokerSessionPreLaunch`), et non depuis la console de gestion. Si vous désactivez l'expiration du délai, elle n'apparaît pas dans l'affichage de la console pour ce groupe de mise à disposition ou dans l'Assistant **Modifier le groupe de mise à disposition**.

- **Seuils :** les sessions pré-lancées se terminant automatiquement et les sessions de persistance basées sur la charge d'un serveur assurent que les sessions restent ouvertes le plus longtemps possible, en supposant que les ressources serveur sont disponibles. Les sessions pré-lancées et les sessions de persistance inutilisées ne provoquent pas de refus de connexions, car elles sont arrêtées automatiquement lorsque les ressources sont nécessaires pour de nouvelles sessions utilisateur.

  Vous pouvez configurer deux seuils : la charge de pourcentage moyenne de tous les serveurs dans le groupe de mise à disposition et le pourcentage maximal de charge d'un serveur dans le groupe. Lorsqu'un seuil est dépassé, les sessions qui se sont trouvées dans un état de pré-lancement ou de persistance pour la période la plus longue est terminée. Les sessions sont

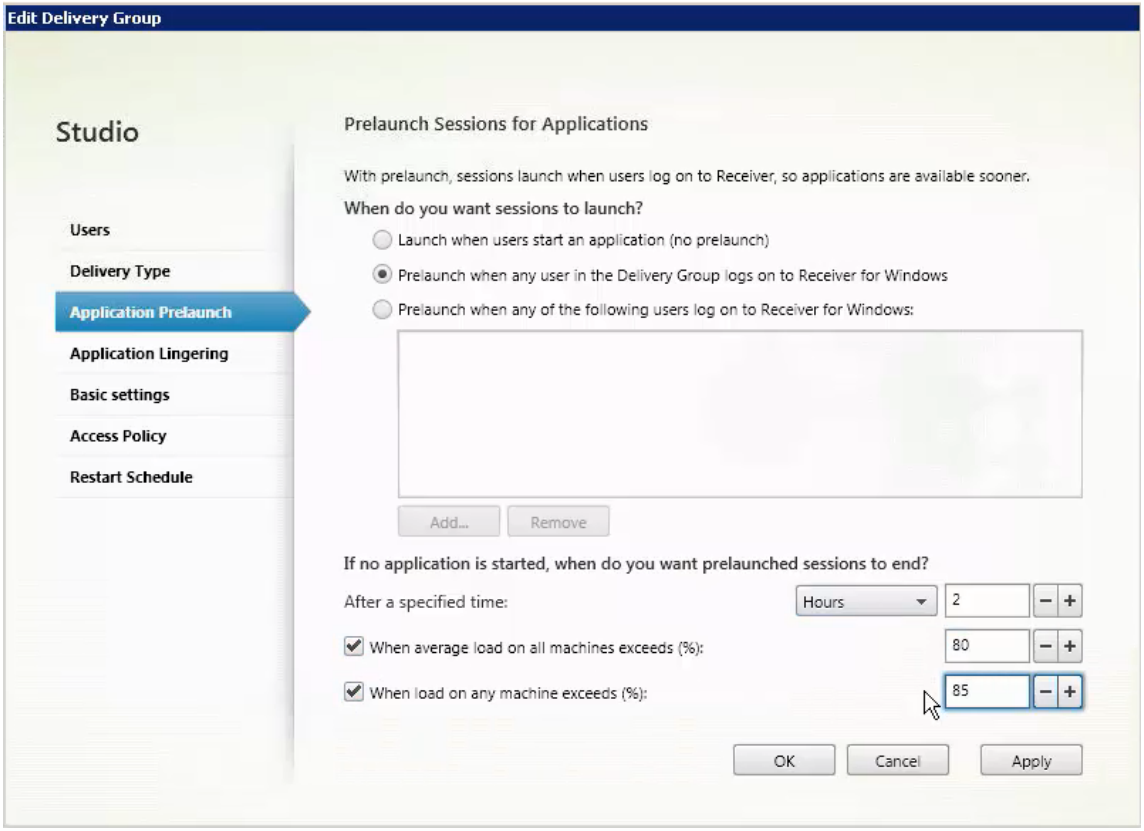
arrêtées une à une à toutes les minutes jusqu'à ce que la charge tombe en dessous du seuil. Lorsque la valeur de seuil est dépassée, aucune nouvelle session de pré-lancement n'est démarrée.

Les serveurs avec des VDA qui n'ont pas été inscrits avec un Controller et les serveurs en mode de maintenance sont considérés comme entièrement chargés. Un problème inattendu provoque la fermeture automatique des sessions de pré-lancement et des sessions de persistance pour libérer de la capacité.

**Pour activer le pré-lancement de session**

1. Sélectionnez un groupe, puis cliquez sur **Modifier le groupe de mise à disposition** dans la barre d'actions.
2. Sur la page **Pré-démarrage d'application**, activez le pré-lancement de session, en choisissant le moment de démarrage des sessions :
    - Lorsqu'un utilisateur démarre une application. C'est le réglage par défaut. Le pré-lancement de session est désactivé.
    - Lorsqu'un utilisateur du groupe de mise à disposition ouvre une session sur l'application Citrix Workspace pour Windows.
    - Lorsque tout le monde dans une liste d'utilisateurs et de groupes d'utilisateurs ouvre une session sur l'application Citrix Workspace pour Windows. Veuillez également spécifier les utilisateurs ou les groupes d'utilisateurs si vous choisissez cette option.




3. Une session pré-lancée est remplacée par une session régulière lorsque l'utilisateur démarre une application. Si l'utilisateur ne démarre pas une application (la session pré-lancée n'est pas utilisée), les paramètres suivants affectent la durée pour laquelle la session reste active.

    - Lorsqu'un intervalle de temps spécifié expire. Vous pouvez modifier l'intervalle de temps (1-99 jours, 1-2 376 heures, heures ou 1-142 560 minutes).
    - Lorsqu'une charge moyenne sur toutes les machines du groupe de mise à disposition dépasse un pourcentage spécifié : 1-99%.
    - Lorsque la charge de toute machine du groupe de mise à disposition dépasse un pourcentage spécifié : 1-99%.

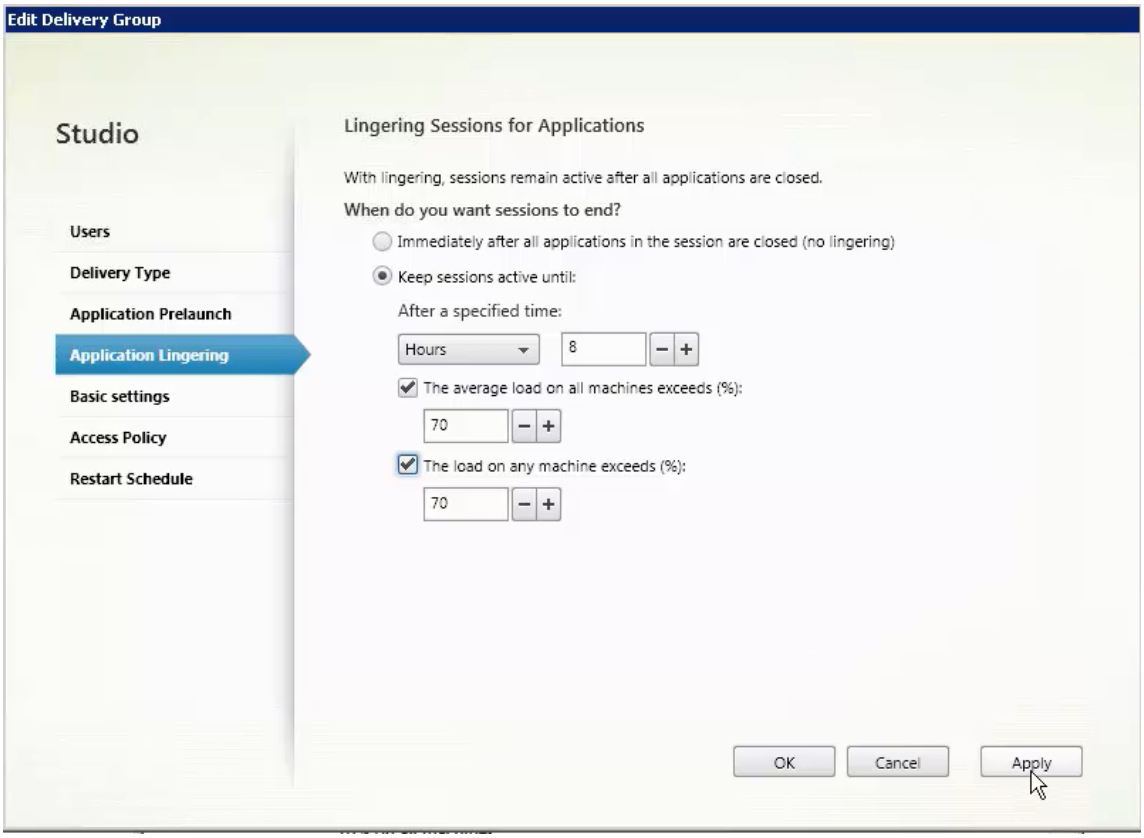
    Récapitulatif : une session pré-lancée reste active jusqu'à ce que l'un des événements suivants se produise : un utilisateur lance une application, la durée spécifiée est écoulée, ou un seuil de charge spécifié est dépassé.

**Pour activer la persistance de session**

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier le groupe de mise à disposition** dans la barre d'actions.

3. Sur la page **Attente d'application**, activez la persistance de session en sélectionnant **Maintenir les sessions dans l'état actif jusqu'à**.




4. Plusieurs paramètres affectent la durée pendant laquelle une session persistante reste active si l'utilisateur ne démarre pas d'autre application.

   - Lorsqu'un intervalle de temps spécifié expire. Vous pouvez modifier l'intervalle de temps : 1-99 jours, 1-2 376 heures, heures ou 1-142 560 minutes.
   - Lorsqu'une charge moyenne sur toutes les machines du groupe de mise à disposition dépasse un pourcentage spécifié : 1-99%.
   - Lorsque la charge de toute machine du groupe de mise à disposition dépasse un pourcentage spécifié : 1-99%.

   Récapitulatif : une session de persistance reste active jusqu'à ce que l'un des événements suivants se produise : un utilisateur démarre une application, la durée spécifiée est écoulée, ou un seuil de charge spécifié est dépassé.

**Contrôler la reconnexion de session en cas de déconnexion d'une machine en mode de maintenance**

> **REMARQUE :**
>
> Cette fonctionnalité est disponible uniquement dans PowerShell.

Vous pouvez contrôler si les sessions déconnectées sur des machines en mode de maintenance sont autorisées à se reconnecter aux machines du groupe de mise à disposition.

Avant la version 2106, la reconnexion n'était pas autorisée pour les sessions de bureaux groupés mono-session qui s'étaient déconnectées des machines en mode de maintenance. À partir de la version 2106, vous pouvez configurer un groupe de mise à disposition pour autoriser ou interdire les reconnexions (quel que soit le type de session) après déconnexion d'une machine en mode de maintenance.

Lors de la création ou de la modification d'un groupe de mise à disposition (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), utilisez le paramètre `-AllowReconnectInMaintenanceMode <boolean>` pour autoriser ou interdire les reconnexions des machines déconnectées d'une machine en mode de maintenance.

- Lorsque la valeur est définie sur true, les sessions peuvent se reconnecter aux machines du groupe.
- Lorsque la valeur est définie sur false, les sessions ne peuvent pas se reconnecter aux machines du groupe.

Valeurs par défaut :

- Mono-session : désactivé
- Multi-session : activé

### Configurer l'itinérance de session

Par défaut, l'itinérance de session est activée pour les groupes de mise à disposition. Les sessions sont partagées entre les machines clientes de l'utilisateur. Lorsque l'utilisateur ouvre une session et bascule sur une autre machine, la même session est utilisée et les applications sont disponibles sur les deux machines en même temps. Vous pouvez afficher les applications sur plusieurs périphériques. Les applications suivent, quelle que soit la machine ou que les sessions en cours existent ou non. Souvent, les imprimantes et les autres ressources attribuées à l'application suivent également. Vous pouvez également utiliser PowerShell. Pour plus d'informations, consultez la section Itinérance de session.

**Configurer l'itinérance de session pour les applications** Pour configurer l'itinérance de session pour les applications, procédez comme suit :

1. Dans la console, sélectionnez **Groupes de mise à disposition** dans le volet de gauche.

2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans la barre d'actions.
3. Sur la page **Utilisateurs**, activez l'itinérance de session en cochant la case **Les sessions se déplacent avec les utilisateurs lorsqu'ils passent d'un périphérique à l'autre**.
    - Si cette option est activée, lorsque l'utilisateur ouvre une session d'application et bascule sur un autre périphérique, la même session est utilisée et disponible sur les deux périphériques. Lorsque cette option est désactivée, la session ne passe plus d'un périphérique à l'autre.
4. Sélectionnez **OK** pour appliquer les modifications et fermer la fenêtre.

**Configurer l'itinérance de session pour les bureaux** Pour configurer l'itinérance de session pour un bureau, procédez comme suit :

1. Dans la console, sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier** dans la barre d'actions.
3. Sur la page **Bureaux**, sélectionnez le bureau, puis sélectionnez **Modifier**.
4. Activez l'itinérance de session en cochant la case **Itinérance de session**.

- Si cette option est activée, lorsque l'utilisateur lance le bureau et bascule sur un autre périphérique, la même session est utilisée et les applications sont disponibles sur les deux périphériques. Lorsque cette option est désactivée, la session ne passe plus d'un périphérique à l'autre.

Sélectionnez **OK** pour appliquer les modifications et fermer la fenêtre.

## Dépannage

- Les VDA qui ne sont pas enregistrés auprès d'un Delivery Controller ne sont pas pris en compte lors du lancement de sessions non négociées. Cela entraîne une sous-utilisation des ressources disponibles. Il existe un certain nombre de raisons pour lesquelles un VDA peut ne pas être enregistré, un grand nombre d'entre elles pouvant être résolues par un administrateur. L'écran des détails offre des informations de dépannage dans l'Assistant de création de catalogue de machines, et après l'ajout d'un catalogue de machines à un groupe de mise à disposition.

  Une fois que vous avez créé un groupe de mise à disposition, le panneau de détails pour un groupe de mise à disposition indique le nombre de machines qui peuvent être enregistrées, mais ne le sont pas. Par exemple, une ou plusieurs machines peuvent être sous tension et pas en mode de maintenance, mais pas enregistrées auprès d'un Controller. Lors de l'affichage d'

une machine « non enregistrée », mais qui devrait l'être, l'onglet **Dépannage** dans le panneau Détails fournit des causes possibles et les actions correctives recommandées.

Pour les messages sur le niveau fonctionnel, consultez la section Versions VDA et niveaux fonctionnels.

Pour plus d'informations sur le dépannage de l'enregistrement de VDA, voir l'article CTX136668.

- Dans l'écran d'un groupe de mise à disposition, la **version de VDA installée** dans le panneau Détails peut différer de la version installée sur les machines. Les programmes et fonctionnalités Windows de la machine affichent la version actuelle du VDA.
- Pour les machines affichant un **état d'alimentation inconnu**, consultez l'article CTX131267 pour plus d'informations.

## Créer des groupes d'applications

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

### Introduction

Les groupes d'applications vous permettent de gérer des collections d'applications. Créez des groupes d'applications pour les applications partagées entre différents groupes de mise à disposition. Ou bien, les applications utilisées par un sous-ensemble d'utilisateurs dans des groupes de mise à disposition. Les groupes d'applications sont facultatifs ; ils offrent une alternative à l'ajout des mêmes applications sur plusieurs groupes de mise à disposition. Associez des groupes de mise à disposition à plusieurs groupes d'applications et associez un groupe d'applications à plusieurs groupes de mise à disposition.

Comparativement à l'utilisation d'un plus grand nombre de groupes de mise à disposition, les groupes d'applications permettent de gérer les applications et de contrôler les ressources :

- Le regroupement logique d'applications et de leurs paramètres vous permet de gérer ces applications comme une unité unique. Par exemple, vous n'avez pas besoin d'ajouter (publier) la même application, une par une, à des groupes de mise à disposition individuels.

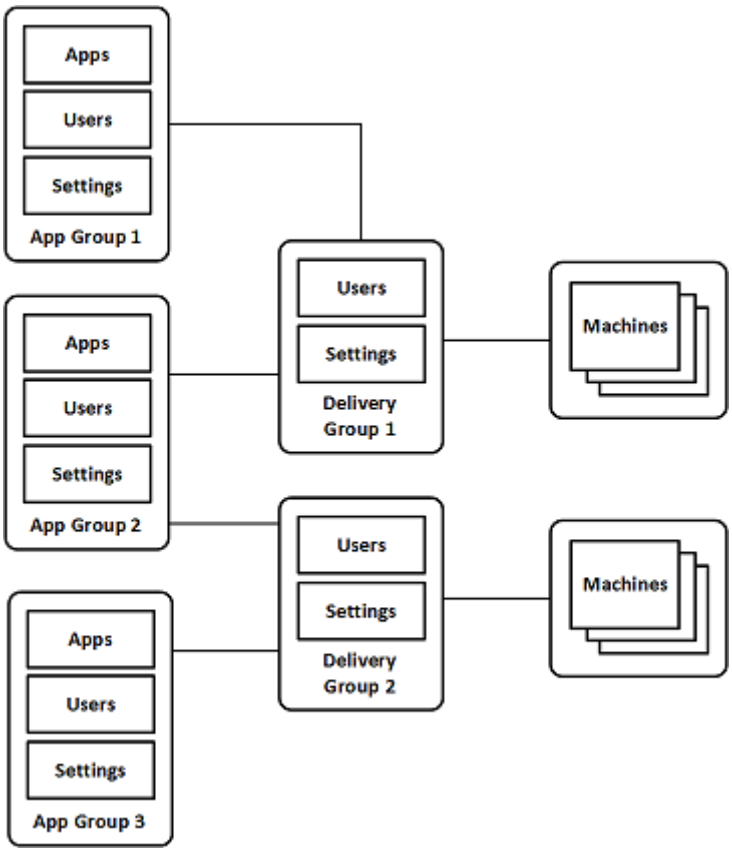
 

- Le partage de session entre des groupes d'applications peut économiser la consommation de ressources. Dans d'autres cas, la désactivation du partage de session entre les groupes d'applications peut s'avérer bénéfique.
- Vous pouvez utiliser la fonction de restriction de balise pour publier des applications à partir d'un groupe d'applications, prenant en compte un seul sous-ensemble de machines dans les groupes de mise à disposition sélectionnés. Avec les restrictions de balise, vous pouvez utiliser des machines existantes pour plusieurs tâches de publication, éliminant ainsi les coûts associés avec le déploiement et la gestion de machines supplémentaires. L'utilisation d'une restriction de balise équivaut à diviser (ou partitionner) des machines dans un groupe de mise à disposition. L'utilisation d'un groupe d'applications ou de bureaux avec une restriction de balise peut s'avérer utile pour isoler et dépanner un sous-ensemble de machines dans un groupe de mise à disposition.

## Exemples de configuration

### Exemple 1 :

Le graphique suivant illustre un déploiement Citrix Virtual Apps and Desktops qui comprend des groupes d'applications :




Dans cette configuration, les applications sont ajoutées à des groupes d'applications, et non à des

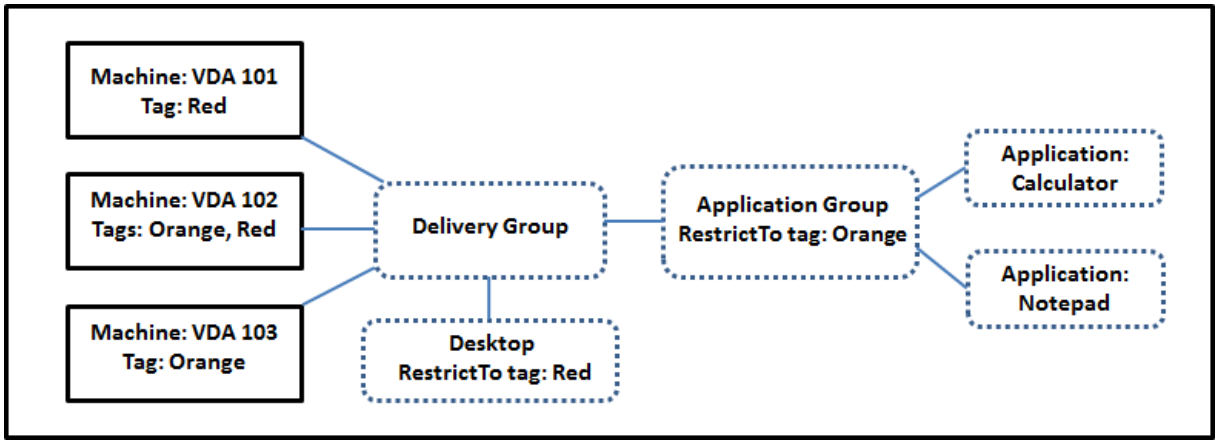
groupes de mise à disposition. Les groupes de mise à disposition spécifient les machines utilisées. (Bien que cela ne soit pas affiché, les machines se trouvent dans des catalogues de machines).

Le groupe d'applications 1 est associé au groupe de mise à disposition 1. Accès aux applications du groupe d'applications 1 par les utilisateurs spécifiés dans le groupe d'applications 1. Ces groupes n'apparaissent que s'ils figurent également dans la liste d'utilisateurs du groupe de mise à disposition 1. Cette approche suit les recommandations selon lesquelles la liste d'utilisateurs d'un groupe d'applications est un sous-ensemble (une restriction) des listes d'utilisateurs des groupes de mise à disposition associés. Les paramètres du groupe d'applications 1 (tels que le partage de session d'application entre groupes d'applications, groupes de mise à disposition associés) s'appliquent aux applications et utilisateurs de ce groupe. Les paramètres du groupe de mise à disposition de 1 s'appliquent aux utilisateurs des groupes d'applications 1 et 2, car ces groupes d'applications ont été associés à ce groupe de mise à disposition.

Le groupe d'applications 2 est associé à deux groupes de mise à disposition : 1 et 2. Chacun de ces groupes de mise à disposition se voit attribuer une priorité dans le groupe d'applications 2, ce qui indique l'ordre dans lequel les groupes de mise à disposition sont vérifiés lorsqu'une application est lancée. La charge des groupes de disposition ayant le même niveau de priorité est équilibrée. Accès aux applications du groupe d'applications 2 par les utilisateurs spécifiés dans le groupe d'applications 2. Toutefois, ils doivent également apparaître dans les listes d'utilisateurs pour le groupe de mise à disposition 1 et le groupe de mise à disposition 2.

**Exemple 2 :**

Cette configuration simple utilise des restrictions de balise pour limiter les machines qui sont prises en compte pour certains lancements de bureau et d'application. Le site dispose d'un groupe de mise à disposition partagé, d'un bureau publié et d'un groupe d'applications configuré avec deux applications.




Des balises ont été ajoutées à chacune des trois machines (VDA 101-103).

Le groupe d'applications a été créé avec la restriction de balise « Orange ». Chacune de ses applications est lancée uniquement sur les machines de ce groupe de mise à disposition qui ont la balise

« Orange », VDA 102 et 103.

Pour obtenir des exemples et des instructions sur l'utilisation des restrictions de balise dans des groupes d'applications (et pour des bureaux), veuillez consulter l'article Balises.

### Conseils et considérations

Citrix vous recommande d'ajouter des applications à des groupes d'applications ou des groupes de mise à disposition, mais pas aux deux. Sinon, la complexité engendrée par le fait d'avoir des applications dans deux types de groupes peut rendre leur gestion plus difficile.

Par défaut, un groupe d'applications est activé. Lorsque vous créez un groupe d'applications, vous pouvez modifier le groupe pour modifier ce paramètre. Consultez Gérer des groupes d'applications.

Par défaut, le partage de session d'application entre les groupes d'applications est activé. Consultez l'article Partage de session entre des groupes d'applications.

Citrix recommande de mettre à niveau vos groupes de mise à disposition vers la version actuelle. Ce processus nécessite :

1. Mise à niveau des VDA sur les machines utilisées dans le groupe de mise à disposition
2. Mise à niveau des catalogues de machines contenant ces machines
3. Mise à niveau du groupe de mise à disposition

Pour de plus amples informations, consultez la section Gérer des groupes d'applications.

Pour utiliser des groupes d'applications, vos composants principaux doivent être à la version minimale 7.9.

La création de groupes d'applications nécessite les autorisations d'administration déléguée du rôle intégré d'administrateur de groupe de mise à disposition. Consultez Administration déléguée pour plus de détails.

Cet article fait référence à l'« association » d'une application avec plusieurs groupes d'applications. Il ne s'agit pas d'ajouter des instances de cette application à partir d'une source disponible. De même, les groupes de mise à disposition sont associés à des groupes d'applications, plutôt que des ajouts ou des composants de l'un ou l'autre.

### Partage de session avec des groupes d'applications

Lorsque le partage de session d'application est activé, toutes les applications démarrent dans la même session d'application. Cette option permet d'économiser les coûts associés au lancement de sessions d'application supplémentaires et d'utiliser les fonctionnalités applicatives qui impliquent

le Presse-papiers, telles que les opérations de copier-coller. Cependant, dans certaines situations, vous pouvez effacer le partage de session.

Lorsque vous utilisez des groupes d'applications, vous pouvez configurer le partage de session d'application de trois manières qui étendent le comportement du partage de session standard disponible lorsque vous utilisez uniquement des groupes de mise à disposition :

- Partage de session activé entre des groupes d'applications
- Partage de session activé uniquement entre les applications d'un même groupe d'applications
- Partage de session désactivé.

#### Partage de session entre des groupes d'applications

Vous pouvez activer le partage de session d'application entre groupes d'applications, ou vous pouvez le désactiver pour limiter le partage de session d'application aux applications d'un même groupe d'applications.

- **Exemple dans lequel l'activation du partage de session entre des groupes d'applications est utile :**

  Le groupe d'applications 1 contient des applications Microsoft Office telles que Word et Excel. Le groupe d'applications 2 contient d'autres applications telles que le bloc-notes et la calculatrice, et les deux groupes d'applications sont associés au même groupe de mise à disposition. Un utilisateur qui a accès aux deux groupes d'applications démarre une session d'application en lançant Word, puis ouvre le bloc-notes. Si le Controller détermine que la session existante de l'utilisateur exécutant Word peut exécuter le bloc-notes, le bloc-notes est démarré dans la session existante. Si le bloc-notes ne peut pas être exécuté à partir de la session existante (par exemple, si la restriction de balise exclut la machine sur laquelle la session est en cours d'exécution), une nouvelle session sur une machine appropriée est préférée au partage de session.

- **Exemple dans lequel la désactivation du partage de session entre des groupes d'applications est utile :**

  Configuration avec un ensemble d'applications qui ne fonctionnent pas correctement avec d'autres applications installées sur les mêmes machines. Telles que deux versions différentes de la même suite logicielle ou deux versions différentes du même navigateur Web. Vous ne souhaitez pas autoriser un utilisateur à lancer les deux versions dans la même session.

  Créez un groupe d'applications pour chaque version de la suite logicielle, et ajoutez les applications de chaque version de la suite logicielle au groupe d'applications correspondant. Si le partage de session entre les groupes est désactivé pour chacun de ces groupes d'application, un utilisateur spécifié dans ces groupes peuvent exécuter les applications de la même version dans la même session. L'utilisateur peut toujours exécuter d'autres applications simultanément, mais pas dans la même session. Lors du lancement d'une des applications dont la ver-

sion est différente, ou d'une application qui ne figure pas dans un groupe d'applications, cette application est lancée dans une nouvelle session.

Cette fonctionnalité de partage de session entre groupes d'applications n'est pas une fonctionnalité de sécurité faisant appel à un sandbox. Elle n'est pas infaillible et elle ne peut pas empêcher les utilisateurs de lancer des applications dans leurs sessions via d'autres moyens (par exemple, au travers de l'Explorateur Windows).

Si une machine fonctionne à pleine capacité, les nouvelles sessions ne sont pas démarrées sur cette dernière. De nouvelles applications sont démarrées dans les sessions existantes sur la machine, selon les besoins, à l'aide du partage de session.

Vous pouvez uniquement mettre des sessions pré-lancées à disposition des groupes d'applications pour lesquels le partage de session d'application est autorisé. (Les sessions qui utilisent la fonctionnalité de persistance de session sont à disposition de tous les groupes d'application.) Ces fonctionnalités doivent être activées et configurées dans chacun des groupes de mise à disposition associés au groupe d'applications. Vous ne pouvez pas les configurer dans les groupes d'applications.

Par défaut, le partage de session d'applications entre groupes d'applications est activé lorsque vous créez un groupe d'applications. Vous ne pouvez pas changer ce paramètre lors de la création du groupe. Lorsque vous créez un groupe d'applications, vous pouvez modifier le groupe pour modifier ce paramètre. Consultez Gérer des groupes d'applications.

#### Désactiver le partage de session dans un groupe d'applications

Vous pouvez empêcher le partage de session d'application entre les applications qui appartiennent au même groupe d'applications.

- **Exemple dans lequel la désactivation du partage de session dans des groupes d'applications est utile :**

  Vous voulez que vos utilisateurs accèdent à plusieurs sessions plein écran simultanées d'une application sur des écrans distincts.

  Vous créez un groupe d'applications et ajoutez les applications à ce groupe.

Par défaut, le partage de session d'applications est activé lorsque vous créez un groupe d'applications. Vous ne pouvez pas changer ce paramètre lors de la création du groupe. Lorsque vous créez un groupe d'applications, vous pouvez modifier le groupe pour modifier ce paramètre. Consultez Gérer des groupes d'applications.

### Créer un groupe d'applications

Pour créer un groupe d'applications :

1. Connectez-vous à Web Studio.
2. Sélectionnez **Applications** dans le volet gauche de Studio, puis sélectionnez l'onglet **Groupes d'applications**.
3. Pour organiser les groupes d'applications sous forme de dossiers, créez des dossiers dans le dossier racine **Groupes d'applications**.
4. Sélectionnez le dossier dans lequel vous souhaitez créer le groupe, puis cliquez sur **Créer groupe d'applications**. L'assistant de création de groupe s'ouvre avec une page d'**introduction**. Vous pourrez retirer cette page lors des prochains lancements de cet assistant.
5. Suivez l'assistant pour configurer les paramètres sur les pages décrites ci-dessous. Lorsque vous avez terminé chaque page, sélectionnez **Suivant** jusqu'à la page **Résumé**.

#### Étape 1. Groupes de mise à disposition

La page **Groupes de mise à disposition** répertorie tous les groupes de mise à disposition, avec le nombre de machines que chaque groupe contient.

- La liste **Groupes de mise à disposition compatibles** contient les groupes de mise à disposition que vous pouvez sélectionner. Les groupes de mise à disposition compatibles contiennent des machines avec OS multi-session ou mono-session aléatoires (non attribuées de façon permanente ou statique).
- La liste **Groupes de mise à disposition incompatibles** contient les groupes de mise à disposition que vous ne pouvez pas sélectionner. Chaque entrée explique pourquoi un groupe n'est pas compatible, par exemple parce qu'il contient machines attribuées de manière statique.

Un groupe d'applications peut être associé à des groupes de mise à disposition contenant des machines partagées (non privées) qui peuvent mettre à disposition des applications.

Vous pouvez également sélectionner des groupes de mise à disposition contenant des machines partagées qui ne fournissent que des postes de travail, si les deux conditions suivantes sont remplies :

- Le groupe de mise à disposition contient des machines partagées et a été créé avec une version XenDesktop antérieure à 7.9.x.
- Vous avez l'autorisation Modifier le groupe de mise à disposition.

Le type de groupe de mise à disposition est automatiquement converti en « bureaux et applications » lorsque l'assistant Créer groupe d'applications est validé.

Bien que vous puissiez créer un groupe d'applications qui n'est associé à aucun groupe de mise à disposition (par exemple pour organiser les applications ou pour servir de stockage aux applications non utilisées) le groupe d'applications ne peut pas être utilisé pour mettre à disposition des applications tant qu'il ne spécifie pas au moins un groupe de mise à disposition. En outre, vous ne pouvez

pas ajouter d'applications au groupe d'applications à partir de la source **Depuis le menu Démarrer** si aucun groupe de mise à disposition n'est spécifié.

Les groupes de mise à disposition que vous sélectionnez spécifient les machines qui sont utilisées pour mettre à disposition des applications. Sélectionnez les cases à cocher en regard des groupes de mise à disposition que vous souhaitez associer au groupe d'applications.

Pour ajouter une restriction de balise, sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise dans la liste déroulante.

#### Étape 2. Utilisateurs

Spécifiez les utilisateurs d'applications dans le groupe d'applications. Vous pouvez autoriser tous les utilisateurs et groupes d'utilisateurs dans les groupes de mise à disposition que vous avez sélectionnés sur la page précédente, ou sélectionner des utilisateurs et groupes d'utilisateurs spécifiques à partir de ces groupes de mise à disposition. Si vous limitez l'utilisation aux utilisateurs spécifiés, seuls les utilisateurs spécifiés dans le groupe de mise à disposition et le groupe d'applications peuvent accéder aux applications dans ce groupe. Concrètement, la liste d'utilisateurs du groupe d'applications filtre les listes d'utilisateurs des groupes de mise à disposition.

La possibilité d'activer ou de désactiver l'utilisation d'applications par des utilisateurs non authentifiés est uniquement disponible dans les groupes de mise à disposition, et pas dans les groupes d'applications.

Pour plus d'informations sur l'emplacement des listes d'utilisateurs dans un déploiement, voir Où les listes d'utilisateurs sont spécifiées.

#### Étape 3. Applications

À savoir :

- Par défaut, les applications que vous ajoutez sont placées dans un dossier nommé **Applications**. Vous pouvez spécifier un dossier différent. Si vous essayez d'ajouter une application et qu'une application avec le même nom existe dans ce dossier, vous êtes invité à renommer l'application que vous ajoutez. Si vous acceptez le nom unique suggéré, l'application est ajoutée avec ce nouveau nom. Sinon, vous devez la renommer vous-même avant de pouvoir l'ajouter. Pour de plus amples informations, consultez la section Gérer les dossiers d'applications.
- Vous pouvez modifier les propriétés d'une application (paramètres) lorsque vous l'ajoutez ou ultérieurement. Voir la section Modifier les propriétés de l'application. Si vous publiez deux applications du même nom vers les mêmes utilisateurs, modifiez la propriété **Nom de l'application (pour l'utilisateur)** dans Web Studio. Sinon, des noms en double s'affichent dans l'application Citrix Workspace.

- Lorsque vous ajoutez une application à plusieurs groupes d'applications, vous risquez de rencontrer un problème de visibilité si vous ne disposez pas d'autorisations suffisantes pour afficher l'application dans tous ces groupes. Dans ce cas, consultez un administrateur disposant des autorisations appropriées ou demandez une extension de vos autorisations à tous les groupes auxquels l'application a été ajoutée.

Cliquez sur **Ajouter** dans le menu déroulant pour afficher les sources de l'application.

- **À partir du menu Démarrer :** applications qui sont découvertes sur une machine dans les groupes de mise à disposition sélectionnés. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**.

  Cette source ne peut pas être sélectionnée si vous avez sélectionné l'une des options suivantes :

  - Groupes d'applications qui n'ont pas de groupes de mise à disposition associés.
  - Groupes d'applications avec des groupes de mise à disposition associés qui ne contiennent pas de machines.
  - Un groupe de mise à disposition ne contenant pas de machines.

- **Manuellement définies :** applications qui se trouvent dans le site ou ailleurs dans votre réseau. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez taper le chemin d'accès de l'exécutable, le répertoire de travail, les arguments de la ligne de commande (facultatifs), et les noms affichés des administrateurs et des utilisateurs. Après avoir entré ces informations, cliquez sur **OK**.

- **Existantes :** applications déjà ajoutées au site. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**. Cette source ne peut pas être sélectionnée si le site ne dispose d'aucune application.

- **App-V :** applications dans des packages App-V. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez sélectionner le **serveur App-V** ou la **bibliothèque d'applications**. À partir de l'écran qui s'affiche, sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**. Pour plus d'informations, consultez la section Déployer et fournir des applications App-V. Cette source ne peut pas être sélectionnée (ou peut ne pas s'afficher) lorsque App-V n'est pas configuré pour le site.

Comme indiqué, certaines sources dans la liste déroulante **Ajouter** ne peuvent pas être sélectionnées s'il n'existe source valide de ce type. Les sources qui ne sont pas compatibles ne sont pas répertoriées (par exemple, vous ne pouvez pas ajouter de groupe d'applications à des groupes d'applications, par conséquent la source n'est pas répertoriée lorsque vous créez un groupe d'applications).

#### Étape 4. Étendues

Cette page s'affiche uniquement si vous avez déjà créé une étendue. personnalisée Par défaut, l'étendue **Tous** est sélectionnée. Pour plus d'informations, consultez Administration déléguée.

#### Étape 5. Résumé

Entrez un nom pour le groupe d'applications. Vous pouvez également entrer une description (facultatif).

Consultez les informations récapitulatives, puis cliquez sur **Terminer**.

## Gérer des groupes d'applications

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

### Introduction

Cet article décrit comment gérer les groupes d'applications que vous avez créés.

Consultez Applications pour savoir comment gérer les applications de groupes d'applications ou de groupes de mise à disposition, notamment comment :

- Ajouter ou supprimer des applications d'un groupe d'applications.
- Modifier les associations de groupes d'applications.

La gestion des groupes d'applications nécessite les autorisations d'administration déléguée du rôle intégré d'administrateur de groupe de mise à disposition. Consultez Administration déléguée pour plus de détails.

### Activer ou désactiver un groupe d'applications

Lorsqu'un groupe d'applications est activé, il peut mettre à disposition les applications qui lui ont été ajoutées. La désactivation d'un groupe d'applications désactive chaque application dans ce groupe.

Cependant, si ces applications sont également associées à d'autres groupes d'applications activés, elles peuvent être mises à disposition à partir de ces groupes. Si l'application a été expressément ajoutée à des groupes de mise à disposition associés au groupe d'applications, la désactivation du groupe d'applications n'affecte pas les applications dans ces groupes de mise à disposition.

Un groupe d'applications est activé lorsque vous le créez. Vous ne pouvez pas changer cette configuration lors de la création du groupe.

1. Sélectionnez **Applications** dans le volet gauche de Studio, puis sélectionnez l'onglet **Groupes d'applications**.
2. Sélectionnez un groupe d'applications, puis sélectionnez **Modifier groupe d'applications** dans la barre d'actions.
3. Sur la page **Paramètres**, sélectionnez ou désélectionnez la case à cocher **Activer groupe d'applications**.
4. Cliquez sur **Appliquer** pour garder la fenêtre ouverte, ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

### Activer ou désactiver le partage de session d'application entre des groupes d'applications

Le partage de session entre groupes d'applications est activé lorsque vous créez un groupe d'applications. Vous ne pouvez pas changer cette configuration lors de la création du groupe. Pour de plus amples informations, consultez la section Partage de session avec des groupes d'applications.

1. Sélectionnez **Applications** dans le volet gauche de Studio, puis sélectionnez l'onglet **Groupes d'applications**.
2. Sélectionnez un groupe d'applications, puis sélectionnez **Modifier groupe d'applications** dans la barre d'actions.
3. Sur la page **Paramètres**, sélectionnez ou désélectionnez la case à cocher **Activer le partage de session d'application entre les groupes d'applications**.
4. Cliquez sur **Appliquer** pour garder la fenêtre ouverte, ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

### Désactiver le partage de session d'application dans un groupe d'applications

Le partage de session entre applications dans le même groupe d'applications est activé par défaut lorsque vous créez un groupe d'applications. Si vous désactivez le partage de session d'application entre groupes d'applications, le partage de session entre applications dans le même groupe d'applications reste activé.

Vous pouvez utiliser le SDK PowerShell pour configurer des groupes d'applications avec le partage de session d'application désactivé entre les applications qu'ils contiennent. Dans certaines circonstances, cette option est souhaitable. Par exemple, vous pouvez souhaiter que les utilisateurs lancent des applications non transparentes dans des fenêtres d'application plein écran utilisent sur des écrans distincts.

Lorsque vous désactivez le partage de session d'application dans un groupe d'applications, chaque application dans ce groupe se lance dans une nouvelle session d'application. Si une session déconnectée appropriée exécutant la même application est disponible, elle est reconnectée. Par exemple, lorsque vous lancez le Bloc-notes avec une session déconnectée avec le Bloc-notes en cours d'exécution, cette session est reconnectée au lieu d'en créer une. Si plusieurs sessions déconnectées appropriées sont disponibles, l'une des sessions est choisie pour la reconnexion, de manière aléatoire mais déterministe. Si la situation se reproduit dans les mêmes circonstances, la même session est choisie, mais la session n'est pas toujours prévisible.

Utilisez le KSDK PowerShell pour désactiver le partage de session d'application pour toutes les applications d'un groupe d'applications existant, ou pour créer un groupe avec le partage de session d'application désactivé.

#### Exemples d'applets de commande PowerShell

Pour désactiver le partage de session, utilisez les applets de commande Broker PowerShell `New-BrokerApplicationGroup` ou `Set-BrokerApplicationGroup` avec le paramètre `SessionSharingEnabled` défini sur `False` et le paramètre `SingleAppPerSession` défini sur `True`.

- Par exemple pour créer un groupe d'applications avec le partage de session d'application désactivé pour toutes les applications dans le groupe :

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- Par exemple pour désactiver le partage de session d'application entre toutes les applications d'un groupe d'applications existant :

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

#### Considérations

- Pour activer la propriété `SingleAppPerSession`, vous devez définir la propriété `SessionSharingEnabled` sur False. Les deux propriétés ne doivent pas être activées

en même temps. Le paramètre `SessionSharingEnabled` fait référence au partage de sessions entre groupes d'applications.
- Le partage de session d'application ne fonctionne que pour les applications qui sont associées à des groupes d'applications, mais qui ne sont pas associées à des groupes de mise à disposition. Toutes les applications associées directement à un groupe de mise à disposition partagent les sessions par défaut.
- Si une application est affectée à plusieurs groupes d'applications, assurez-vous que les groupes n'ont pas de paramètres en conflit. Par exemple, un groupe avec l'option définie sur `True` et l'option d'un autre groupe sur `False` entraîne un comportement imprévisible.

### Renommer un groupe d'applications

1. Sélectionnez **Applications** dans le volet gauche de Studio, puis sélectionnez l'onglet **Groupes d'applications**.
2. Sélectionnez un groupe d'applications, puis sélectionnez **Renommer groupe d'applications** dans la barre d'actions.
3. Spécifiez le nouveau nom unique puis cliquez sur **OK**.

### Ajouter, supprimer ou modifier la priorité d'associations de groupe de mise à disposition avec un groupe d'applications

Un groupe d'applications peut être associé à des groupes de mise à disposition contenant des machines partagées (non privées) qui peuvent mettre à disposition des applications.

Vous pouvez également sélectionner des groupes de mise à disposition contenant des machines partagées qui ne fournissent que des postes de travail, si les deux conditions suivantes sont remplies :

- Le groupe de mise à disposition contient des machines partagées et a été créé avec une version antérieure à 7.9.x.
- Vous avez l'autorisation Modifier le groupe de mise à disposition.

Le type de groupe de mise à disposition est automatiquement converti en « bureaux et applications » lorsque la boîte de dialogue **Modifier groupe d'applications** est validée.

1. Sélectionnez **Applications** dans le volet gauche de Studio, puis sélectionnez l'onglet **Groupes d'applications**.
2. Sélectionnez un groupe d'applications, puis sélectionnez **Modifier groupe d'applications** dans la barre d'actions.
3. Sélectionnez la page **Groupes de mise à disposition**.

4. Pour ajouter des groupes de mise à disposition, cliquez sur **Ajouter**. Sélectionnez les cases à cocher des groupes de mise à disposition disponibles. (Les groupes de mise à disposition non compatibles ne peuvent pas être sélectionnés). Lorsque vous avez terminé vos sélections, cliquez sur **OK**.
5. Pour supprimer des groupes de mise à disposition, cochez les cases des groupes que vous souhaitez supprimer, puis cliquez sur **Supprimer**. Confirmez la suppression lorsque vous y êtes invité.
6. Pour modifier la priorité des groupes de mise à disposition, cochez la case du groupe de mise à disposition, puis cliquez sur **Modifier la priorité**. Entrez la priorité (0 = priorité la plus élevée), puis cliquez sur **OK**.
7. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

### Ajouter, modifier ou supprimer une restriction de balise dans un groupe d'applications

L'ajout, la modification et la suppression de restrictions de balise peut avoir des effets inattendus sur les machines qui sont prises en compte pour le démarrage de l'application. Consultez les informations et précautions dans la section Balises.

1. Sélectionnez **Applications** dans le volet gauche de Studio, puis sélectionnez l'onglet **Groupes d'applications**.
2. Sélectionnez un groupe d'applications, puis sélectionnez **Modifier groupe d'applications** dans la barre d'actions.
3. Sélectionnez la page **Groupes de mise à disposition**.
4. Pour ajouter une restriction de balise, sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise dans la liste déroulante.
5. Pour modifier ou supprimer une restriction de balise, sélectionnez une autre balise ou supprimez la restriction de balise complètement en désactivant le paramètre **Restreindre les lancements aux machines dotées de balises**.
6. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

### Ajouter ou supprimer des utilisateurs d'un groupe d'applications

Pour de plus amples informations sur les utilisateurs, consultez la section Créer des groupes de mise à disposition.

1. Sélectionnez **Applications** dans le volet gauche de Studio, puis sélectionnez l'onglet **Groupes d'applications**.
2. Sélectionnez un groupe d'applications, puis sélectionnez **Modifier groupe d'applications** dans la barre d'actions.
3. Sélectionnez la page **Utilisateurs**. Indiquez si vous souhaitez autoriser tous les utilisateurs dans les groupes de mise à disposition associés à utiliser les applications du groupe d'applications, ou uniquement des utilisateurs et groupes spécifiques. Pour ajouter des utilisateurs, cliquez sur **Ajouter**, puis spécifiez les utilisateurs que vous souhaitez ajouter. Pour supprimer des utilisateurs, sélectionnez un ou plusieurs utilisateurs, puis cliquez sur **Supprimer**.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

### Ajouter, modifier ou supprimer une icône d'application d'un groupe d'applications

Procédez comme suit pour ajouter, modifier ou supprimer une icône d'application.

1. Sélectionnez **Applications** dans le volet de gauche.
2. Sous l'onglet **Applications**, sélectionnez une application, puis sélectionnez **Propriétés**.

   Pour apporter des modifications au niveau d'un groupe d'applications, accédez à l'onglet **Groupes d'applications**, sélectionnez une application dans un groupe, puis sélectionnez **Propriétés**.
3. Sélectionnez la page **Mise à disposition**, puis sélectionnez **Modifier**. La fenêtre **Sélectionner une icône** apparaît.
4. Dans la fenêtre **Sélectionner une icône**, effectuez l'une des opérations suivantes :

   - Pour ajouter une icône, sélectionnez **Ajouter**, puis accédez à l'icône.
   - Pour supprimer une icône, sélectionnez-la, puis sélectionnez **Supprimer**.
   - Pour changer d'icône, sélectionnez-la pour l'application.

   > **Important :**
   >
   > - Vous ne pouvez pas ajouter une icône dont la taille est supérieure à 200 Ko.
   > - Vous ne pouvez ajouter que des fichiers .icon.
   > - Vous ne pouvez pas supprimer les icônes intégrées.
   > - Vous ne pouvez pas supprimer l'icône d'une application en cours d'utilisation.

5. Sélectionnez **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

### Modifier les étendues dans un groupe d'applications

Vous pouvez modifier une étendue uniquement si vous avez créé une étendue (vous ne pouvez pas modifier l'étendue Tout). Pour plus d'informations, consultez Administration déléguée.

1. Sélectionnez **Applications** dans le volet gauche de Studio, puis sélectionnez l'onglet **Groupes d'applications**.
2. Sélectionnez un groupe d'applications, puis sélectionnez **Modifier groupe d'applications** dans la barre d'actions.
3. Sélectionnez la page **Étendues**. Cochez ou décochez la case à cocher en regard d'une étendue.
4. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

### Modifier les étendues dans un groupe d'applications

Vous pouvez modifier une étendue uniquement si vous avez créé une étendue (vous ne pouvez pas modifier l'étendue Tout). Pour plus d'informations, consultez Administration déléguée.

1. Sélectionnez **Applications** dans le volet gauche de Studio, puis sélectionnez l'onglet **Groupes d'applications**.
2. Sélectionnez un groupe d'applications, puis sélectionnez **Modifier groupe d'applications** dans la barre d'actions.
3. Sélectionnez la page **Étendues**. Activez ou désactivez la case à cocher en regard des étendues que vous souhaitez modifier.
4. Sélectionnez **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou sélectionnez **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

### Supprimer un groupe d'applications

Une application doit être associée à au moins un groupe de mise à disposition ou groupe d'applications. Si la suppression d'un groupe d'applications a pour conséquence qu'une ou plusieurs applications n'appartiennent plus à un groupe, vous êtes averti que la suppression de ce groupe supprime également ces applications. Vous pouvez ensuite confirmer ou annuler la suppression.

La suppression d'une application ne la supprime pas de sa source d'origine. Toutefois, si vous souhaitez la rendre à nouveau disponible, vous devez l'ajouter à nouveau.

1. Sélectionnez **Applications** dans le volet gauche de Studio, puis sélectionnez l'onglet **Groupes d'applications**.

2. Sélectionnez un groupe d'applications, puis sélectionnez **Supprimer le groupe** dans la barre d'actions.
3. Confirmez la suppression lorsque vous y êtes invité.

## Organiser les groupes d'applications sous forme de dossiers

Vous pouvez créer des dossiers pour organiser les groupes d'applications afin d'en faciliter l'accès.

### Rôles requis

Par défaut, vous pouvez créer et gérer des dossiers pour les groupes d'applications si vous disposez de l'un des rôles intégrés suivants :

- Administrateur Cloud
- Administrateur complet
- Administrateur de groupes d'applications

Vous pouvez déléguer des actions de gestion à d'autres utilisateurs en créant des rôles personnalisés. Le tableau suivant répertorie les autorisations requises pour chaque action.

| Action | Autorisations requises |
|---|---|
| Créer des dossiers de groupe d'applications | Créer dossier de groupe d'applications |
| Supprimer des dossiers de groupe d'applications | Supprimer dossier de groupe d'applications |
| Déplacer des dossiers de groupe d'applications | Déplacer dossier de groupe d'applications |
| Renommer des dossiers de groupe d'applications | Modifier dossier de groupe d'applications |
| Déplacer des dossiers de groupe d'applications | Modifier dossier de groupe d'applications, Modifier propriétés du groupe d'applications |

Pour plus d'informations, consultez Créer et gérer des rôles.

### Créer et gérer des dossiers

Vous pouvez utiliser la barre d'actions ou le menu contextuel pour créer et gérer des dossiers de groupe d'applications. Vous pouvez aussi faire glisser un groupe d'applications ou un dossier vers l'emplacement de votre choix dans l'arborescence des dossiers.

À savoir :

- Vous pouvez imbriquer des dossiers sur un maximum de cinq niveaux (à l'exception du dossier racine par défaut).
- Un dossier peut contenir des groupes d'applications et des sous-dossiers. Vous pouvez supprimer un dossier uniquement si celui-ci et ses sous-dossiers ne contiennent pas de groupes d'applications.
- Tous les nœuds (tels que les catalogues de machines, les groupes de mise à disposition, les applications et les groupes d'applications) partagent une arborescence de dossiers dans le serveur principal. Pour éviter les conflits de nom avec d'autres dossiers de ressources lorsque vous renommez ou déplacez des dossiers, nous vous recommandons de donner des noms différents aux dossiers de premier niveau dans différentes arborescences.

## Remote PC Access

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Remote PC Access est une fonctionnalité de Citrix Virtual Apps and Desktops qui permet aux entreprises d'autoriser facilement leurs employés à accéder aux ressources de l'entreprise à distance et de manière sécurisée. La plate-forme Citrix rend cet accès sécurisé possible en donnant aux utilisateurs l'accès à leurs ordinateurs de bureau physiques. Si les utilisateurs peuvent accéder à leurs ordinateurs de bureau, ils peuvent accéder à toutes les applications, données et ressources dont ils ont besoin pour effectuer leur travail. Remote PC Access élimine le besoin d'introduire et de fournir d'autres outils pour permettre le télétravail. Par exemple, les bureaux virtuels ou les applications et l'infrastructure associée.

Remote PC Access utilise les composants Citrix Virtual Apps and Desktops qui fournissent des bureaux virtuels et des applications. Par conséquent, les exigences et le processus de déploiement et de configuration de Remote PC Access sont les mêmes que ceux requis pour déployer Citrix Virtual Apps and Desktops pour la mise à disposition de ressources virtuelles. Cette uniformité offre une expérience administrative cohérente et unifiée. Les utilisateurs bénéficient d'une meilleure expérience utilisateur lorsque Citrix HDX est utilisé pour fournir leur session PC de bureau.

La fonction consiste en un catalogue de machines de type **Remote PC Access** qui fournit les fonctionnalités suivantes :

- Possibilité d'ajouter des machines en spécifiant des unités d'organisation. Cette capacité facilite l'ajout de PC en bloc.
- Attribution automatique d'utilisateur en fonction de l'utilisateur qui se connecte au PC Windows de bureau. Les attributions à un seul utilisateur et à plusieurs utilisateurs sont prises en charge. Par défaut, plusieurs utilisateurs sont automatiquement attribués à la machine non attribuée suivante. Pour restreindre l'attribution automatique à un seul utilisateur, connectez-vous à Web Studio, accédez à **Paramètres** et désactivez le paramètre **Activer l'attribution automatique de plusieurs utilisateurs pour Remote PC Access**.

Citrix Virtual Apps and Desktops peut prendre en charge davantage de cas d'utilisation pour les PC physiques en utilisant d'autres types de catalogues de machines. Parmi les cas d'utilisation :

- PC Linux physiques
- PC physiques regroupés (c'est-à-dire attribués aléatoirement, non dédiés)

> **Remarques :**
>
> Pour plus d'informations sur les versions de système d'exploitation prises en charge, consultez la configuration système requise pour le VDA pour OS mono-session et Linux VDA.
>
> Pour les déploiements sur site, Remote PC Access est uniquement valide pour les licences Advanced et Premium de Citrix Virtual Apps and Desktops. Les sessions consomment des licences de la même manière que les autres sessions Citrix Virtual Desktops. Pour Citrix Cloud, Remote PC Access est valide pour Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) et Workspace Premium Plus.

### Considérations

Bien que toutes les exigences techniques et considérations qui s'appliquent à Citrix Virtual Apps and Desktops s'appliquent en général également à Remote PC Access, certaines peuvent être plus pertinentes ou limitées à l'utilisation de PC physique.

> **Important :**
>
> Les systèmes physiques Windows 11 (et certains exécutant Windows 10) incluent des fonctionnalités de sécurité basées sur la virtualisation qui font que le logiciel VDA les détecte de manière incorrecte en tant que machines virtuelles. Pour atténuer ce problème, les options suivantes s'offrent à vous :
>
> - Utiliser l'option « /physicalmachine » ainsi que l'option « /remotepc » dans le cadre de l'installation avec ligne de commande du VDA
> - Ajouter la valeur de registre suivante après l'installation du VDA si l'option susmentionnée n'a pas été utilisée

> `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
> - Nom : ForceEnableRemotePC
> - Type : DWORD
> - Données : 1

### Considérations de déploiement

Lors de la planification du déploiement de Remote PC Access, prenez quelques décisions générales.

- Vous pouvez ajouter Remote PC Access à un déploiement Citrix Virtual Apps and Desktops existant. Avant de choisir cette option, tenez compte des éléments suivants :
  - Les Delivery Controller ou Cloud Connector actuels sont-ils capables de gérer la charge supplémentaire associée aux VDA Remote PC Access ?
  - Les bases de données de site et les serveurs de base de données locaux sont-ils capables de gérer la charge supplémentaire associée aux VDA Remote PC Access ?
  - Les VDA existants et les nouveaux VDA Remote PC Access vont-ils dépasser le nombre maximal de VDA pris en charge par site ?
- Vous devez déployer le VDA sur les PC de bureau via un processus automatisé. Les options disponibles sont les suivantes :
  - Outils de distribution électronique de logiciels (ESD) tels que SCCM : Installer des VDA à l'aide de SCCM.
  - Scripts de déploiement : Installer les VDA à l'aide de scripts.
- Consultez les Considérations de sécurité Remote PC Access.

> **Remarque :**
>
> Lors de la conception de Remote PC Access, vous devez tenir compte du nombre de moniteurs physiques connectés au GPU sur le PC distant et actuellement configurés/en fonctionnement. Même si le moniteur n'est pas utilisé dans la session Citrix, mais qu'il est détecté par le GPU, la présence du moniteur est comptée dans le calcul de la limite maximale prise en charge par le GPU.

### Considérations de catalogue de machines

Le type de catalogue de machines requis dépend du cas d'utilisation :

- Catalogue de machines Remote PC Access
  - PC dédiés Windows

  - PC multi-utilisateurs dédiés Windows. Ce cas d'utilisation s'applique aux ordinateurs de bureau physiques auxquels plusieurs utilisateurs peuvent accéder à distance lors de différentes plages de travail.
  - PC Windows regroupés. Ce cas d'utilisation s'applique aux PC physiques auxquels plusieurs utilisateurs aléatoires peuvent accéder, tels que les laboratoires informatiques.

- Catalogue de machines avec OS mono-session
  - Statique - PC Linux dédiés
  - Aléatoire - PC Linux regroupés

Une fois que vous avez identifié le type de catalogue de machines, tenez compte des éléments suivants :

- Une machine peut uniquement être attribuée à un seul catalogue de machines à la fois.
- Pour simplifier l'administration déléguée, envisagez de créer des catalogues de machines en fonction de l'emplacement géographique, du département ou de tout autre regroupement qui facilite la délégation de l'administration de chaque catalogue aux administrateurs appropriés.
- Lorsque vous choisissez les unités d'organisation dans lesquelles les comptes de machine résident, sélectionnez des unités de niveau inférieur pour une plus grande granularité. Si une telle granularité n'est pas requise, vous pouvez choisir des unités de plus haut niveau. Par exemple, dans le cas d'employés de banque, sélectionnez **Guichets** pour une plus grande granularité. Sinon, vous pouvez sélectionner **Agents** ou **Banque** en fonction des besoins.
- Le déplacement ou la suppression d'unités d'organisation après leur attribution à un catalogue de machines Remote PC Access affecte les associations de VDA et entraîne des problèmes avec les attributions futures. Par conséquent, assurez-vous de planifier en conséquence afin que les mises à jour des attributions d'unité d'organisation pour les catalogues de machines soient prises en compte dans le plan de modification Active Directory.
- S'il n'est pas facile de choisir des unités d'organisation pour ajouter des machines au catalogue de machines en raison de la structure organisationnelle, vous n'avez pas à sélectionner d'unités d'organisation. Vous pouvez utiliser PowerShell pour ajouter des machines au catalogue par la suite. Les attributions automatiques d'utilisateur continuent de fonctionner si l'attribution de bureaux est correctement configurée dans le groupe de mise à disposition. Un exemple de script permettant d'ajouter des machines au catalogue de machines ainsi que des attributions d'utilisateur est disponible dans GitHub.
- Le Wake on LAN intégré est disponible uniquement avec le catalogue de machines de type **Remote PC Access**.

### Considérations sur le VDA Linux

Ces considérations sont spécifiques au VDA Linux :

- Utilisez le VDA Linux sur des machines physiques uniquement en mode non-3D. En raison de limitations sur le pilote de NVIDIA, l'écran local du PC ne peut pas être éteint et affiche les activités de la session lorsque le mode HDX 3D est activé. L'affichage de cet écran représente un risque pour la sécurité.
- Utilisez des catalogues de machines de type OS mono-session pour les machines Linux physiques.
- L'attribution automatique d'utilisateurs n'est pas disponible pour les machines Linux.
- Si les utilisateurs sont déjà connectés localement à leur PC, les tentatives de lancement des PC à partir de StoreFront échouent.
- Les options d'économie d'énergie ne sont pas disponibles pour les machines Linux.

### Configuration technique requise et considérations

Cette section contient les exigences techniques et les considérations relatives aux PC physiques.

- Les éléments suivants ne sont pas pris en charge :
  - Commutateurs KVM ou autres composants qui peuvent déconnecter une session.
  - PC hybride, y compris PC et ordinateurs portables tout en un et NVIDIA Optimus.
  - Machines à double démarrage.
- Connectez le clavier et la souris directement au PC. La connexion au moniteur ou à d'autres composants qui peuvent être désactivés ou déconnectés peut rendre ces périphériques indisponibles. Si vous devez connecter des périphériques d'entrée à des composants tels que des moniteurs, ne les éteignez pas.
- Les PC doivent être joints à un domaine des services de domaine Active Directory.
- Le démarrage sécurisé est pris en charge sous Windows 10 et Windows 11 uniquement.
- Le PC doit disposer d'une connexion réseau active. Une connexion filaire est préférable pour plus de fiabilité et de bande passante.
- Si vous utilisez le Wi-Fi, procédez comme suit :
  1. Définissez les paramètres d'alimentation pour laisser la carte sans fil allumée.
  2. Configurez la carte sans fil et le profil réseau pour autoriser la connexion automatique au réseau sans fil avant que l'utilisateur ouvre une session. Sinon, le VDA ne s'enregistre pas tant que l'utilisateur ne se connecte pas. Le PC n'est pas disponible pour l'accès à distance tant qu'un utilisateur n'a pas ouvert de session.
  3. Assurez-vous que les Delivery Controller ou Cloud Connector sont accessibles depuis le réseau Wi-Fi.

- Vous pouvez utiliser Remote PC Access sur des ordinateurs portables. Assurez-vous que l'ordinateur portable est connecté à une source d'alimentation et ne fonctionne pas sur la batterie. Configurez les options d'alimentation de l'ordinateur portable pour qu'elles correspondent à un ordinateur de bureau. Par exemple :

  1. Désactivez la fonctionnalité de veille prolongée.
  2. Désactivez la fonctionnalité de veille.
  3. Définissez l'action de fermeture de l'écran sur **Ne rien faire**.
  4. Définissez l'action d'appuyer sur le bouton d'alimentation sur **Arrêter**.
  5. Désactivez les fonctionnalités d'économie d'énergie de la carte vidéo et de la carte réseau.

- Remote PC Access est pris en charge sur les Surface Pro avec Windows 10. Suivez les mêmes directives pour les ordinateurs portables mentionnés précédemment.

- Si vous utilisez une station d'accueil, vous pouvez ancrer et retirer les ordinateurs portables. Lorsque vous retirez l'ordinateur portable, le VDA se réenregistre auprès des Delivery Controller ou Cloud Connector via Wi-Fi. Toutefois, lorsque vous reconnectez l'ordinateur portable, le VDA ne bascule pas pour utiliser la connexion filaire, sauf si vous déconnectez la carte sans fil. Certains périphériques proposent des fonctionnalités intégrées pour déconnecter la carte sans fil lors de l'établissement d'une connexion filaire. Les autres périphériques nécessitent des solutions personnalisées ou des utilitaires tiers pour déconnecter la carte sans fil. Prenez en compte les considérations relatives au Wi-Fi mentionnées précédemment.

  Procédez comme suit pour activer l'ancrage et le retrait pour les périphériques Remote PC Access :

  1. Dans le menu **Démarrer**, sélectionnez **Paramètres > Système > Alimentation et mise en veille** et définissez **Mettre en veille** sur **Jamais**.
  2. Sous **Gestionnaire de périphériques > Cartes réseau > Carte Ethernet**, accédez à **Gestion de l'alimentation** et désactivez **Autoriser l'ordinateur à éteindre ce périphérique pour économiser de l'énergie** . Vérifiez que l'option **Autoriser ce périphérique à sortir l'ordinateur du mode veille** est cochée.

- Plusieurs utilisateurs avec l'accès au même PC de bureau voient la même icône dans Citrix Workspace. Lorsqu'un utilisateur ouvre une session sur Citrix Workspace, cette ressource apparaît comme indisponible si elle est déjà utilisée par un autre utilisateur.

- Installez l'application Citrix Workspace sur chaque machine cliente (par exemple, un PC personnel) qui accède au PC de bureau.

### Séquence de configuration

Cette section contient une vue d'ensemble de la configuration de Remote PC Access lors de l'utilisation du catalogue de machines de type **Remote PC Access**. Pour plus d'informations sur la création

d'autres types de catalogues de machines, reportez-vous à la section Créer des catalogues de machines.

1. Site local uniquement : pour utiliser la fonction Wake on LAN intégrée, configurez les prérequis décrits dans Wake on LAN.
2. Si un nouveau site Citrix Virtual Apps and Desktops a été créé pour Remote PC Access :

   a) Sélectionnez le type de site **Remote PC Access**.
   b) Sur la page **Gestion de l'alimentation**, vous choisir de activer ou de désactiver la gestion de l'alimentation pour le catalogue de machines Remote PC Access par défaut. Vous pouvez modifier ce paramètre ultérieurement en modifiant les propriétés du catalogue de machines. Pour plus d'informations sur la configuration de Wake on LAN, reportez-vous à la section Wake on LAN.
   c) Complétez les informations sur les pages **Utilisateurs** et **Comptes de machines**.

   L'exécution de ces étapes crée un catalogue de machines nommé **Machines Remote PC Access** et un groupe de mise à disposition nommé **Bureaux Remote PC Access**.
3. Si vous ajoutez à un site Citrix Virtual Apps and Desktops existant :

   a) Créez un catalogue de machines de type **Remote PC Access** (page Système d'exploitation de l'assistant). Pour plus d'informations sur la création d'un catalogue de machines, voir Création de catalogues de machines. Assurez-vous d'attribuer l'unité d'organisation correcte afin que les PC cibles soient mis à disposition pour une utilisation avec Remote PC Access.
   b) Créez un groupe de mise à disposition pour permettre aux utilisateurs d'accéder aux PC du catalogue de machines. Pour plus d'informations sur la création d'un groupe de mise à disposition, voir Créer un groupe de mise à disposition. Assurez-vous d'attribuer le groupe de mise à disposition à un groupe Active Directory qui contient les utilisateurs ayant besoin d'accéder à leurs PC.
4. Déployez le VDA sur les PC de bureau.

   - Nous vous recommandons d'utiliser le programme d'installation VDA principal pour OS mono-session (VDAWorkstationCoreSetup.exe).
   - Vous pouvez également utiliser le programme d'installation VDA complet mono-session (VDAWorkstationSetup.exe) avec l'option `/remotepc/physicalmachine`, qui obtient le même résultat que l'utilisation du programme d'installation VDA principal.

     > **Remarque :**
     >
     > Pour une installation RemotePC, utilisez l'argument `/physicalmachine` avec `/remotepc` pour le VDA afin que le VDA se comporte comme prévu dans certains scé-

> narios utilisateur.

- Envisagez d'activer l'assistance à distance Windows pour permettre aux équipes du centre d'assistance de fournir un support à distance via Citrix Director. Pour ce faire, utilisez l'option `/enable_remote_assistance`. Consultez la section Installer à l'aide de la ligne de commande pour plus de détails.
- Pour afficher les informations sur la durée d'ouverture de session dans Director, vous devez utiliser le programme d'installation complet du VDA mono-session et inclure le composant **Citrix User Profile Management WMI Plugin**. Pour inclure ce composant, utilisez l'option `/includeadditional`. Consultez la section Installer à l'aide de la ligne de commande pour plus de détails.
- Pour plus d'informations sur le déploiement du VDA à l'aide de SCCM, reportez-vous à la section Installer des VDA à l'aide de SCCM.
- Pour plus d'informations sur le déploiement du VDA via des scripts de déploiement, voir Installer des VDA à l'aide de scripts.

Après avoir terminé avec succès les étapes 2 à 4, les utilisateurs sont automatiquement attribués à leurs propres machines lorsqu'ils se connectent localement sur les PC.

5. Demandez aux utilisateurs de télécharger et d'installer l'application Citrix Workspace sur chaque machine cliente qu'ils utilisent pour accéder au PC de bureau à distance. L'application Citrix Workspace est disponible depuis `https://www.citrix.com/downloads/` ou depuis les magasins d'applications pour appareils mobiles.

## Fonctions gérées via le registre

> **Attention :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

### Désactiver les attributions automatiques de plusieurs utilisateurs

Sur chaque Delivery Controller, ajoutez le paramètre de Registre suivant :

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- Nom : AllowMultipleRemotePCAssignments

- Type : DWORD
- Données : 0

#### Mode veille (version minimum 7.16)

Pour permettre à une machine Remote PC Access de passer en état de veille, ajoutez ce paramètre de registre sur le VDA, puis redémarrez la machine. Après le redémarrage, les paramètres d'économie d'énergie du système d'exploitation sont respectés. La machine passe en mode veille après le temps d'inactivité configuré. Une fois la machine réveillée, elle se réenregistre auprès du Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nom : DisableRemotePCSleepPreventer
- Type : DWORD
- Données : 1

#### Gestion des sessions

Par défaut, une session d'utilisateur distant est automatiquement déconnectée lorsqu'un utilisateur local initie une session sur cette machine (en appuyant sur CTRL+ALT+Suppr). Pour éviter cette action automatique, ajoutez l'entrée de registre suivante sur le PC de bureau, puis redémarrez la machine.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nom : SasNotification
- Type : DWORD
- Données : 1

Par défaut, l'utilisateur distant a priorité sur l'utilisateur local lorsque le message de connexion n'est pas confirmé dans le délai d'expiration. Pour configurer le comportement, utilisez ce paramètre :

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nom : RpcaMode
- Type : DWORD
- Données :
  - 1 = L'utilisateur distant a toujours priorité s'il ne répond pas à l'interface utilisateur de messagerie dans le délai imparti. Ce comportement est le comportement par défaut si ce paramètre n'est pas configuré.
  - 2 = L'utilisateur local a priorité.

Le délai d'expiration du mode Remote PC Access est de 30 secondes par défaut. Vous pouvez configurer ce délai d'expiration mais ne le définissez pas sur une valeur inférieure à 30 secondes. Pour configurer le délai d'expiration, utilisez ce paramètre de Registre :

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nom : RpcaTimeout
- Type : DWORD
- Données : nombre de secondes pour le délai d'expiration en valeurs décimales

Lorsque l'utilisateur souhaite forcer l'accès à la console : l'utilisateur local peut appuyer sur Ctrl+Alt+Suppr à deux reprises à intervalle de 10 secondes pour obtenir le contrôle local d'une session distante et forcer une déconnexion.

Une fois le Registre modifié et la machine redémarrée, si un utilisateur local appuie sur Ctrl+Alt+Suppr pour ouvrir une session sur ce PC lorsqu'il est en cours d'utilisation par un utilisateur distant, cet utilisateur reçoit une invite lui demandant s'il souhaite autoriser. L'invite demande si la connexion de l'utilisateur local doit être autorisée ou refusée. L'action d'autorisation de la connexion déconnecte la session de l'utilisateur distant.

## Journalisation de la gestion des sessions

Remote PC Access possède désormais des fonctionnalités de journalisation qui indiquent lorsqu'un utilisateur tente d'accéder à un PC avec une session ICA active. Cela vous permet de surveiller votre environnement afin d'identifier toute activité indésirable ou inattendue, et de pouvoir auditer ces événements si vous devez examiner des incidents.

Les événements sont enregistrés à l'aide de l'Observateur d'événements Windows et se trouvent dans **Applications et services > Citrix > HostCore > Service ICA > Admin**.

Trois événements distincts sont enregistrés lors de l'utilisation de Remote PC Access.

### Événement Ctrl+Alt+Suppr

Cet événement apparaît lorsque l'utilisateur local appuie sur Ctrl+Alt+Suppr sur le clavier de la console avec une session distante active.

### Détails de l'événement

- Nom du journal : Application et services
- ID d'événement : 43, 44, 45
- Source : Service ICA

**ID d'événement 43** Cet ID d'événement s'affiche lorsque la valeur de registre SasNotification n'existe pas ou lorsque la valeur de registre SasNotification est 0.

- Message :

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to automatically
               disconnect the remote session.
```

**ID d'événement 44** Cet ID d'événement s'affiche lorsque la valeur de registre SasNotification est 1 et que la valeur de registre RpcaMode est 1 ou que la valeur de registre RpcaMode n'existe pas.

- Message :

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to notify the
               remote user. The user preference is set to remote user
               .
```

**ID d'événement 45** Cet ID d'événement s'affiche lorsque la valeur de registre SasNotification est 1 et la valeur de registre RpcaMode est 2.

- Message :

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to notify the
               remote user.
3          The user preference is set to local user.
```

#### Événement de déconnexion de la session distante

Cet événement se produit lorsque la session distante a été déconnectée pour diverses raisons.

#### Détails de l'événement

- Nom du journal : Application et services
- ID d'événement : 46, 47, 48
- Source : Service ICA

**ID d'événement 46** Cet ID d'événement s'affiche lorsque la session distante a été déconnectée et lorsque la valeur de registre SasNotification n'existe pas ou que la valeur de registre SasNotification est 0.

- Message :

```
1          The remote session for <remoteUserName> has been
               disconnected.
```

**ID d'événement 47** Cet ID d'événement apparaît lorsque l'utilisateur distant accepte de déconnecter la session, et lorsque la valeur de registre SasNotification est 1 et que la valeur de registre RpcaMode est 1 ou que la valeur de registre RpcaMode est 2 ou que la valeur de registre RpcaMode n'existe pas.

- Message :

```
The remote session for <remoteUserName> has been
   disconnected because the user accepted the request to
   disconnect the session.
```

**ID d'événement 48** Cet ID d'événement s'affiche lorsque l'utilisateur distant ne refuse pas la demande de déconnexion dans le délai d'expiration spécifique, et lorsque la valeur de registre SasNotification est 1 et la valeur de registre RpcaMode est 2.

- Message :

```
The remote session for <remoteUserName> has been
   disconnected because the user did not decline the
   disconnection request within the configured timeout
   period (<timeout period>).
```

**Événement Ctrl+Alt+Suppr sélectionné deux fois** Cet événement apparaît lorsqu'un utilisateur appuie deux fois sur Ctrl+Alt+Suppr dans les 10 secondes.

#### Détails de l'événement

- Nom du journal : Application et services
- ID d'événement : 49
- Source : Service ICA

**ID d'événement 49** Cet ID d'événement apparaît lorsqu'un utilisateur appuie deux fois sur Ctrl+Alt+Suppr dans les 10 secondes.

- Message :

```
The remote session for <remoteUserName> has been forcibly
    disconnected.
```

### Wake on LAN

Remote PC Access prend en charge Wake on LAN, qui donne aux utilisateurs la possibilité d'activer des ordinateurs physiques à distance. Cette fonctionnalité permet aux utilisateurs de garder leur PC

de bureau éteint lorsqu'il n'est pas en cours d'utilisation, et d'économiser de l'énergie. Elle offre également un accès distant quand une machine a été éteinte par inadvertance.

Avec la fonction Wake on LAN, les paquets magiques sont envoyés directement à partir du VDA exécuté sur le PC vers le sous-réseau dans lequel réside le PC selon les instructions du Delivery Controller. Cela permet à la fonction d'opérer sans dépendances sur des composants d'infrastructure supplémentaires ou des solutions tierces pour la mise à disposition de paquets magiques.

La fonction Wake on LAN diffère de la fonction Wake on LAN d'ancienne génération basée sur SCCM. Pour plus d'informations sur la fonction Wake on LAN basée sur SCCM, consultez Fonction Wake on LAN intégrée à SCCM.

#### Configuration système requise

Vous trouverez ci-dessous la configuration système requise pour l'utilisation de la fonction Wake on LAN :

- Plan de contrôle :
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 ou version ultérieure
- PC physiques :
  - VDA version 2009 ou ultérieure
  - Windows 10 ou Windows 11. Pour plus d'informations sur la prise en charge, consultez la configuration système requise pour le VDA.
  - Wake on LAN activé dans BIOS/UEFI
  - Wake on LAN activé dans les propriétés de la carte réseau dans la configuration Windows

#### Configurer Wake on LAN

Si vous utilisez Citrix Virtual Apps and Desktops sur site, la configuration de Wake on LAN intégré est uniquement prise en charge avec PowerShell.

Pour configurer Wake on LAN :

1. Créez le catalogue de machines Remote PC Access si vous n'en avez pas déjà.
2. Créez la connexion hôte Wake on LAN si vous n'en avez pas déjà.

> **Remarque :**
>
> Pour utiliser la fonction Wake on LAN, si vous disposez d'une connexion hôte du type « Microsoft Configuration Manager Wake on LAN », créez une nouvelle connexion hôte.

3. Récupérez l'identifiant unique de la connexion hôte Wake on LAN.
4. Associez la connexion hôte Wake on LAN à un catalogue de machines.

Pour créer la connexion hôte Wake on LAN :

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "*citrix*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                   >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
   $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
       $hypHc.HypervisorConnectionUid
 }

<!--NeedCopy-->
```

Lorsque la connexion hôte est prête, exécutez les commandes suivantes pour récupérer l'identifiant unique de la connexion hôte :

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
<!--NeedCopy-->
```

Après avoir récupéré l'identifiant unique de la connexion, exécutez les commandes suivantes pour associer la connexion au catalogue de machines Remote PC Access :

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
   RemotePCHypervisorConnectionUid $hypUid
<!--NeedCopy-->
```

### Considérations relatives à la conception

Lorsque vous envisagez d'utiliser Wake on LAN avec Remote PC Access, tenez compte des points suivants :

- Plusieurs catalogues de machines peuvent utiliser la même connexion hôte Wake on LAN.
- Pour qu'un PC réveille un autre PC, les deux PC doivent se trouver dans le même sous-réseau et utiliser la même connexion hôte Wake on LAN, qu'ils soient dans les mêmes catalogues de machines ou non.
- Les connexions hôtes sont affectées à des zones spécifiques. Si votre déploiement contient plusieurs zones, vous avez besoin d'une connexion hôte Wake on LAN dans chaque zone. Il en va de même pour les catalogues de machines.
- Les paquets magiques sont diffusés à l'aide de l'adresse de diffusion globale 255.255.255.255. Assurez-vous que l'adresse n'est pas bloquée.
- Il doit y avoir au moins un PC allumé dans le sous-réseau - pour chaque connexion Wake on LAN - pour pouvoir réveiller les machines de ce sous-réseau.

### Considérations opérationnelles

Les considérations suivantes sont à prendre en compte lors de l'utilisation de la fonctionnalité Wake on LAN :

- Le VDA doit s'enregistrer au moins une fois avant que le PC puisse être réveillé à l'aide de la fonction Wake on LAN intégrée.
- La fonction Wake on LAN ne peut être utilisée que pour réveiller les PC. Elle ne prend pas en charge d'autres actions d'alimentation, telles que le redémarrage ou l'arrêt.
- Une fois la connexion Wake on LAN créée, elle est visible dans Web Studio. Toutefois, la modification de ses propriétés dans Web Studio n'est pas prise en charge si vous utilisez Citrix Virtual Apps and Desktops sur site.
- Les paquets magiques sont envoyés de l'une des deux manières suivantes :

    1. Lorsqu'un utilisateur tente de lancer une session sur son PC et que le VDA n'est pas enregistré
    2. Lorsqu'un administrateur envoie manuellement une commande de mise sous tension à partir de Web Studio ou PowerShell

- Comme le Delivery Controller ne connaît pas l'état d'alimentation d'un PC, Web Studio affiche **Non pris en charge** sous l'état d'alimentation. Le Delivery Controller utilise donc l'état d'enregistrement du VDA pour déterminer si un PC est allumé ou éteint.

## Fonction Wake on LAN intégrée à SCCM

La fonction Wake on LAN intégrée à SCCM est une option alternative Wake on LAN pour Remote PC Access qui n'est disponible qu'avec une instance Citrix Virtual Apps and Desktops locale.

### Configuration système requise

Vous trouverez ci-dessous la configuration système requise pour l'utilisation de la fonction Wake on LAN intégrée à SCCM :

- Citrix Virtual Apps and Desktops 1912 ou versions ultérieures
- PC physiques :
  - VDA version 1912 ou ultérieure.
  - Windows 10. Pour plus d'informations sur la prise en charge, consultez la configuration système requise pour le VDA.
  - Wake on LAN activé dans BIOS/UEFI
  - Wake on LAN activé dans les propriétés de la carte réseau dans la configuration Windows
- System Center Configuration Manager (SCCM) 2012 R2 ou version ultérieure

### Configurer la fonction Wake on LAN intégrée à SCCM

Remplissez les conditions préalables suivantes :

1. Configurez SCCM 2012 R2, 2016 ou 2019 au sein de l'organisation. Déployez ensuite le client SCCM sur toutes les machines Remote PC Access, tout en allouant un délai suffisant pour l'exécution du cycle d'inventaire SCCM programmé ou en forcer un manuellement, si nécessaire.
2. Pour la prise en charge de Wake Proxy, activez l'option dans SCCM. Pour chaque sous-réseau de l'organisation contenant les PC qui utiliseront la fonctionnalité Remote PC Access Wake on LAN, vérifiez que trois machines ou plus peuvent servir de machines sentinelles.
3. Pour une prise en charge de paquet magique, configurez des routeurs réseau et des pare-feu pour autoriser l'envoi des paquets magiques, en utilisant soit une diffusion dirigée vers un sous-réseau, soit une monodiffusion.
4. Configurez Wake on LAN dans chacun des paramètres BIOS/UEFI du PC.
5. Déployez le VDA sur les PC physiques si vous ne l'avez pas déjà fait.

Après avoir rempli les conditions préalables, procédez comme suit pour permettre au Delivery Controller de communiquer avec SCCM :

1. Créez une connexion hôte pour SCCM. Pour de plus amples informations, consultez les articles Connexions et ressources.

- Sélectionnez **Microsoft Configuration Manager Wake on LAN** comme type de connexion.
- Les informations d'identification entrées doivent avoir accès aux collections de l'étendue et doivent disposer du rôle **Opérateur des outils distants**.

2. Sélectionnez la connexion dans Web Studio, puis sélectionnez **Modifier la connexion**, puis cliquez sur **Avancé**.
3. Sélectionnez l'option appropriée pour gérer Wake on LAN :

   - Si vous utilisez le proxy de mise en éveil, sélectionnez la première option : **Proxy de mise en éveil Microsoft System Center Configuration Manager**.
   - Si vous utilisez des paquets magiques, sélectionnez la deuxième option : **Paquets Wake On LAN transmis par Delivery Controller**.
     - Sélectionnez la méthode de transmission appropriée : **Diffusions dirigées vers le sous-réseau** ou **Monodiffusion**.

Après avoir créé la connexion hôte, associez la connexion à un catalogue Remote PC Access :

- Si vous créez un catalogue Remote PC Access, sur la page **Système d'exploitation** de l'assistant de création de catalogues, sélectionnez **Remote PC Access** comme type de catalogue et choisissez la connexion appropriée dans la liste déroulante.
- Pour ajouter Wake on LAN à un catalogue Remote PC Access existant :

  1. Accédez au nœud **Catalogues de machines** dans Web Studio, sélectionnez le catalogue de machines, puis sélectionnez **Modifier le catalogue de machines**.
  2. Sélectionnez l'onglet **Gestion de l'alimentation** et choisissez **Oui** pour activer la gestion de l'alimentation du catalogue de machines.
  3. Sélectionnez la connexion appropriée dans la liste déroulante et cliquez sur **OK**.

## Dépannage

### Le vidage de l'écran ne fonctionne pas

Si l'écran local du PC Windows n'est pas vide alors qu'une session HDX est active (l'écran local affiche ce qui se passe dans la session), cela est probablement dû à des problèmes avec le pilote du fournisseur de la carte graphique. Pour résoudre le problème, attribuez au pilote Citrix Indirect Display (IDD) une priorité plus élevée que le pilote fournisseur de la carte graphique en définissant la valeur de Registre suivante :

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nom : CitrixIDD
- Type : DWORD
- Données : 3

Pour plus d'informations sur les priorités des cartes graphiques et la création des écrans, consultez l'article du Centre de connaissances CTX237608.

#### La session se déconnecte lorsque vous sélectionnez Ctrl+Alt+Suppr sur la machine sur laquelle la notification de gestion de session est activée

La notification de gestion de session contrôlée par la valeur de registre **SasNotification** ne fonctionne que lorsque le mode Remote PC Access est activé sur le VDA. Si le rôle Hyper-V ou toute fonctionnalité de sécurité basée sur la virtualisation est activée sur le PC physique, le PC est signalé comme machine virtuelle. Si le VDA détecte qu'il est en cours d'exécution sur une machine virtuelle, il désactive automatiquement le mode Remote PC Access. Pour activer le mode Remote PC Access, ajoutez la valeur de registre suivante :

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nom : ForceEnableRemotePC
- Type : DWORD
- Données : 1

Redémarrez le PC pour que le paramètre prenne effet.

#### Informations de diagnostic

Les informations de diagnostic sur Remote PC Access sont écrites dans le Journal d'événements d'application Windows. Les messages d'informations ne sont pas optimisés. Les messages d'erreur sont optimisés en éliminant les messages en double.

- 3300 (informations) : machine ajoutée au catalogue
- 3301 (informations) : machine ajoutée au groupe de mise à disposition
- 3302 (informations) : machine attribuée à l'utilisateur
- 3303 (erreur) : exception

#### Gestion de l'alimentation

Lorsque la gestion de l'alimentation est activée pour Remote PC Access, il se peut que des diffusions dirigées par des sous-réseaux ne parviennent pas à démarrer des machines qui sont situées sur un sous-réseau différent du Controller. Si vous avez besoin de la gestion de l'alimentation sur les sous-réseaux utilisant des diffusions dirigées par des sous-réseaux et AMT n'est pas disponible, essayez la méthode du proxy de mise en éveil ou de monodiffusion. Assurez-vous que ces paramètres sont activés dans les propriétés avancées de la connexion de gestion de l'alimentation.

#### La session distante active enregistre la saisie sur l'écran tactile local

Lorsque le VDA active le mode Remote PC Access, la machine ignore la saisie sur l'écran tactile local pendant une session active. Si le rôle Hyper-V ou toute fonctionnalité de sécurité basée sur la virtualisation est activée sur le PC physique, le PC est signalé comme machine virtuelle. Si le VDA détecte qu'il est en cours d'exécution sur une machine virtuelle, il désactive automatiquement le mode Remote PC Access. Pour activer le mode Remote PC Access, ajoutez le paramètre de registre suivant :

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nom : ForceEnableRemotePC
- Type : DWORD
- Données : 1

Redémarrez le PC pour que le paramètre prenne effet.

### Plus de ressources

Autres ressources pour Remote PC Access :

- Conseils de conception de la solution : Décisions de conception Remote PC Access.
- Exemples d'architectures Remote PC Access :Architecture de référence pour la solution Citrix Remote PC Access.

## Publier du contenu

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Vous pouvez publier une application qui est simplement une URL ou un chemin UNC vers une ressource, par exemple un document Microsoft Word ou un lien web. Cette fonctionnalité est appelée contenu publié. La possibilité de publier du contenu offre davantage de souplesse pour livrer le contenu aux utilisateurs. Vous bénéficiez du contrôle d'accès et de la gestion des applications existants. Vous pouvez également spécifier s'il est nécessaire d'utiliser des applications locales ou publiées pour ouvrir le contenu.

Le contenu publié apparaît comme les autres applications de StoreFront et de l'application Citrix Workspace. Les utilisateurs y accèdent de la même manière qu'ils accèdent aux applications. Sur le client, la ressource s'ouvre comme d'habitude.

- Si une application installée localement est appropriée, elle est lancée pour ouvrir la ressource.
- Si une association de type de fichier a été définie, une application publiée est lancée pour ouvrir la ressource.

Vous publiez contenu à l'aide du SDK PowerShell. Vous ne pouvez pas utiliser Web Studio pour publier le contenu. Cependant, vous pouvez utiliser Web Studio pour modifier les propriétés d'application plus tard, après leur publication.

### Présentation et préparation de la configuration

La publication de contenu utilise l'applet de commande `New-BrokerApplication` avec les principales propriétés suivantes. (Reportez-vous à l'aide de l'applet de commande pour obtenir une description de toutes les propriétés de l'applet de commande).

```
1 New-BrokerApplication –ApplicationType PublishedContent -
     CommandLineExecutable location -Name app-name -DesktopGroup delivery
     -group-name
2 <!--NeedCopy-->
```

La propriété `ApplicationType` doit être `PublishedContent`.

La propriété `CommandLineExecutable` spécifie l'emplacement du contenu publié. Les formats suivants sont pris en charge, avec une limite de 255 caractères.

- adresse de site Web HTML (http://www.citrix.com, par exemple) ;
- fichier de document sur un serveur Web (`https://www.citrix.com/press/pressrelease.doc`, par exemple) ;
- répertoire sur un serveur FTP (`ftp://ftp.citrix.com/code`, par exemple) ;
- fichier de document sur un serveur FTP (`ftp://ftp.citrix.com/code/Readme.txt`, par exemple) ;
- chemin de répertoire UNC (`file://myServer/myShare or \\\\\myServer\\myShare`, par exemple) ;
- chemin de fichier UNC (`file://myServer/myShare/myFile.asf` ou `\\myServer\myShare\myFile.asf`, par exemple).

Assurez-vous que vous disposez du kit de développement logiciel correct.

- Pour les déploiements des services Citrix DaaS (anciennement Citrix Virtual Apps and Desktops), téléchargez et installez le SDK Citrix Virtual Apps and Desktops Remote PowerShell.

- Pour les déploiements sur site Citrix Virtual Apps and Desktops, utilisez le SDK PowerShell qui est installé avec le Delivery Controller. L'ajout d'une application avec contenu publié requiert une version minimale de 7.11 pour le Delivery Controller.

Les procédures suivantes utilisent des exemples. Dans les exemples :

- Un catalogue de machines a été créé.
- Un groupe de mise à disposition nommé `PublishedContentApps` a été créé. Le groupe utilise une machine avec OS multi-session du catalogue. L'application WordPad a été ajoutée au groupe.
- Les attributions sont effectuées pour le nom du groupe de mise à disposition, l'emplacement de `CommandLineExecutable` et le nom de l'application.

### Prise en main

Sur la machine contenant le SDK PowerShell, ouvrez PowerShell.

L'applet de commande suivante ajoute le composant logiciel enfichable SDK PowerShell approprié et attribue l'enregistrement de groupe de mise à disposition renvoyé.

```
Add-PsSnapin Citrix\* $dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

Si vous utilisez Citrix DaaS, authentifiez-vous en saisissant vos informations d'identification Citrix Cloud. S'il y a plusieurs clients, choisissez-en un.

#### Publier une URL

Après avoir affecté l'emplacement et le nom de l'application, l'applet de commande suivante publie la page d'accueil Citrix comme application.

```
1 $citrixUrl = "https://www.citrix.com/"
2 $appName = "Citrix Home Page"
3
4 New-BrokerApplication –ApplicationType PublishedContent –
     CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.
     Uid
5 <!--NeedCopy-->
```

Vérifiez si la commande a réussi :

- Ouvrez StoreFront et connectez-vous en tant qu'utilisateur qui peut accéder à des applications dans le groupe de mise à disposition PublishedContentApps. L'affichage inclut l'application nouvellement créée avec l'icône par défaut. Pour en savoir plus sur la personnalisation de l'

icône, voir https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-xd7/.

- Cliquez sur l'application **Citrix Home Page**. L'URL s'ouvre dans un nouvel onglet dans une instance locale de votre navigateur par défaut.

### Publier des ressources situées sur des chemins UNC

Dans cet exemple, l'administrateur a déjà créé un partage nommé `PublishedResources`. Après avoir affecté les emplacements et les noms d'application, les applets de commande suivantes publient un fichier RTF et un fichier DOCX dans ce partage en tant que ressource.

```
$rtfUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx
    "
$docxAppName = "PublishedDOCX"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
<!--NeedCopy-->
```

Vérifiez si la commande a réussi :

- Actualisez votre fenêtre StoreFront pour voir les documents publiés récemment.
- Cliquez sur les applications **PublishedRTF** et **PublishedDOCX**. Chaque document s'ouvre dans un WordPad en cours d'exécution au niveau local.

### Afficher et modifier les applications PublishedContent

Vous gérez le contenu publié à l'aide des méthodes que vous utilisez pour les autres types d'applications.

Pour afficher et modifier des applications `PublishedContent`, procédez comme suit :

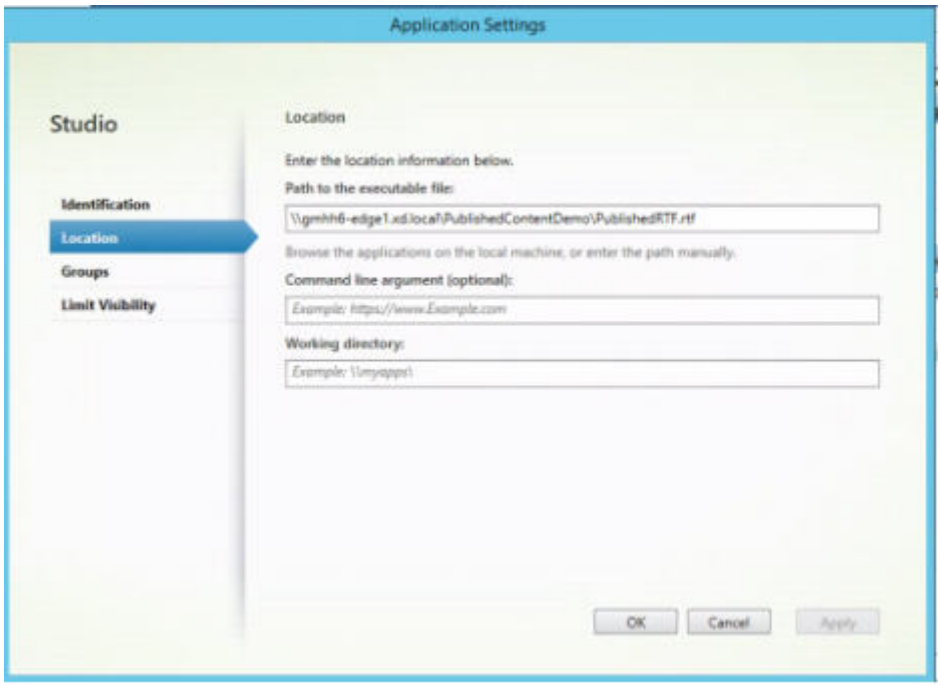
1. Connectez-vous à Web Studio et sélectionnez **Applications** dans le volet de gauche.
2. Dans l'onglet **Applications**, sélectionnez une application PublishedContent, puis sélectionnez **Propriétés**.

   Les propriétés de l'application (par exemple, la visibilité de l'utilisateur, l'association de groupe et le raccourci) s'appliquent au contenu publié. Cependant, vous ne pouvez pas modifier les

propriétés d'argument de ligne de commande ou de répertoire de travail sur la page **Emplacement**.

3. Pour modifier la ressource, modifiez le champ **Chemin d'accès au fichier exécutable** sur cette page.

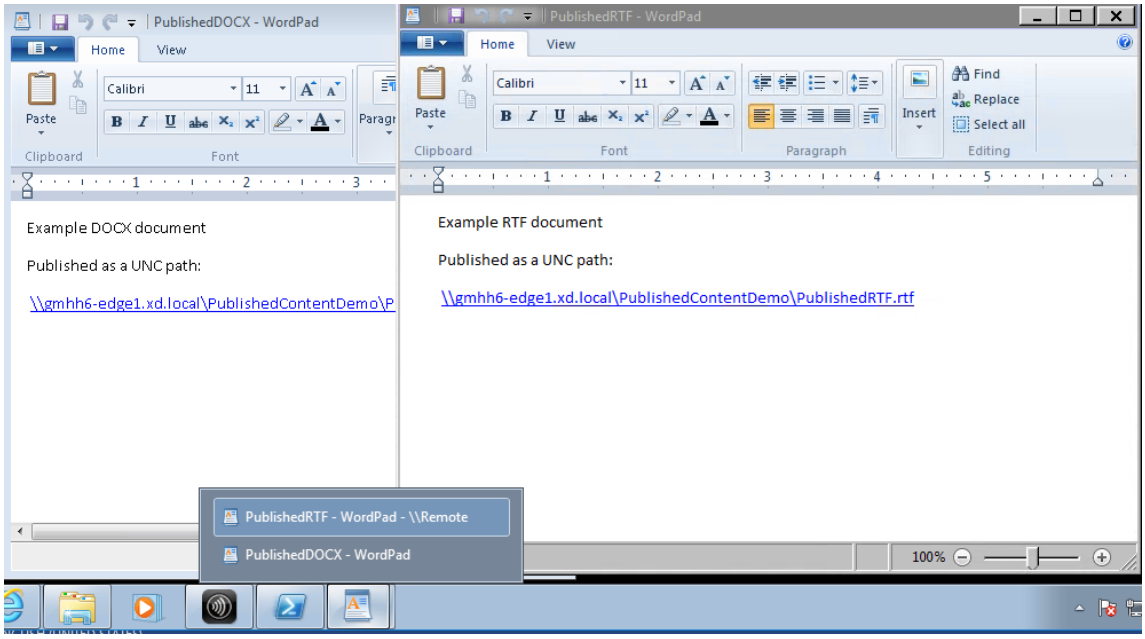



4. Pour utiliser une application publiée pour ouvrir une application `PublishedContent` (plutôt qu'une application locale), procédez comme suit :

   Dans cet exemple, l'application WordPad publiée est modifiée pour créer une association de type de fichier pour les fichiers .rtf.

   a) Activez le mode de maintenance pour le groupe de mise à disposition.
   b) Modifiez la propriété **Association de type de fichier**.
   c) Désactivez le mode maintenance lorsque vous avez terminé.
   d) Actualisez StoreFront pour charger les modifications apportées à l'association de type de fichier, puis cliquez sur les applications **PublishedRTF** et **PublishedDOCX**. Notez la différence. **PublishedDOCX** s'ouvre encore dans le WordPad local. Cependant, **PublishedRTF** s'ouvre maintenant dans le WordPad publié en raison de l'association de type de fichier.




### Pour plus d'informations

- Créer des catalogues de machines
- Créer des groupes de mise à disposition
- Modifier les propriétés d'une application

## Server VDI

June 27, 2024

Utilisez la fonctionnalité Server VDI (Virtual Desktop Infrastructure) pour mettre à disposition un bureau depuis un système d'exploitation serveur vers un utilisateur unique.

- Les administrateurs d'entreprise peuvent mettre à disposition des systèmes d'exploitation serveur en tant que bureaux VDI, ce qui peut être utile pour les utilisateurs tels que les ingénieurs et les concepteurs.
- Les fournisseurs de service peuvent offrir des bureaux depuis le cloud. Ces bureaux sont conformes avec Microsoft Services Provider License Agreement (SPLA).

Assistance :

- Dans les déploiements du service Citrix Virtual Apps and Desktops et de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops), Server VDI est pris en charge sur Windows Server 2022, Windows Server 2019 et Windows Server 2016.

- Tous les déploiements Server VDI prennent en charge la technologie de couche de personnalisation utilisateur.
- Pour que Server VDI fonctionne avec des périphériques TWAIN tels que des scanners, la fonctionnalité Expérience utilisateur de Windows Server doit être installée.
- Les fonctionnalités suivantes ne peuvent pas être utilisées avec Server VDI :
  - Applications hébergées
  - Local App Access
  - Connexions de bureau directes (sans broker)
  - Remote PC Access

### Installer et configurer Server VDI

1. Préparez le serveur Windows en vue de l'installation.
   - Utilisez le Gestionnaire de serveur Windows pour vous assurer que les services de rôle des services Bureau à distance ne sont pas installés. Supprimez-les si précédemment installés. L'installation de VDA échoue si ces services de rôle sont installés.
   - Assurez-vous que la propriété **Restreindre chaque utilisateur à une seule session** est activée. Sur le serveur Windows, modifiez le Registre pour Terminal Server :

     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`

     `DWORD fSingleSessionPerUser = 1`
2. Utilisez l'interface de ligne de commande du programme d'installation Citrix Virtual Apps and Desktops pour installer un VDA sur un serveur pris en charge ou sur une image principale de serveur, en spécifiant les options `/quiet` et `/servervdi` : (Par défaut, l'interface graphique du programme d'installation bloque le VDA avec OS mono-session Windows sur un système d'exploitation de serveur. La ligne de commande ignore ce comportement.) Utilisez l'une des commandes suivantes :
   - Déploiements de Citrix Virtual Apps and Desktops :
     - `XenDesktopVdaSetup.exe /quiet /servervdi`
     - `VDAWorkstationSetup.exe /quiet /servervdi`
   - Déploiements de Citrix DaaS :
     - `VDAWorkstationSetup.exe /quiet /servervdi`

   Autres options :
   - Utilisez `/controllers` pour spécifier des Delivery Controller ou des Cloud Connector.

- Utilisez /`enable_hdx_ports` pour ouvrir des ports dans le pare-feu, sauf si le pare-feu doit être configuré manuellement.
- Utilisez /`mastermcsimage` (ou /`masterimage`) si vous installez le VDA sur une image, et que vous allez utiliser MCS pour créer des VM de serveur depuis cette image.
- Consultez la section Installer à l'aide de la ligne de commande pour plus de détails sur toutes les options.

3. Créez un catalogue de machines pour Server VDI. Dans l'assistant de création de catalogues :

   - Sur la page **Système d'exploitation**, sélectionnez **OS mono-session**.
   - Sur la page **Résumé**, spécifiez un nom de catalogue de machines et une description pour les administrateurs qui l'identifient clairement en tant que Server VDI. C'est le seul indicateur dans Studio que le catalogue prend en charge Server VDI.

   Lors de l'utilisation de la fonction de recherche dans Studio, le catalogue Server VDI s'affichera sur la page de l'onglet **Machines avec OS mono-session**, même si le VDA est installé sur une machine multi-session.

4. Créez un groupe de mise à disposition et sélectionnez le catalogue Server VDI que vous avez créé.

Si vous n'avez pas spécifié de Delivery Controller ou de Cloud Connector lors de l'installation du VDA, n'oubliez pas de les spécifier ultérieurement. Consultez la section Enregistrement de VDA pour plus de détails.

## Couche de personnalisation de l'utilisateur

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

La fonctionnalité de couche de personnalisation utilisateur pour Citrix Virtual Apps and Desktops étend les fonctionnalités des catalogues de machines non persistants afin de préserver les données des utilisateurs et les applications installées localement pour toutes les sessions. Optimisée par la technologie Citrix App Layering sous-jacente, la fonctionnalité de couche de personnalisation des utilisateurs fonctionne avec Citrix Provisioning et Machine Creation Services (MCS) dans un catalogue de machines non persistant.

Les composants de la fonctionnalité de couche de personnalisation des utilisateurs sont installés avec Virtual Delivery Agent dans l'image principale. Un fichier VHD stocke localement les applications installées par l'utilisateur. Le disque dur virtuel monté sur l'image agit comme disque dur virtuel de l'utilisateur.

> **Important :**
>
> Vous pouvez déployer des couches de personnalisation utilisateur dans Citrix Virtual Apps and Desktops ou utiliser les couches utilisateur App Layering activées dans un modèle d'image, et non les deux. N'installez pas la fonctionnalité de couche de personnalisation utilisateur sur une couche dans App Layering.

Cette fonctionnalité remplace Personal vDisk (PvD), tout en offrant une expérience d'espace de travail persistante pour les utilisateurs dans un environnement de bureau non persistant (groupé).

Pour déployer la fonctionnalité de couche de personnalisation utilisateur, installez-la et configurez-la à l'aide de la procédure détaillée dans l'article.

## Prise en charge des applications

Mis à part les exceptions suivantes, toutes les applications qu'un utilisateur installe localement sur le bureau sont prises en charge dans la couche de personnalisation.

### Exceptions

Les applications suivantes sont des exceptions et ne sont pas prises en charge sur la couche de personnalisation des utilisateurs :

- Applications d'entreprise, telles que MS Office et Visual Studio.
- Applications qui modifient le matériel ou la pile réseau. Exemple : un client VPN.
- Applications qui ont des pilotes au niveau du démarrage. Exemple : un analyseur de virus.
- Applications avec des pilotes qui utilisent le magasin de pilotes. Exemple : un pilote d'imprimante.

  > **Remarque :**
  >
  > Vous pouvez rendre les imprimantes disponibles à l'aide des objets de stratégie de groupe (GPO) Windows.

N'autorisez *pas* les utilisateurs à installer localement des applications non prises en charge. Installez plutôt ces applications directement sur l'image principale.

#### Applications nécessitant un compte d'utilisateur ou d'administrateur local

Lorsqu'un utilisateur installe une application localement, elle est placée dans sa couche utilisateur. Si l'utilisateur ajoute ou modifie ensuite un utilisateur ou un groupe local, les modifications ne persistent pas au-delà de la session.

> **Important :**
>
> Ajoutez tout utilisateur ou groupe local requis dans l'image principale.

### Exigences

La fonction de couche de personnalisation des utilisateurs nécessite les composants suivants :

- Citrix Virtual Apps and Desktops 7 1909 ou version ultérieure
- Virtual Delivery Agent (VDA), version 1912 ou ultérieure
- Citrix Provisioning, version 1909 ou ultérieure
- Partage de fichiers Windows (SMB) ou Azure Files avec l'authentification AD sur site activée

Vous pouvez déployer la fonctionnalité de couche de personnalisation utilisateur sur les versions Windows suivantes lorsque le système d'exploitation est déployé en tant que session unique. Cette fonctionnalité est limitée à un seul utilisateur sur une seule session.

- Windows 11 Entreprise x64
- Windows 10 Entreprise x64, version 1607 ou ultérieure
- Windows Server 2016 (Azure Files pris en charge)
- Windows Server 2019 (Azure Files pris en charge)
- Windows Server 2022 (Azure Files pris en charge)

Pour Citrix Virtual Apps and Desktops 7, l'utilisation d'Azure Files avec couches de personnalisation utilisateur est prise en charge sur les clients Windows Server 2022, Windows Server 2019, Windows Server 2016 et Windows 10.

> **Remarque :**
>
> Si vous utilisez un système d'exploitation de serveur, seul le serveur VDI est pris en charge. Pour plus de détails sur le déploiement, consultez l'article Server VDI.
>
> La couche de personnalisation utilisateur prend en charge un seul utilisateur à la fois par machine, puis la machine doit redémarrer pour réinitialiser les disques. Vous ne pouvez pas utiliser la couche de personnalisation utilisateur avec les systèmes d'exploitation serveur multi-session, uniquement avec des systèmes serveur mono-session. La couche de personnalisation utilisateur est prise en charge pour les bureaux non persistants uniquement.

Désinstallez la fonction de couche de personnalisation utilisateur, si elle est installée. Redémarrez l'image principale avant d'installer la dernière version.

### Configurer votre partage de fichiers

La fonctionnalité de couche de personnalisation utilisateur nécessite un stockage SMB (Windows Server Message Block). Pour créer un partage de fichiers Windows, suivez les étapes habituelles pour le système d'exploitation Windows sur lequel vous êtes.

Pour plus d'informations sur l'utilisation d'Azure Files avec des catalogues Azure, consultez Configurer le stockage Azure Files pour les couches de personnalisation utilisateur.

### Recommandations

Suivez les recommandations de cette section pour réussir le déploiement de la couche de personnalisation des utilisateurs.

#### Microsoft System Center Configuration Manager (SCCM)

Si vous utilisez SCCM avec la fonction de couche de personnalisation utilisateur, suivez les consignes de Microsoft pour préparer votre image dans un environnement VDI. Reportez-vous à cet article Microsoft TechNet pour plus d'informations.

#### Taille de la couche utilisateur

Une couche utilisateur est un disque à allocation dynamique qui se développe au fur et à mesure que l'espace sur le disque est utilisé. La taille par défaut allouée à une couche utilisateur est de 10 Go, le minimum recommandé.

> **Remarque :**
>
> Lors de l'installation, si la valeur est définie sur zéro (0), la taille de couche utilisateur par défaut est définie sur 10 Go.

Si vous souhaitez modifier la taille de la couche utilisateur, vous pouvez entrer une valeur différente pour la stratégie **Taille de la couche utilisateur**. Reportez-vous à l'**étape 5 : Créer des stratégies personnalisées de groupe de mise à disposition**, sous **Facultatif : cliquez sur Sélectionner en regard de Taille de la couche utilisateur en Go**.

#### Outils permettant de remplacer la taille de la couche utilisateur (Facultatif)

Vous pouvez remplacer la taille de la couche utilisateur à l'aide d'un outil Windows pour définir un quota sur le partage de fichiers de la couche utilisateur.

Utilisez l'un des outils de quota Microsoft suivants pour définir un quota dur sur le répertoire de couches utilisateur nommé **Utilisateurs** :

- Gestionnaire de ressources du serveur de fichiers (FSRM)
- Gestion de quota

> **Remarque :**
>
> L'augmentation du quota affecte les nouvelles couches utilisateur et étend les couches existantes. La diminution du quota n'affecte que les nouvelles couches utilisateur. Les couches utilisateur existantes ne diminuent jamais en taille.

### Déployer une couche de personnalisation utilisateur

Lors du déploiement de la fonctionnalité de personnalisation utilisateur, vous définissez les stratégies dans Web Studio. Vous affectez ensuite les stratégies au groupe de mise à disposition lié au catalogue de machines, où la fonctionnalité est déployée.

Si vous laissez l'image principale sans configuration de couche de personnalisation de l'utilisateur, les services restent inactifs et ne peuvent pas interférer avec les activités de création.

Si vous définissez les stratégies dans l'image principale, les services tentent d'exécuter et de monter une couche utilisateur dans l'image principale. L'image principale présente des comportements inattendus et des problèmes de stabilité.

Pour déployer la fonction de couche de personnalisation des utilisateurs, procédez comme suit dans cet ordre :

- Étape 1 : Vérifier si un environnement Citrix Virtual Apps and Desktops est disponible.
- Étape 2 : Préparer votre image principale.
- Étape 3 : Créer un catalogue de machines.
- Étape 4 : Créer un groupe de mise à disposition.
- Étape 5 : Créer des stratégies personnalisées de groupe de mise à disposition.

> **Remarque :**
>
> La première connexion après la mise à niveau de Windows 10 sur l'image prend plus de temps que d'habitude. La couche de l'utilisateur doit être mise à jour pour la nouvelle version de Windows 10, ce qui augmente le temps d'ouverture de session.

#### Étape 1 : Vérifier si l'environnement Citrix Virtual Apps and Desktops est disponible

Assurez-vous que votre environnement Citrix Virtual Apps and Desktops peut être utilisé avec cette nouvelle fonctionnalité. Pour plus d'informations sur l'installation, reportez-vous à la section Installer et configurer Citrix Virtual Apps and Desktops.

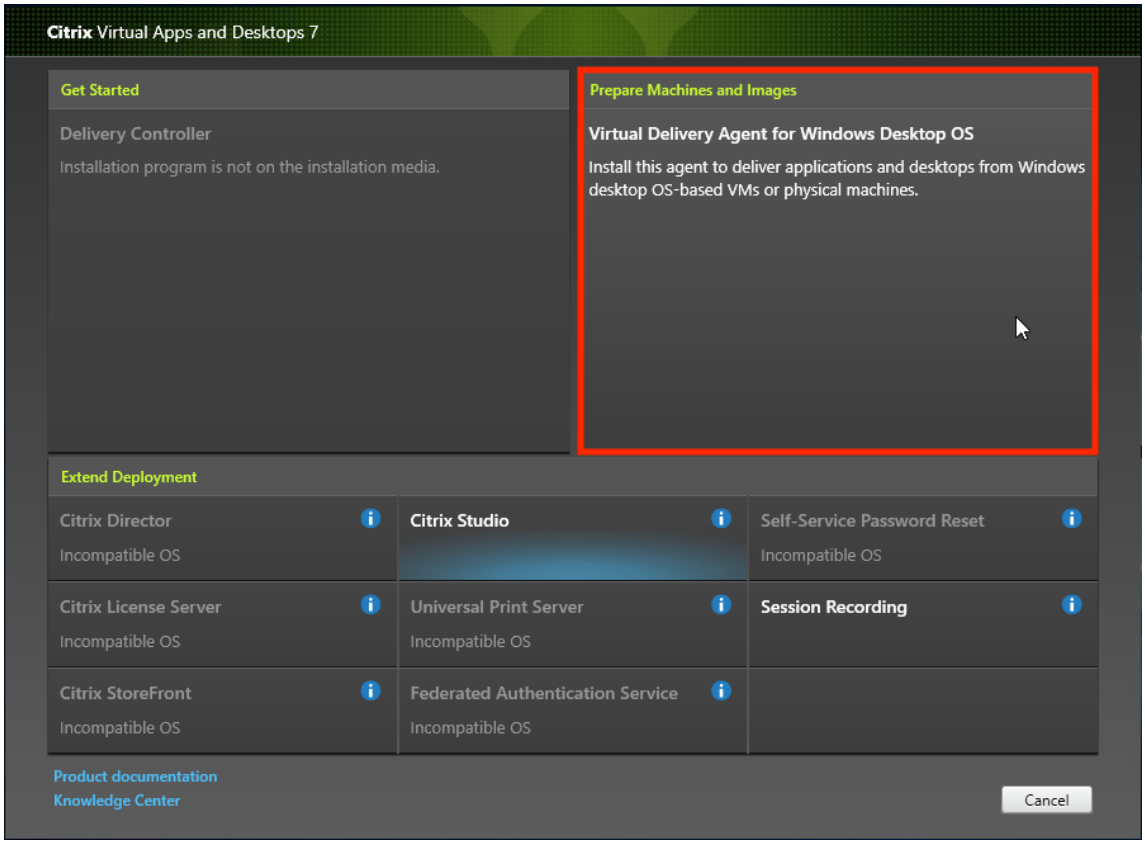
#### Étape 2 : Préparer votre image principale

Pour préparer votre image principale :

1. Repérez l'image principale. Installez les applications d'entreprise de votre organisation et toutes les autres applications que vos utilisateurs trouvent généralement utiles.
2. Si vous déployez Server VDI, suivez les étapes décrites dans l'article Server VDI. Veillez à inclure le composant facultatif, la **couche de personnalisation utilisateur**. Pour plus d'informations, consultez les options de ligne de commande pour installer un VDA.
3. Si vous utilisez Windows 10, installez Virtual Delivery Agent (VDA) 1912 ou version ultérieure. Si une ancienne version du VDA est déjà installée, désinstallez d'abord l'ancienne version. Lors de l'installation de la nouvelle version, veillez à sélectionner et installer le composant facultatif **Couche de personnalisation des utilisateurs de Citrix**, comme suit :

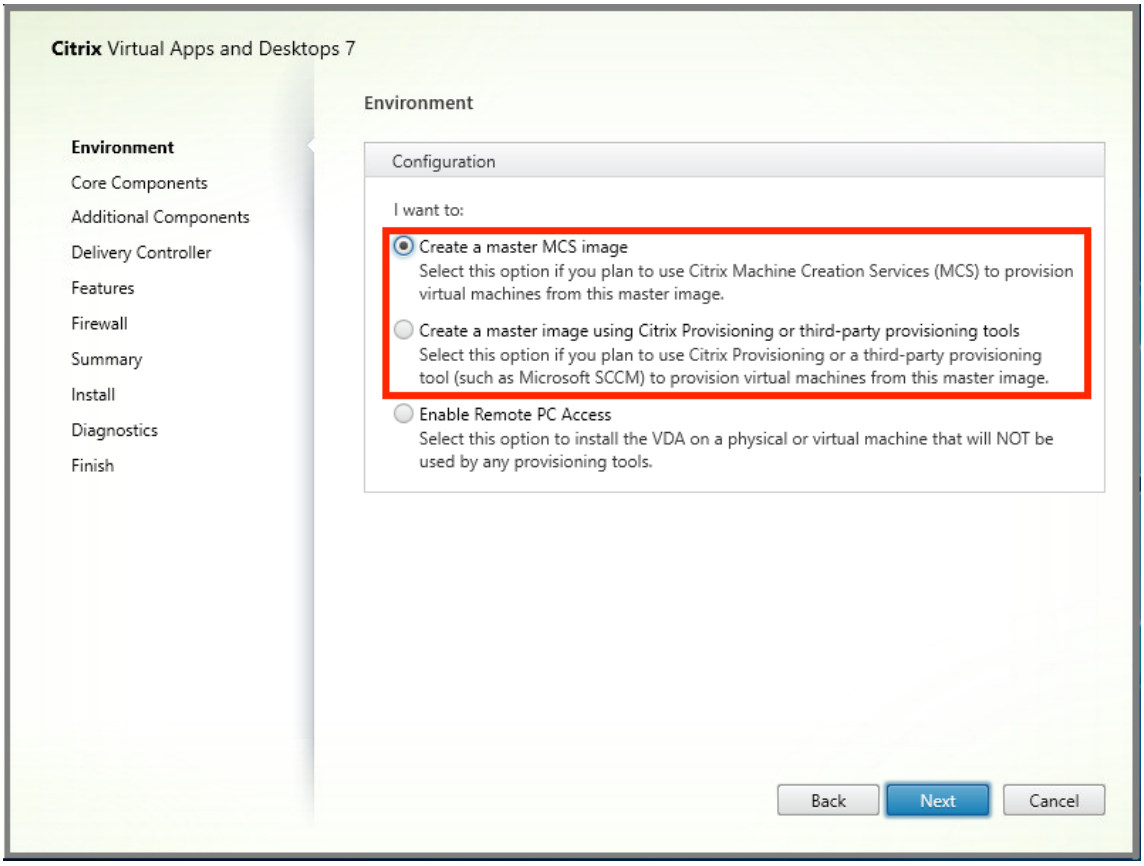
    a) Cliquez sur la mosaïque **Virtual Delivery Agent pour système d'exploitation de bureau Windows** :




a) **Environnement :** sélectionnez **Créer une image MCS principale** ou **Créer une image principale à l'aide de Citrix Provisioning ou d'outils de provisioning tiers**.

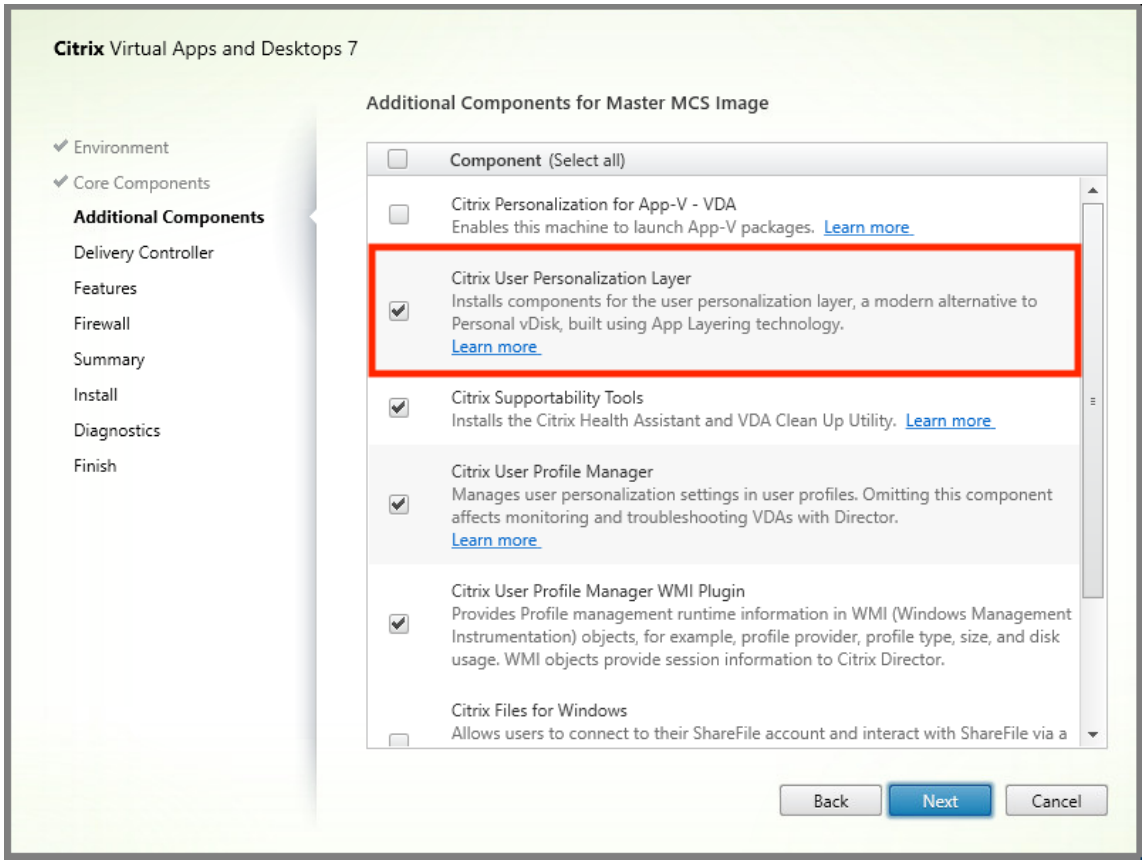
 




a) **Composants principaux :** cliquez sur **Suivant**.

b) **Composants supplémentaires :** sélectionnez **Couche de personnalisation des utilisateurs Citrix**.




a) Cliquez sur les fenêtres d'installation restantes, configurez le VDA selon vos besoins, puis cliquez sur **Installer**. L'image redémarre une ou plusieurs fois pendant l'installation.

4. N'activez pas les **mises à jour Windows**. Le programme d'installation de la couche de personnalisation des utilisateurs désactive les mises à jour Windows sur l'image. N'activez pas les mises à jour.

L'image est prête à être téléchargée dans Web Studio.

> **Remarque :**
>
> Si vous souhaitez simplement mettre à niveau la couche de personnalisation utilisateur (UPL), vous pouvez le faire à l'aide d'une version plus récente d'UPL et du package autonome. Il n'est pas nécessaire de mettre à niveau le VDA.

### Étape 3 : Créer un catalogue de machines

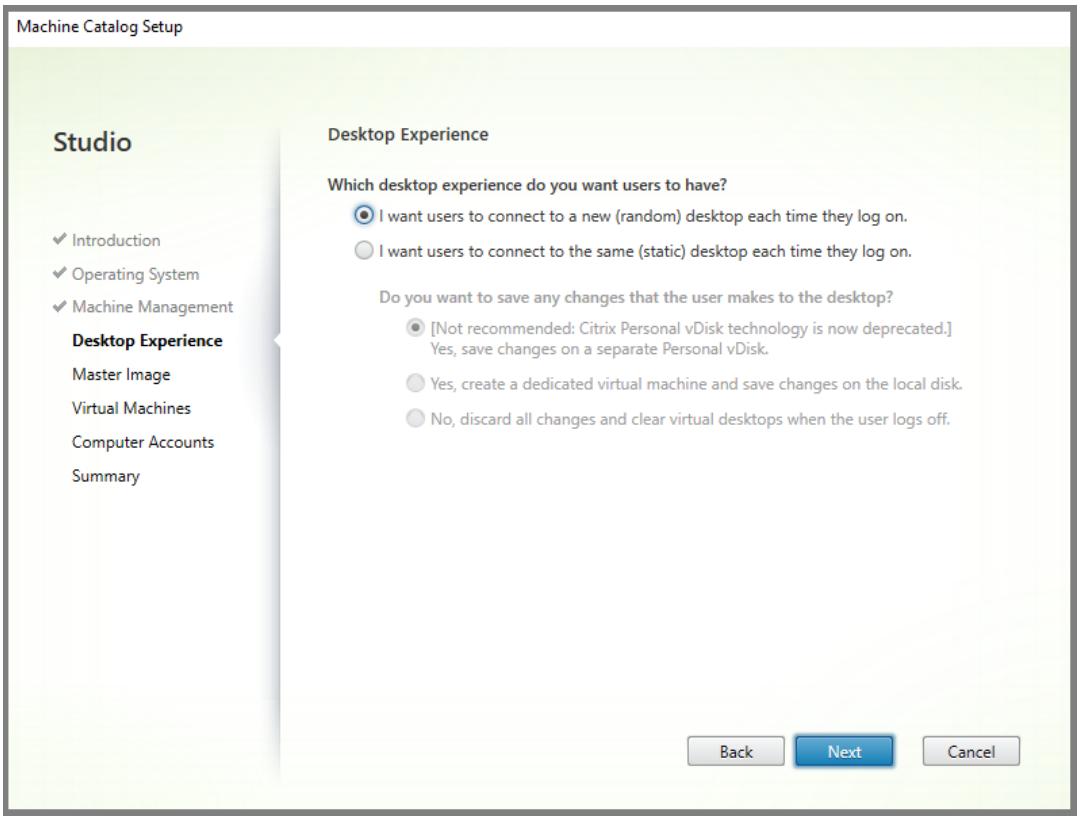
Dans Web Studio, suivez les étapes pour créer un catalogue de machines. Utilisez les options suivantes lors de la création du catalogue :

1. Sélectionnez **Système d'exploitation** et définissez sur **OS mono-session**.

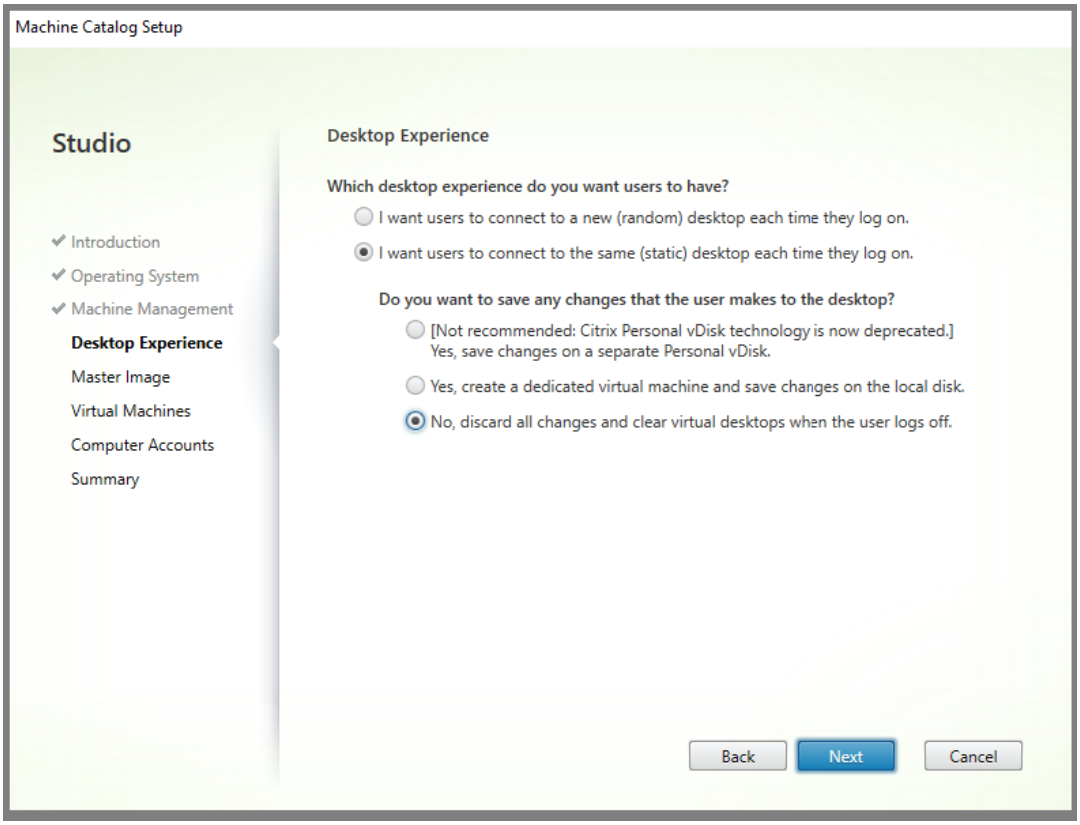
2. Sélectionnez **Gestion des machines** et définissez sur **des machines dont l'alimentation est gérée**. Par exemple, des machines virtuelles ou des PC lames.
3. Sélectionnez **Expérience de bureau** et définissez sur le type de catalogue avec **regroupement aléatoire** ou **regroupement statique**, comme dans les exemples suivants :

   - **Regroupement aléatoire :**




   - **Regroupement statique :** si vous sélectionnez le regroupement statique, configurez les bureaux de sorte qu'ils ignorent toutes les modifications et effacent les bureaux virtuels lorsque l'utilisateur se déconnecte, comme indiqué dans la capture d'écran suivante :




> **Remarque :**
>
> La couche de personnalisation des utilisateurs ne prend pas en charge les catalogues avec regroupement statique configurés pour utiliser Citrix Personal vDisk ou affectés en tant que machines virtuelles dédiées.

4. Si vous utilisez MCS, sélectionnez **Image** et l'instantané de l'image créée dans la section précédente.
5. Configurez les propriétés de catalogue restantes selon les besoins de votre environnement.

### Étape 4 : Créer un groupe de mise à disposition

Créez et configurez un **groupe de mise à disposition** comprenant les machines du catalogue de machines que vous avez créé. Pour de plus amples informations, consultez la section Créer des groupes de mise à disposition.

### Étape 5 : Créer des stratégies personnalisées de groupe de mise à disposition

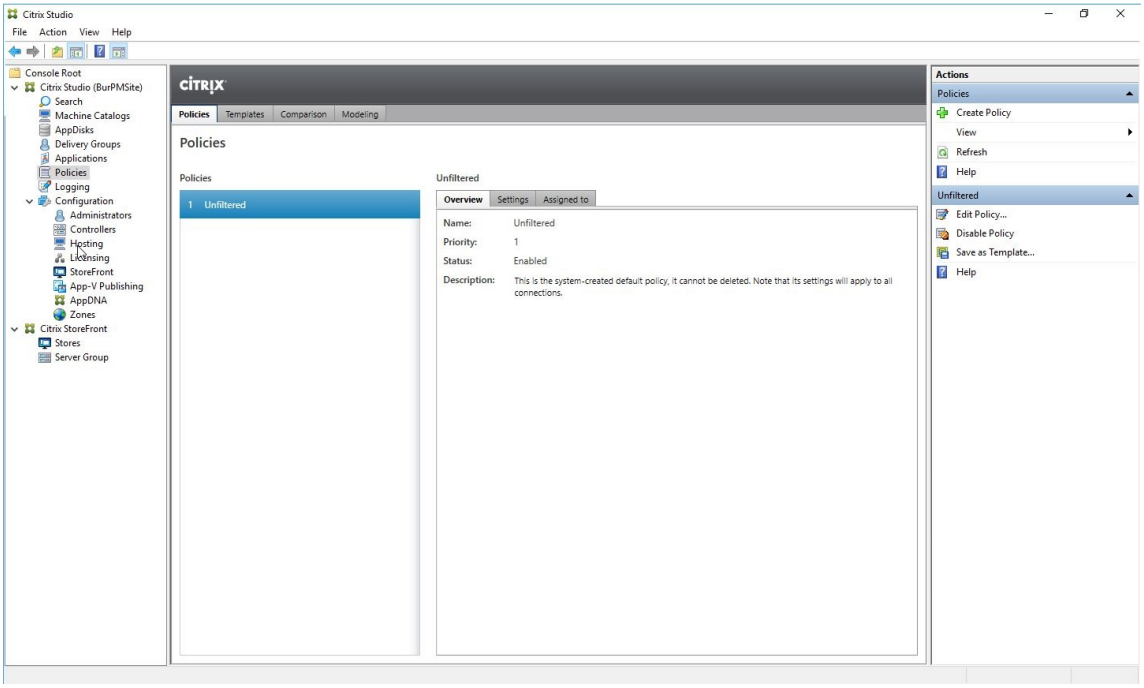
Pour activer le montage des couches utilisateur dans les VDA, utilisez les paramètres de configuration pour spécifier :

- Où accéder aux couches utilisateur sur le réseau.
- La taille à laquelle permettre à la couche utilisateur de se développer.

Pour définir les paramètres en tant que stratégies Citrix personnalisées dans Web Studio et les attribuer à votre groupe de mise à disposition :

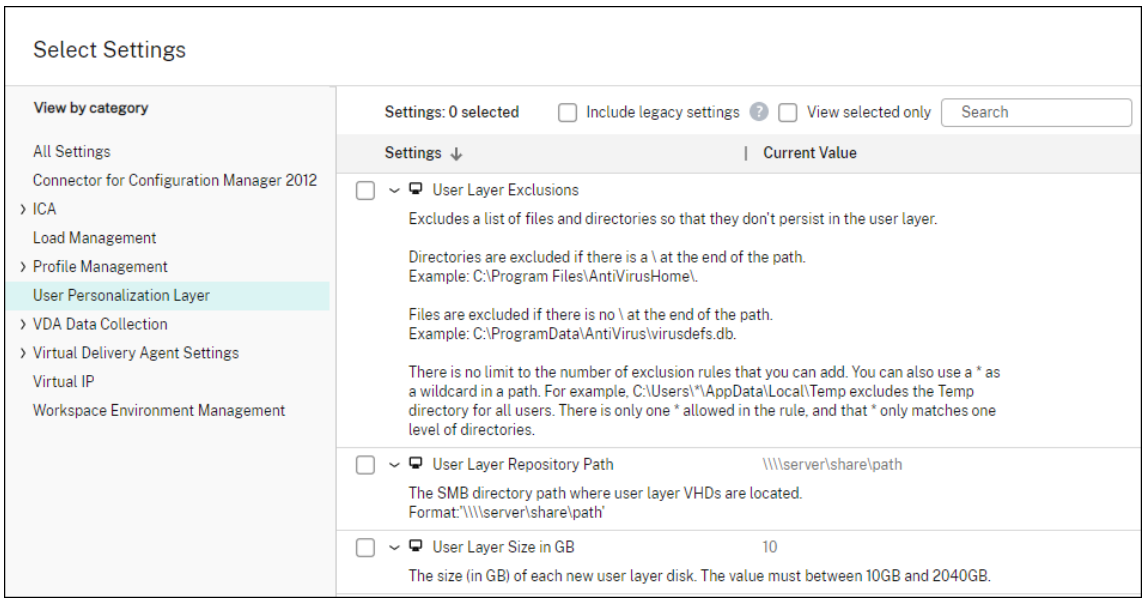
1. Connectez-vous à Web Studio et sélectionnez **Stratégies** dans le volet de gauche :




2. Sélectionnez **Créer une stratégie** dans la barre d'actions. La fenêtre Créer une stratégie s'affiche.
3. Entrez `user layer` dans le champ de recherche. Les trois stratégies suivantes apparaissent dans la liste des stratégies disponibles :
   - Exclusions de couche utilisateur
   - Chemin du référentiel de couche utilisateur
   - Taille de la couche utilisateur en Go

   > **Remarque :**
   >
   > L'augmentation de la taille affecte les nouvelles couches utilisateur et étend les couches utilisateur existantes. La diminution de la taille n'affecte que les nouvelles couches utilisateur. Les couches utilisateur existantes ne diminuent jamais en taille.

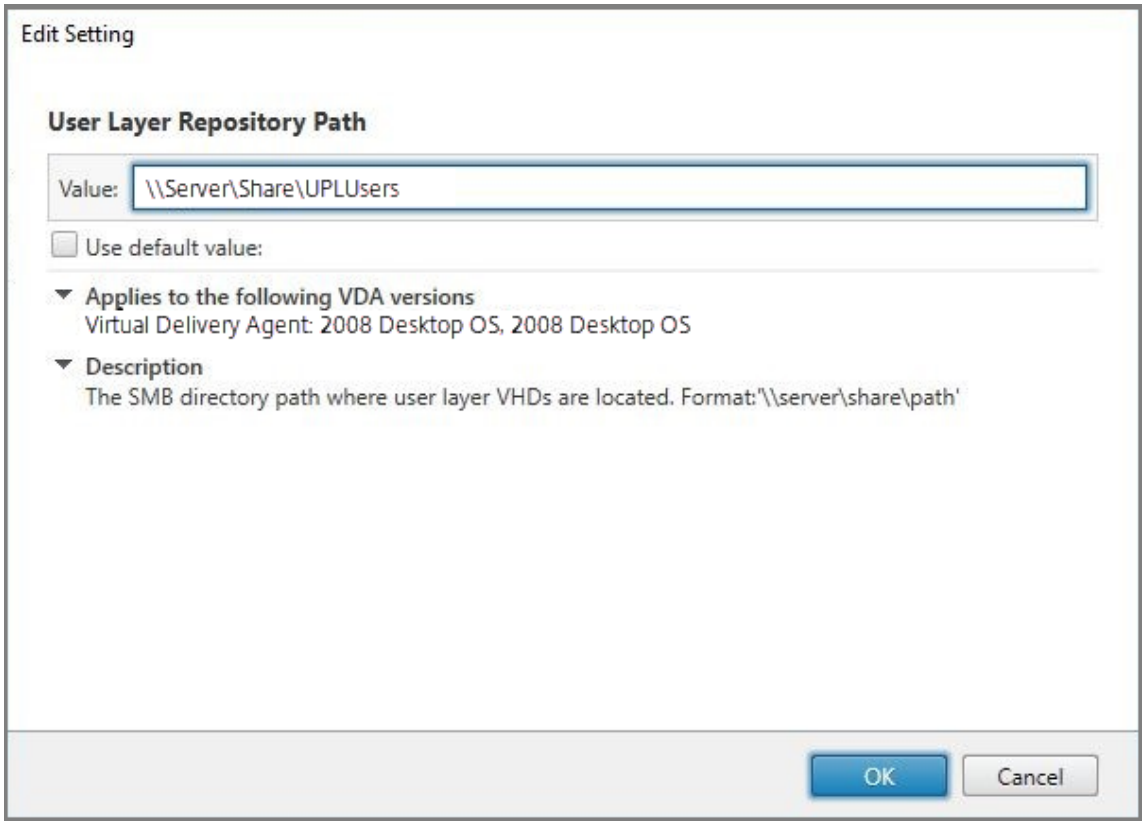
 




4. Cochez la case en regard de **Chemin du référentiel de couche utilisateur** et cliquez sur **Modifier**. La fenêtre **Modifier le paramètre** s'affiche.
5. Entrez un chemin dans le champ **Valeur**, puis cliquez sur **Enregistrer** :

   - **Format du chemin d'accès :** `\\server-name-or-address\share-name\folder`
   - **Exemple de chemin d'accès :** `\\Server\Share\UPLUsers`
   - **Exemple de chemin obtenu :**pour un utilisateur nommé **Alex** dans **CoolCompanyDomain**, le chemin d'accès correspond à :`\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

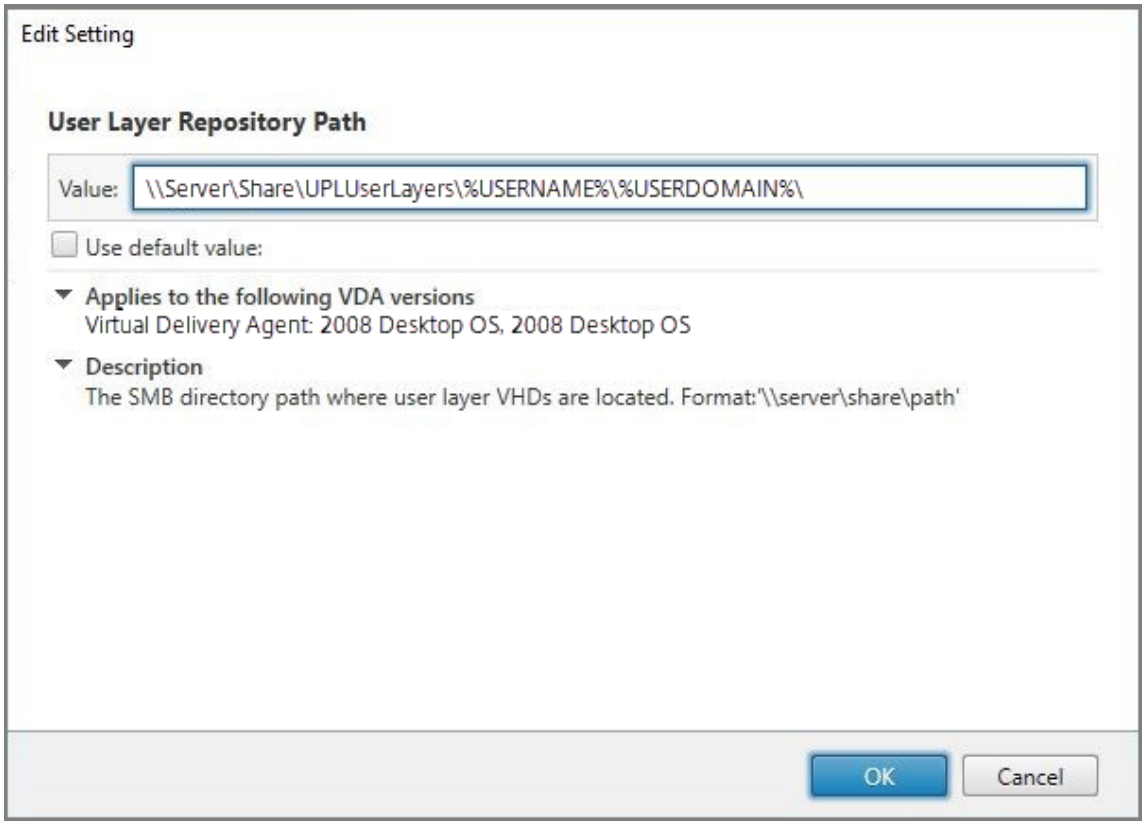



Vous pouvez personnaliser le chemin à l'aide des variables %USERNAME% et %USERDOMAIN% , des variables d'environnement de la machine et des attributs Active Directory (AD). Lorsqu' elles sont développées, ces variables entraînent des chemins explicites.

Exemples de variables d'environnement :

- **Format du chemin d'accès :** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **Exemple de chemin d'accès :** `\\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%`
- **Exemple de chemin obtenu :**Pour un utilisateur nommé **Alex** dans **CoolCompanyDomain**, le chemin d'accès correspond à :`\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

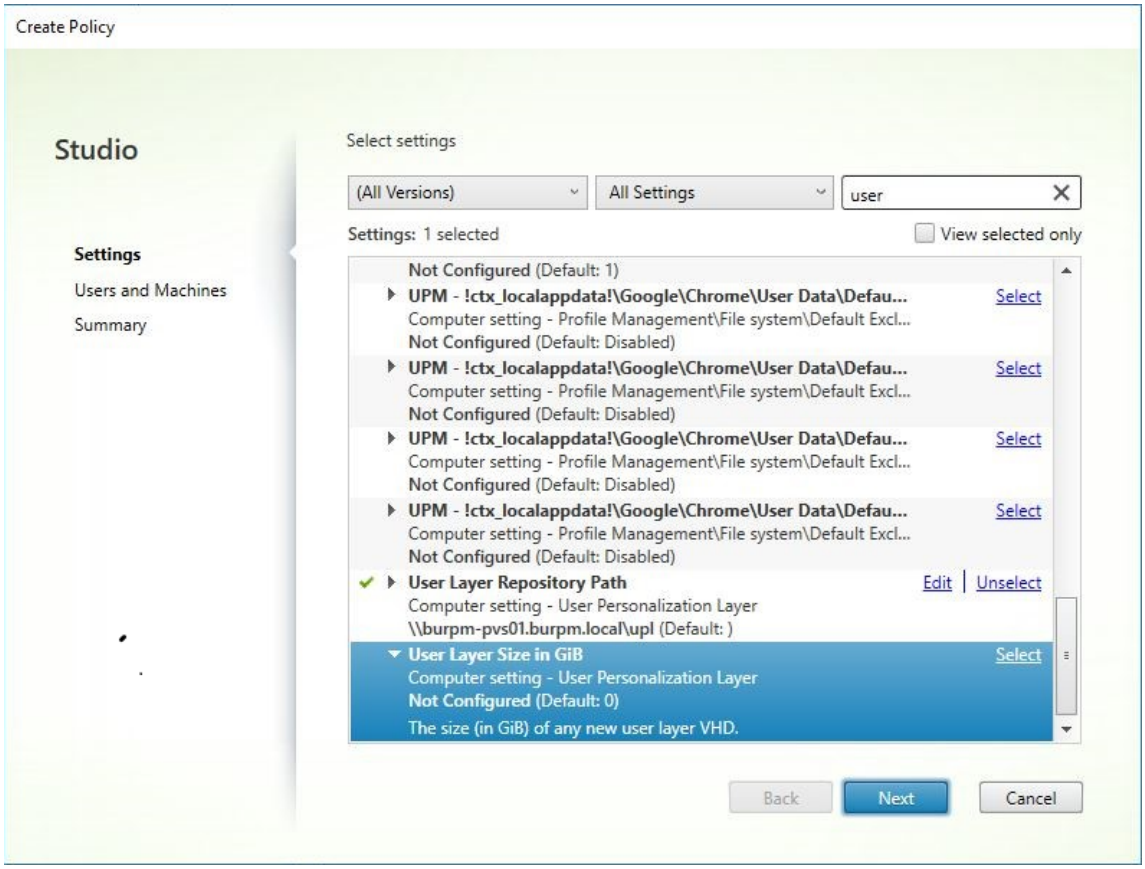



Exemple d'attributs AD personnalisés :

- Format du chemin d'accès : `\\Server-name-or-address\share-name\AD-attribute`
- Exemple de chemin d'accès : `\\Server\share\\#sAMAccountName#`
- Exemple de chemins résultants : `\\Server\share\JohnSmith` (si #sAMAccount-Name # correspond à JohnSmith pour l'utilisateur actuel)

6. Facultatif : cochez la case en regard de **Taille de la couche utilisateur en Go** et cliquez sur **Modifier** :

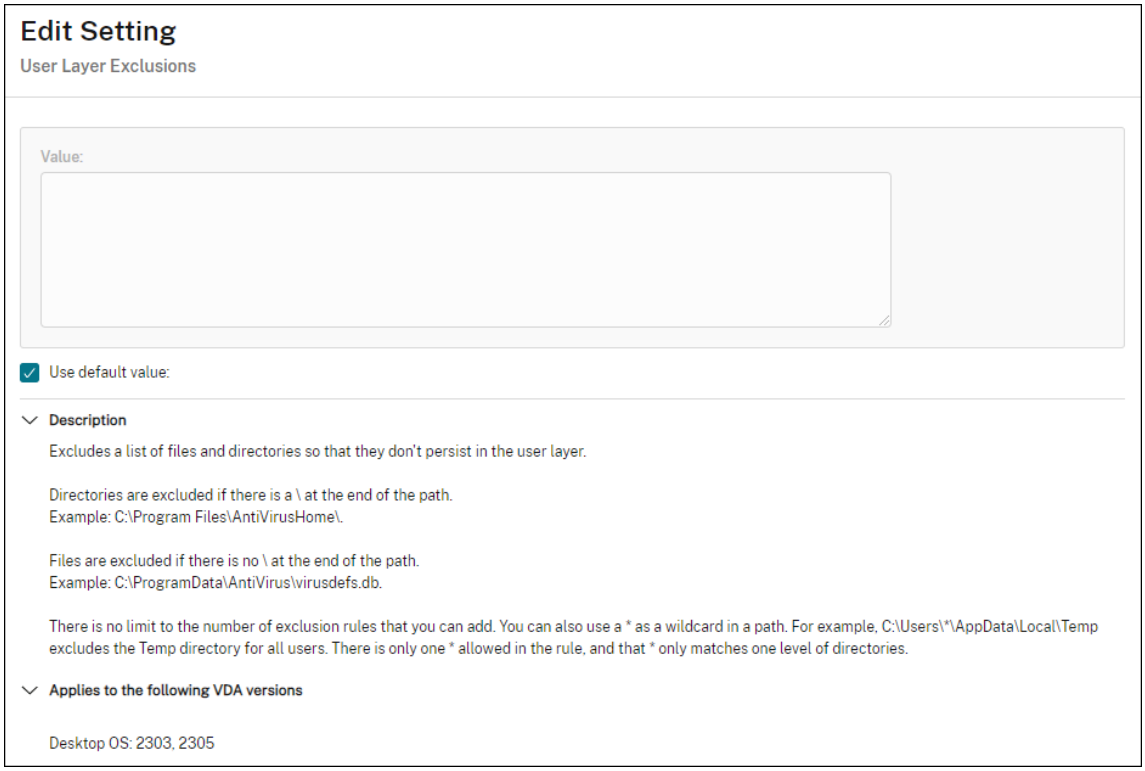
 




La fenêtre Modifier les paramètres s'affiche.

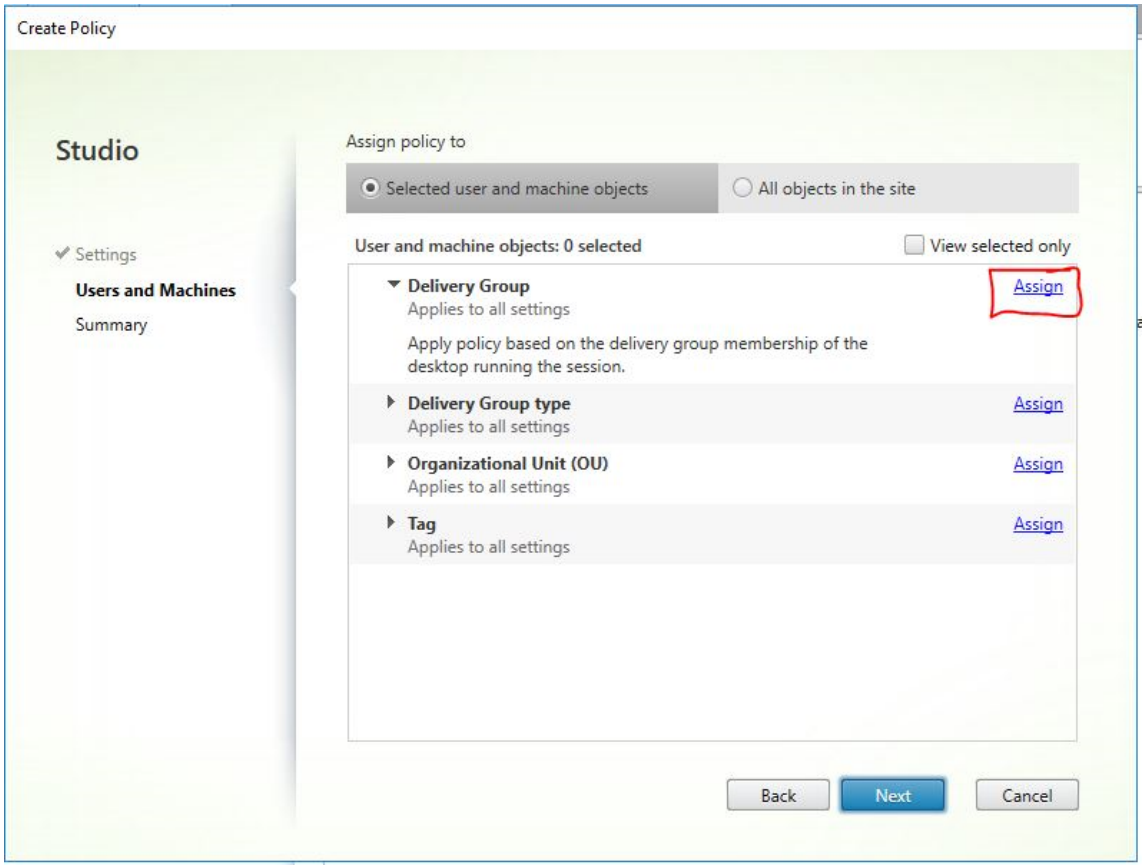
7. Facultatif : remplacez la valeur par défaut de **10 Go** par la taille maximale que chaque couche utilisateur peut atteindre. Cliquez sur **Enregistrer**.
8. Facultatif : cochez la case en regard de **Exclusions de couche utilisateur** et cliquez sur **Modifier**.



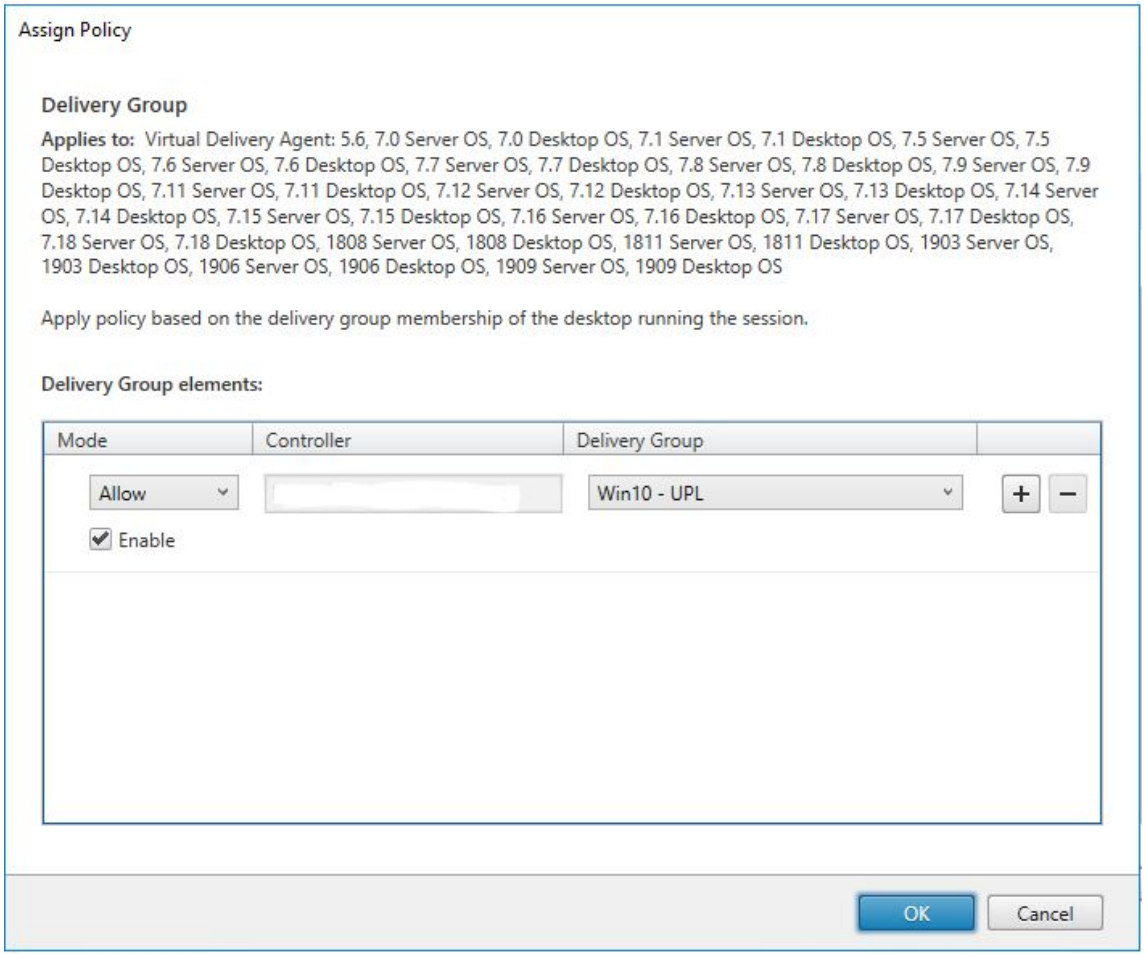

9. Facultatif : spécifiez les fichiers et les dossiers à exclure, puis cliquez sur **Enregistrer**. Pour plus d'informations, consultez la documentation de Citrix App Layering.
10. Cliquez sur **Suivant** pour configurer les utilisateurs et les machines auxquels vous souhaitez attribuer des tâches. Cliquez sur le lien **Groupe de mise à disposition > Attribuer** mis en surbrillance dans cette image :



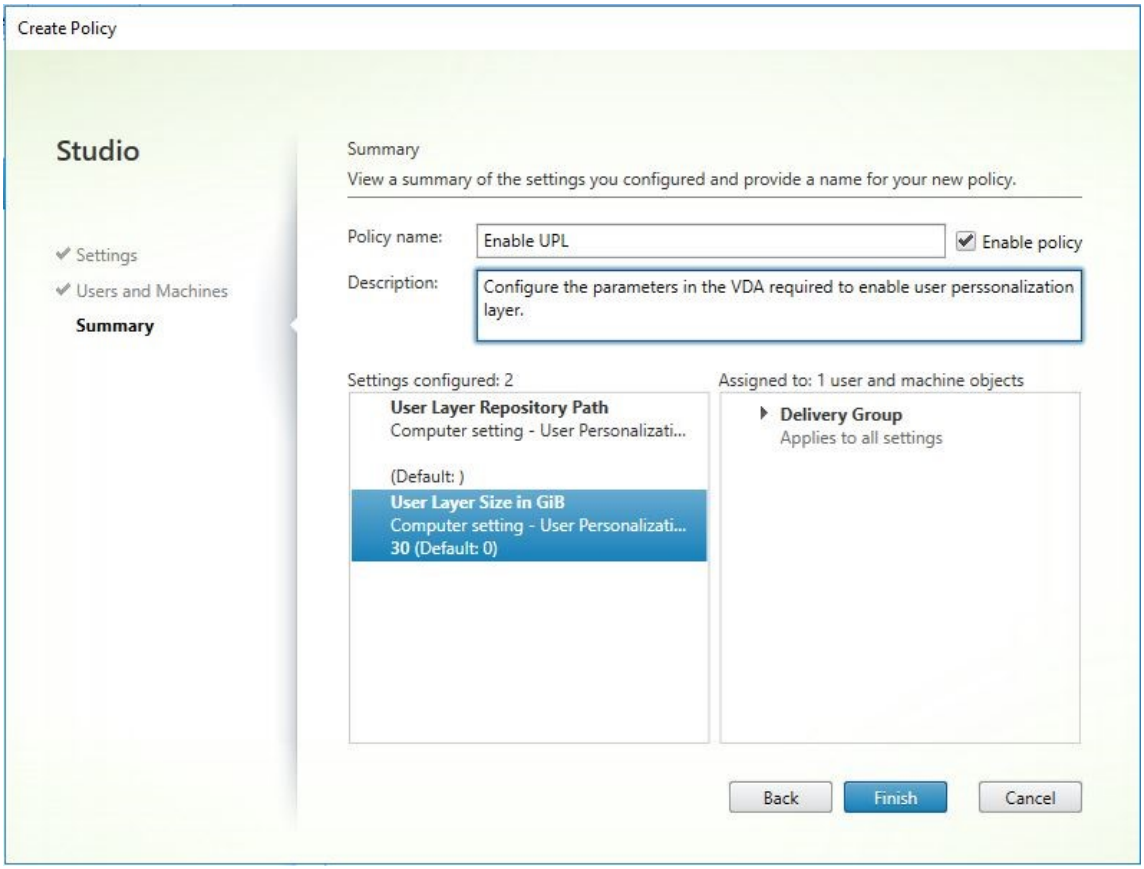

11. Dans le menu **Groupe de mise à disposition**, sélectionnez le groupe de mise à disposition créé dans la section précédente. Cliquez sur **OK**.




12. Entrez un nom pour la stratégie. Cliquez sur la case à cocher pour activer la stratégie, puis cliquez sur **Terminer**.




### Configurer les paramètres de sécurité sur le dossier de la couche utilisateur

En tant qu'administrateur de domaine, vous pouvez spécifier plusieurs emplacements de stockage pour vos couches utilisateur. Créer un sous-dossier `\Users` pour chaque emplacement de stockage (y compris l'emplacement par défaut). Sécurisez chaque emplacement à l'aide des paramètres suivants.

| Nom du paramètre | Valeur | Appliquer à |
|---|---|---|
| Créateur propriétaire | Modifier | Sous-dossiers et fichiers uniquement |
| Droits du propriétaire | Modifier | Sous-dossiers et fichiers uniquement |
| Utilisateurs ou groupe | Création de dossier/ajout de données ; Parcours du dossier/exécution du fichier ; Liste du dossier/lecture de données ; Lecture des attributs | Dossier sélectionné uniquement |

| Nom du paramètre | Valeur | Appliquer à |
| --- | --- | --- |
| Système | Contrôle total | Dossier sélectionné, sous-dossiers et fichiers |
| Administrateurs de domaine et groupe d'administrateurs sélectionné | Contrôle total | Dossier sélectionné, sous-dossiers et fichiers |

### Messages de couche utilisateur

Lorsqu'un utilisateur n'est pas en mesure d'accéder à sa couche utilisateur, il reçoit l'un de ces messages de notification.

- **Couche utilisateur en cours d'utilisation**

  ```
  We were unable to attach your user layer because it is in use.
  Any changes you make to application settings or data will not be
  saved. Be sure to save any work to a shared network location.<!--
  NeedCopy-->
  ```

- **Couche utilisateur non disponible**

  ```
  We were unable to attach your user layer. Any changes you make to
   application settings or data will not be saved. Be sure to save
  any work to a shared network location.<!--NeedCopy-->
  ```

- **Le système n'a pas été réinitialisé après la déconnexion de l'utilisateur**

  ```
  This system was not shut down properly. Please log off immediately
   and contact your system administrator.<!--NeedCopy-->
  ```

### Fichiers journaux à utiliser lors du dépannage

Le fichier journal, ulayersvc.log, contient la sortie du logiciel de couche de personnalisation des utilisateurs où les modifications sont enregistrées.

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
2 <!--NeedCopy-->
```

### Couche utilisateur/récupération d'espace UPL

Vous pouvez utiliser la **couche utilisateur/récupération d'espace UPL** pour compresser automatiquement les fichiers VHDX chaque fois que l'utilisateur ferme sa session.

Pour plus d'informations, consultez Couche utilisateur/récupération d'espace UPL

### Limitations

Gardez à l'esprit les limitations suivantes lors de l'installation et de l'utilisation de la fonction de couche de personnalisation des utilisateurs.

- N'essayez *pas* de déployer le logiciel de couche de personnalisation utilisateur sur une couche dans App Layering. Déployez des couches de personnalisation utilisateur dans Citrix Virtual Apps and Desktops ou activez les couches utilisateur dans un modèle d'image App Layering, et non les deux. L'un ou l'autre processus produit les couches utilisateur dont vous avez besoin.
- *Ne pas* configurer la fonction de couche de personnalisation des utilisateurs avec des catalogues de machines persistants.
- *Ne pas* utiliser des hôtes de session.
- *Ne pas* mettre à jour le catalogue de machines avec une image exécutant une nouvelle installation du système d'exploitation (y compris la même version de Windows 10). La meilleure pratique consiste à appliquer les mises à jour au système d'exploitation dans l'image principale utilisée lors de la création du catalogue de machines.
- Ne *pas* utiliser des pilotes de démarrage, ni aucune autre personnalisation de démarrage.
- *Ne pas* migrer les données PvD vers la fonctionnalité de couche de personnalisation de l'utilisateur.
- *Ne pas* migrer les couches utilisateur existantes depuis le produit App Layering complet vers la fonctionnalité de couche de personnalisation de l'utilisateur.
- *Ne pas* modifier le chemin SMB de la couche utilisateur pour accéder aux couches utilisateur créées à l'aide d'une autre image de système d'exploitation principale.
- Lorsqu'un utilisateur se déconnecte d'une session puis se connecte à nouveau, la nouvelle session s'exécute sur une autre machine du pool. Dans un environnement VDI, le Centre logiciel Microsoft répertorie une application comme **installée** sur la première machine, mais l'affiche comme **non disponible** sur la deuxième machine.

  Pour connaître l'état réel de l'application, demandez à l'utilisateur de sélectionner l'application dans le Centre logiciel et cliquez sur **Installer**. SCCM affiche alors l'état correct.
- Software Center s'arrête parfois immédiatement après le lancement dans un VDA sur lequel la fonctionnalité de couche de personnalisation des utilisateurs est activée. Pour éviter ce problème, suivez les recommandations de Microsoft concernant la mise en œuvre de SCCM dans un environnement XenDesktop VDI. Assurez-vous également que le service `ccmexec` est en cours d'exécution avant de démarrer Software Center.

- Dans Stratégies de groupe (Paramètres de l'ordinateur), les paramètres de couche utilisateur remplacent les paramètres appliqués à l'image principale. Par conséquent, les modifications apportées dans les paramètres de l'ordinateur à l'aide d'un objet de stratégie de groupe ne sont pas toujours présentes pour l'utilisateur lors de la prochaine session.

  Pour contourner ce problème, créez un script d'ouverture de session utilisateur qui émet la commande :

  ```
  gpupdate /force
  ```

  Par exemple, un client a défini la commande suivante pour qu'elle s'exécute à chaque connexion utilisateur :

  ```
  gpudate /Target:Computer /force
  ```

  Pour obtenir de meilleurs résultats, appliquez les modifications aux paramètres de l'ordinateur directement sur la couche utilisateur, une fois que l'utilisateur s'est connecté.

- Un compte d'utilisateur de domaine ne doit pas être le dernier utilisateur à s'être connecté à une image principale. Sinon, les machines provisionnées à partir de cette image rencontreront des problèmes.
- Les certificats personnalisés ne sont pas conservés lorsque UPL est activé dans un environnement Azure AD pur, en raison d'un problème sous-jacent lié à l'exécution de Windows sur Azure. Si Microsoft corrige ce problème dans une future amélioration, nous mettrons à jour cet article.

## Supprimer des composants

June 27, 2024

Pour supprimer des composants, Citrix vous recommande d'utiliser la fonctionnalité Windows destinée à supprimer ou modifier des programmes. Vous pouvez également supprimer des composants à l'aide de la ligne de commande, ou d'un script sur le support d'installation.

Lorsque vous supprimez des composants, les composants pré-requis ne sont pas supprimés, et les paramètres du pare-feu ne sont pas modifiés. Par exemple, lorsque vous supprimez un Delivery Controller, le logiciel SQL Server et les bases de données ne sont pas supprimés.

Si vous avez mis à niveau un Controller à partir d'un déploiement antérieur contenant l'Interface Web, vous devez supprimer le composant Interface Web séparément. Vous ne pouvez pas utiliser le programme d'installation pour supprimer l'Interface Web.

Pour plus d'informations sur la suppression des fonctionnalités non mentionnées ci-dessous, consultez la documentation de la fonctionnalité.

### Préparation

Avant de supprimer un Controller, supprimez-le du site. Pour plus de détails, voir Supprimer un Controller.

Fermez Studio et Director avant de les supprimer.

### Supprimer des composants à l'aide de la fonctionnalité Windows pour la suppression ou la modification de programmes

À partir de la fonctionnalité Windows pour la suppression ou la modification de programmes :

- Pour supprimer un Controller, Studio, Director, le serveur de licences ou StoreFront, cliquez sur **Citrix Virtual Apps *version*** ou **Citrix Virtual Apps and Desktops *version*** avec le bouton droit de la souris et sélectionnez **Désinstaller**. Le programme d'installation démarre. Sélectionnez les composants à supprimer.

  Sinon, vous pouvez supprimer StoreFront en cliquant avec le bouton droit de la souris sur **Citrix StoreFront** et en sélectionnant **Désinstaller**.
- Pour supprimer un VDA, cliquez sur **Citrix Virtual Delivery Agent *version*** avec le bouton droit de la souris et sélectionnez **Désinstaller**. Le programme d'installation démarre et vous permet de sélectionner les composants à supprimer. La machine redémarre automatiquement après la suppression, par défaut.
- Pour supprimer le Serveur d'impression universelle, cliquez sur **Serveur d'impression universelle Citrix** avec le bouton droit de la souris et sélectionnez **Désinstaller**.

### Supprimer les composants principaux à l'aide de la ligne de commande

À partir du répertoire `\x64\XenDesktop Setup`, exécutez la commande `XenDesktopServerSetup.exe`.

- Pour supprimer un ou plusieurs composants principaux, utilisez les options `/remove` et `/components`.
- Pour supprimer tous les composants, spécifiez l'option `/removeall`.

Pour plus d'informations sur les commandes et les paramètres, consultez la section Installer à l'aide de la ligne de commande.

Par exemple, les commandes suivantes suppriment Web Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
webstudio
```

### Supprimer des VDA à l'aide de la ligne de commande

À partir du répertoire `\x64\XenDesktop Setup`, exécutez la commande `XenDesktopVdaSetup.exe`.

- Pour supprimer un ou plusieurs composants principaux, utilisez les options `/remove` et `/components`. Par exemple, pour supprimer le VDA et l'application Citrix Workspace, utilisez `/remove /components vda,plugin`.
- L'option `/removeall` supprime uniquement le VDA. Elle ne supprime pas l'application Citrix Workspace.

Pour plus d'informations sur les commandes et les paramètres, consultez la section Installer à l'aide de la ligne de commande.

La machine redémarre automatiquement après la suppression, par défaut.

Pour supprimer des VDA à l'aide d'un script dans Active Directory, consultez la section Installer ou supprimer des VDA à l'aide de scripts.

## Mettre à niveau et migrer

June 27, 2024

### Introduction

La mise à niveau migre votre déploiement vers la **version actuelle** (CR) de Citrix Virtual Apps and Desktops 7 sans avoir à définir de nouvelles machines ou de nouveaux sites. Cela s'appelle une mise à niveau sur place.

La mise à niveau vous donne accès aux dernières fonctionnalités et technologies auxquelles vous êtes autorisé. Les mises à niveau peuvent également contenir des correctifs, des clarifications et des améliorations par rapport aux versions antérieures.

#### Présentation de la mise à niveau

1. Consultez l'article Mettre à niveau un déploiement avant de procéder à la mise à niveau. Il s'agit de la principale source d'information pour apprendre à se préparer et à mettre en œuvre une mise à niveau.
2. Assurez-vous que les dates actuelles de Customer Success Services sont valides et qu'elles n'ont pas expiré. Pour plus d'informations sur le renouvellement, voir l'article Licences de renouvellement de Customer Success.

3. Suivez le guide de préparation.
4. Exécutez les programmes d'installation pour mettre à niveau les composants principaux.
5. Mettez à niveau les bases de données système et le site.
6. Mettez à niveau les VDA sur les images (ou directement sur les machines).
7. Mettez à niveau les composants.

Chaque étape de préparation et de mise à niveau est détaillée dans Mettre un déploiement à niveau.

### Versions pouvant être mises à niveau

Vous pouvez effectuer une mise à niveau vers Citrix Virtual Apps and Desktops 2402 LTSR depuis :

- Virtual Apps and Desktops 2203 LTSR avec ou sans mise à jour cumulative, jusqu'à CU4 (incluse)
- Virtual Apps and Desktops 1912 LTSR avec ou sans mise à jour cumulative, jusqu'à CU8 (incluse)
- Versions actuelles (CR) prises en charge de Citrix Virtual Apps and Desktops

Vous pouvez également consulter le [Guide de mise à niveau Citrix](/en-us/upgrade.html) pour obtenir la liste des versions de Citrix Virtual Apps and Desktops (et XenApp et XenDesktop) à partir desquelles vous pouvez effectuer une mise à niveau.

> Remarque :
>
> - Avant de lancer le processus de mise à niveau, Citrix recommande aux clients de tester la mise à niveau dans un environnement contrôlé et de vérifier qu'elle répond à leurs exigences spécifiques. En outre, nous vous conseillons de consulter toute la documentation pertinente du produit, y compris la liste des produits obsolètes et des problèmes connus, afin de garantir une transition fluide. Cette approche permet d'atténuer les risques de perturbation des systèmes de production et d'améliorer l'expérience globale de mise à niveau.
> - Citrix Virtual Apps and Desktops 1912 LTSR arrive bientôt en phase de fin de vie.
>   Pour plus d'informations sur les versions prises en charge, consultez le Tableau des produits.

### Foire aux questions

Cette section répond à certaines questions fréquemment posées sur la mise à niveau de Citrix Virtual Apps and Desktops.

- **Quel est l'ordre correct pour la mise à niveau de mon environnement Virtual Apps and Desktops ?**

  Pour obtenir une illustration et une description de la séquence de mise à niveau recommandée, reportez-vous à Séquence de mise à niveau et Procédure de mise à niveau.

- **Mon site dispose de plusieurs Delivery Controller (dans différentes zones). Que se passe-t-il si je mets à niveau seulement certains d'entre eux ? Suis-je obligé de mettre à niveau chaque Delivery Controller du site pendant la même fenêtre de maintenance ?**

  La meilleure pratique consiste à mettre à niveau tous les Delivery Controller pendant la même fenêtre de maintenance, car différents services sur chaque Delivery Controller communiquent entre eux. L'utilisation de versions différentes peut causer des problèmes. Au cours d'une fenêtre de maintenance, nous vous recommandons de mettre à niveau la moitié des Delivery Controller, de mettre à niveau le site, puis de mettre à niveau les Delivery Controller restants. Pour plus de détails, consultez la procédure de mise à niveau.

- **Puis-je accéder directement à la dernière version ou dois-je effectuer des mises à niveau incrémentielles ?**

  Vous pouvez presque toujours effectuer une mise à niveau vers la dernière version et ignorer les versions intermédiaires, sauf indication explicite spécifiée dans l'article **Nouveautés** pour la version vers laquelle vous effectuez la mise à niveau.
  Consultez le [guide de mise à niveau](/en-us/upgrade).

- **Un client peut-il effectuer une mise à niveau d'un environnement LTSR (Long Term Service Release) vers une version actuelle ?**

  Oui. Les clients ne sont pas tenus de conserver une version LTSR pendant une période prolongée. Les clients peuvent déplacer un environnement LTSR vers une version actuelle, en fonction des exigences et des fonctionnalités de l'entreprise.

- **Les versions mixtes de composants sont-elles autorisées ?**

  Dans chaque site, Citrix recommande la mise à niveau de tous les composants vers la même version. Bien que vous puissiez utiliser des versions antérieures de certains composants, certaines fonctionnalités de la version la plus récente risquent de ne pas être disponibles. Pour plus d'informations, voir Considérations d'environnement mixte.

- **À quelle fréquence une version actuelle doit-elle être mise à niveau ?**

  Les versions actuelles atteignent la fin de la période de maintenance (EOM) 6 mois après la date de publication. Citrix recommande aux clients d'adopter la dernière version actuelle. Les versions actuelles atteignent la fin du cycle de vie 18 mois après la date de publication.

  Pour plus d'informations, consultez la section [Cycle de vie de la version actuelle](https://www.citrix.com/sup
  lifecycle/milestones/citrix-virtual-apps-and-desktops.html).

- **Est-il recommandé d'effectuer une mise à niveau vers la version Long Term Service Release (LTSR) ou la version actuelle (CR) ?**

  Les versions actuelles (CR) offrent les fonctionnalités de virtualisation des applications, des bureaux et des serveurs les plus récentes et les plus innovantes. Ces versions vous permettent de rester à la pointe de la technologie et de devancer votre concurrence.

Les versions LTSR sont idéales pour les environnements de production de grandes entreprises qui préfèrent conserver la même version de base pendant une longue période.

For details, see [Servicing Options]( https://www.citrix.com/support/citrix-customer-success-services/citrix-virtual-apps-and-desktops-servicing-options.html).

- **Dois-je effectuer une mise à niveau de mes licences ?**

  Assurez-vous que la date de licence actuelle n'a pas expiré et qu'elle est valide pour la version vers laquelle vous effectuez la mise à niveau. Voir CTX111618. Pour plus d'informations sur le renouvellement, voir Licences de renouvellement de Customer Success Services.

- **Combien de temps dure une mise à niveau ?**

  Le temps nécessaire à la mise à niveau d'un déploiement varie en fonction de l'infrastructure et du réseau. Nous ne pouvons donc pas fournir de durée exacte.

- **Quelles sont les meilleures pratiques à suivre ?**

  Assurez-vous de comprendre et de suivre les conseils de préparation.

- **Quels systèmes d'exploitation sont pris en charge ?**

  L'article Configuration système requise correspondant à la version vers laquelle vous effectuez la mise à niveau répertorie les systèmes d'exploitation pris en charge.

  Si votre déploiement actuel utilise des systèmes d'exploitation qui ne sont plus pris en charge, reportez-vous à la section Systèmes d'exploitation antérieurs.

- **Quelles versions de VMware vSphere (vCenter + ESXi) sont prises en charge ?**

  L'article CTX131239 répertorie les hôtes et versions pris en charge, ainsi que des liens vers les problèmes connus.

- **Quelle est la date de fin de cycle de vie (EOL) de ma version ?**

  Consultez le tableau des produits.

- **Quels sont les problèmes connus avec la dernière version ?**

  - Citrix Virtual Apps and Desktops
  - StoreFront
  - Citrix Provisioning
  - Serveur de licences Citrix
  - Application Citrix Workspace pour Windows

### Informations supplémentaires

[Long Term Service Release (LTSR)](https://www.citrix.com/support/citrix-customer-success-services/citrix-virtual-apps-and-desktops-servicing-options.html)

Les mises à jour du déploiement **Long Term Service Release (LTSR)** utilisent des mises à jour cumulatives (CU). Une mise à jour cumulative met à jour les composants de base de la version LTSR, et chaque mise à jour cumulative comprend son propre metainstaller.

Chaque mise à jour cumulative a une documentation dédiée. Par exemple, pour la version LTSR 2203, vérifiez le lien sur la page **Nouveautés** de cette version LTSR pour la dernière mise à jour cumulative. Chaque page de mise à jour cumulative contient des informations sur la version prise en charge, des instructions et un lien vers le package de téléchargement de la mise à jour cumulative.

## Migrer

### Migrer vers le cloud

Vous pouvez utiliser l'outil de configuration automatisée pour Citrix Virtual Apps and Desktops pour migrer votre déploiement local vers le cloud. Pour de plus amples informations, consultez la section Migrer vers le cloud.

### Migration héritée

La migration déplace les données depuis déploiement antérieur vers une version plus récente. Le processus comprend l'installation de composants plus récents et la création d'un nouveau site, l'exportation de données à partir de l'ancienne batterie, puis l'importation des données vers le nouveau site.

Il n'existe aucun outil ou script pris en charge pour la migration des versions de XenApp et XenDesktop ou la migration des versions antérieures de Citrix Virtual Apps and Desktops. La *mise à niveau* est prise en charge pour les versions de Citrix Virtual Apps and Desktops répertoriées dans le Guide de mise à niveau Citrix et <!–> décrites dans cette documentation produit.

Pour le contenu de migration XenApp 6.x plus ancien, reportez-vous à la section suivante. Ni les scripts ni les articles ne sont pris en charge ou maintenus.

- Les scripts de migration Open Source pour les versions XenApp 6.x sont disponibles sur https://github.com/citrix/xa65migrationtool. Citrix ne prend pas en charge ni ne gère ces scripts de migration
- Modifications apportées dans la version 7.x
- Mettre à niveau une tâche XenApp 6.5 vers un nouveau VDA
- Migrer XenApp 6.x

# Mettre un déploiement à niveau

June 27, 2024

## Introduction

Vous pouvez mettre à niveau certains déploiements vers des versions plus récentes sans devoir d'abord configurer les nouvelles machines ou sites. C'est ce qu'on appelle une mise à niveau sur place.

Pour savoir quelles versions de Citrix Virtual Apps and Desktops vous pouvez mettre à niveau, consultez le Guide de mise à niveau Citrix.

Avant de procéder à la mise à niveau vers l'une des versions Citrix Virtual Apps and Desktops, assurez-vous que vos abonnement à Customer Success Services est toujours valide et n'a pas expiré. Pour plus d'informations sur le renouvellement, voir l'article Licences de renouvellement de Customer Success.

Pour lancer une mise à niveau, exécutez le programme d'installation à partir de la nouvelle version afin de mettre à niveau les composants principaux, les VDA et certains autres composants précédemment installés. Mettez ensuite à niveau les bases de données et le site.

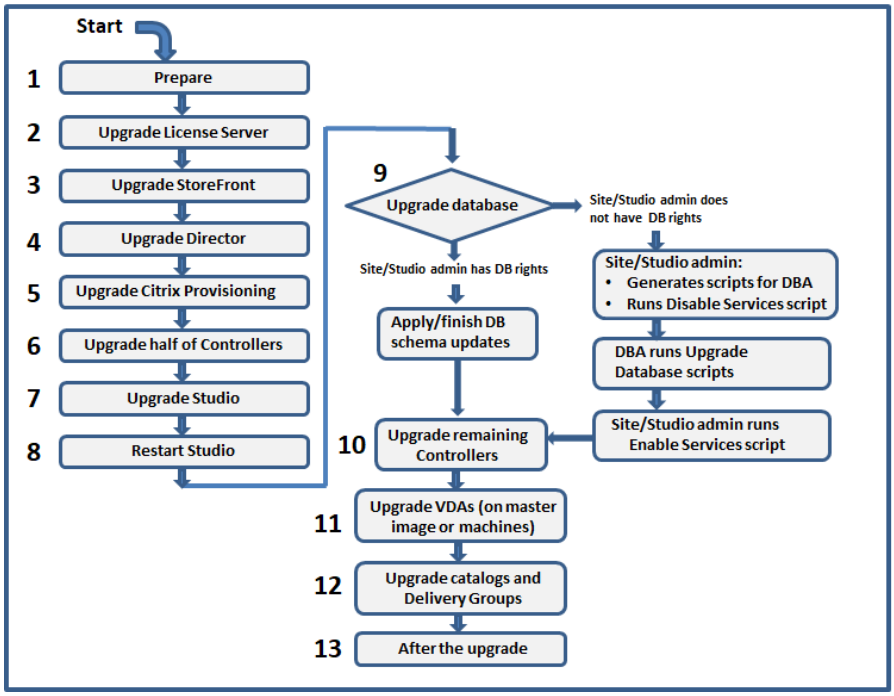
Vous pouvez mettre à niveau tout composant pouvant être installé avec le programme d'installation complet (et les programmes d'installation de VDA autonomes), s'il existe une version plus récente. Pour les autres composants qui ne sont pas installés avec le programme d'installation complet (tels que Citrix Provisioning et Profile Management), consultez la documentation de ce composant pour obtenir des instructions. Pour les mises à niveau de l'hôte, consultez la documentation appropriée.

Consultez toutes les informations dans cet article avant de procéder à une mise à niveau.

## Séquence de mise à niveau

Le diagramme suivant montre les étapes de la séquence de mise à niveau. La procédure de mise à niveau contient les détails de chaque étape du diagramme.




> **Remarque :**
>
> Pour éviter les échecs, vous devez mettre à niveau tous les Delivery Controller et la base de données avant d'effectuer les tâches liées au provisioning et aux groupes de mise à disposition, telles que la création d'un nouveau catalogue de machines, la suppression d'un catalogue de machines, la mise à jour d'une machine dans un groupe de mise à disposition, etc.

## Licences de droits hybrides

Les licences de droits hybrides sont des licences d'abonnement à durée déterminée qui sont fournies, en plus de l'abonnement au service cloud, lorsqu'un client passe d'une licence perpétuelle à un abonnement à un service cloud. Vous pouvez également acheter un module complémentaire de droits hybrides avec vos abonnements DaaS.

Si vous possédez une licence de droits hybrides avec un attribut SaaS, lorsque vous effectuez une mise à niveau vers Citrix Virtual Apps and Desktops LTSR 2203 et versions ultérieures, vous pouvez profiter de fonctionnalités non disponibles avec Citrix Virtual Apps and Desktops LTSR 1912. Ces fonctionnalités incluent le provisioning et l'hébergement de charges de travail dans des clouds publics, tels que Microsoft Azure, AWS EC2 et Google Cloud. Avant de déployer le nouveau fichier de licences, mettez à jour votre serveur de licences vers la version la plus récente.

Si vous avez accès à une licence de droits hybrides sans attribut SaaS, procédez comme suit pour accéder à la nouvelle licence de droits hybrides avec attribut SaaS :

> **Remarque :**
>
> - Vous recevez un e-mail contenant un nouveau code de licence. Pour plus d'informations, consultez Utiliser le code d'accès à la licence.
> - Vos licences existantes sont annulées. Les licences annulées doivent être supprimées des serveurs de licences, et une nouvelle licence doit être installée. Pour de plus amples informations, consultez la section Supprimer des fichiers de licences.

1. Accédez au portail Gestion des licences sur citrix.com et téléchargez le nouveau fichier de licence de droits hybrides avec les droits de provisioning cloud activés (attribut SaaS). Pour plus d'informations, consultez la section Télécharger des licences. L'image suivante montre le fichier de licence de droits hybrides avec attribut SaaS dans la section Incréments.


2. Installez le fichier de licence de droits hybrides sur le serveur de licences. Pour plus d'informations, consultez la section Installer des licences.
3. En cas de modification des éditions ou du modèle de licence, assurez-vous d'exécuter la commande Broker pour définir l'édition et le modèle, puis lancez la mise à niveau sur place. Pour plus d'informations sur les commandes Broker, consultez la section SDK PowerShell de Broker.

Pour plus d'informations sur la prise en charge du cloud public avec les versions actuelles et les versions LTSR de Citrix Virtual Apps and Desktops, consultez l'article CTX270373.

### Procédure de mise à niveau

La plupart des composants principaux du produit peuvent être mis à niveau en exécutant le programme d'installation du produit sur la machine contenant le composant.

Si une machine contient plusieurs composants (par exemple, Studio et Serveur de licences), tous les composants de cette machine sont mis à niveau, si le support produit contient des versions plus récentes de leur logiciel.

Pour utiliser les programmes d'installation :

- Pour exécuter l'interface graphique du programme d'installation complet du produit, ouvrez une session sur la machine, puis insérez le support ou montez le lecteur ISO pour la nouvelle version. Cliquez deux fois sur **Sélection automatique**.
- Pour utiliser l'interface de ligne de commande, exécutez la commande appropriée. Voir la section Installer à l'aide de la ligne de commande.

#### Étape 1 : Préparer

Avant de commencer une mise à niveau, assurez-vous d'être prêt. Lisez et complétez toutes les tâches nécessaires :

- Suppression de PvD, AppDisks et d'hôtes non pris en charge
- VDA dotés de composants PvD ou AppDisks
- Limitations
- Considérations d'environnement mixte
- Systèmes d'exploitation antérieurs
- Préparation
- Tests préliminaires du site
- Vérification de la version de SQL Server

#### Étape 2 : Mettre à niveau le serveur de licences

Si l'installation dispose d'une nouvelle version du logiciel Serveur de licences Citrix, mettez à niveau ce composant avant tout autre composant.

Si vous n'avez pas encore déterminé si votre serveur de licences est compatible avec la nouvelle version, il est essentiel que vous exécutiez le programme d'installation sur le serveur de licences avant de procéder à la mise à niveau des autres composants principaux.

#### Étape 3 : Mettre à niveau StoreFront

Si le support d'installation contient une nouvelle version du logiciel StoreFront, exécutez le programme d'installation sur la machine contenant le serveur StoreFront.

- Dans l'interface graphique, choisissez **Citrix StoreFront** dans la section **Étendre le déploiement**.
- À partir de la ligne de commande, exécutez `CitrixStoreFront-x64.exe`, qui est disponible dans le dossier `x64` du support d'installation de Citrix Virtual Apps and Desktops.

#### Étape 4 : Mettre à niveau Director

Si le support d'installation contient une nouvelle version du logiciel Director, exécutez le programme d'installation sur la machine contenant Director.

#### Étape 5 : Mettre à niveau Citrix Provisioning

Le support d'installation Citrix Provisioning est disponible séparément à partir du support d'installation de Citrix Virtual Apps and Desktops. Pour savoir comment installer et mettre à niveau le logiciel de machine cible et de serveur Citrix Provisioning, reportez-vous à la documentation du produit Citrix Provisioning.

#### Étape 6 : Mettre à niveau la moitié des Delivery Controller

Par exemple, si votre site dispose de quatre Controller, exécutez le programme d'installation sur deux d'entre eux.

Le fait de laisser la moitié des Controller actifs permet aux utilisateurs d'accéder au site. Les VDA peuvent s'enregistrer auprès des Controller restants. Il peut aussi arriver que le site dispose d'une capacité réduite car moins de Controller sont disponibles. La mise à niveau entraîne une brève interruption dans l'établissement de nouvelles connexions client au cours des dernières étapes de mise à niveau de la base de données. Le Controller mis à niveau ne peut pas traiter les demandes tant que l'intégralité du site n'a pas été mise à niveau.

Si votre site comporte un seul Controller, il est inutilisable lors de la mise à niveau.

Les tests de site préliminaires sont exécutés sur le premier Controller avant le démarrage effectif de la mise à niveau. Pour plus de détails, voir Tests préliminaires du site.

#### Étape 7 : Mettre à niveau Studio

Si vous n'avez pas encore mis à niveau Web Studio (car il se trouvait sur la même machine qu'un autre composant), exécutez le programme d'installation sur la machine contenant Studio.

> **Remarque :**
>
> Après la mise à niveau de Web Studio, les informations de version peuvent ne pas être mises à jour immédiatement. Il se peut que vous soyez invité à mettre à niveau Web Studio même s'il est déjà à jour. Pour résoudre le problème, accédez au serveur Web Studio, ouvrez le gestionnaire des services Internet (IIS), accédez à Page de démarrage > Sites > Site Web par défaut, puis sélectionnez **Redémarrer** dans le volet Gérer le site Web.

#### Étape 8 : Redémarrer Studio

Redémarrez Web Studio après sa mise à niveau. Le processus de mise à niveau reprend automatiquement.

### Étape 9 : Mettre à niveau la base de données et le site

> **Remarque :**
>
> Pour éviter les échecs, vous devez mettre à niveau tous les Delivery Controller et la base de données avant d'effectuer les tâches liées au provisioning et aux groupes de mise à disposition, telles que la création d'un nouveau catalogue de machines, la suppression d'un catalogue de machines, la mise à jour d'une machine dans un groupe de mise à disposition, etc.

Vérifiez Préparation pour connaître les autorisations requises pour mettre à jour le schéma des bases de données SQL Server.

- Si vous disposez des autorisations suffisantes pour mettre à jour le schéma de base de données SQL Server, vous pouvez lancer une mise à niveau automatique de la base de données. Passez à Mettre à niveau la base de données et le site automatiquement.
- Si vous ne disposez pas des autorisations de base de données suffisantes, vous pouvez lancer une mise à niveau manuelle utilisant des scripts et procéder avec l'aide de votre administrateur de base de données (qui dispose des autorisations requises). Pour une mise à niveau manuelle, l'utilisateur Studio génère les scripts, puis exécute les scripts qui activent et désactivent les services. L'administrateur de base de données exécute d'autres scripts qui mettent à jour le schéma de base de données, à l'aide de l'utilitaire SQLCMD ou de SQL Server Management Studio en mode SQLCMD. Passez à Mettre à niveau les bases de données et le site manuellement.
- Si vous disposez d'un déploiement multizone et que vous souhaitez mettre à niveau automatiquement la base de données et le site, Citrix recommande que la mise à niveau dbschema soit effectuée dans la même zone que celle qui héberge les bases de données SQL Server du site. Sinon, la mise à niveau automatique de la base de données et du site peut échouer

Citrix recommande fortement de sauvegarder la base de données avant de procéder à la mise à niveau. Voir CTX135207. Lors d'une mise à niveau de base de données, les services du produit sont désactivés. Pendant ce temps, les Controller ne peuvent pas initier de nouvelles connexions pour le site, ainsi effectuez une planification prudente.

#### Mettre à niveau la base de données et le site automatiquement

1. Lancez le logiciel Studio nouvellement mis à niveau.
2. Indiquez que vous souhaitez démarrer automatiquement la mise à niveau du site et confirmez que vous êtes prêt.

La mise à niveau de la base de données et du site se poursuit.

#### Mettre à niveau les bases de données et le site manuellement

1. Lancez le logiciel Studio nouvellement mis à niveau.

2. Indiquez que vous souhaitez mettre à niveau le site manuellement. L'Assistant vérifie la compatibilité du serveur de licences et des demandes de confirmation.
3. Vérifiez que vous avez sauvegardé la base de données.

   L'assistant génère et affiche ensuite les scripts et une checklist des étapes de mise à niveau. Si le schéma d'une base de données n'a pas changé depuis la mise à niveau de la version du produit, ce script n'est pas généré. Par exemple, si le schéma de la base de données de journalisation ne change pas, le script `UpgradeLoggingDatabase.sql` n'est pas généré.
4. Exécutez les scripts suivants dans l'ordre indiqué.

   - `DisableServices.ps1` : l'utilisateur de Studio exécute le script PowerShell sur un Controller pour désactiver les services du produit.
   - `UpgradeSiteDatabase.sql` : l'administrateur de la base de données exécute ce script SQL sur le serveur qui contient la base de données du site
   - `UpgradeMonitorDatabase.sql` : l'administrateur de la base de données exécute ce script SQL sur le serveur qui contient la base de données de surveillance.
   - `UpgradeLoggingDatabase.sql` : l'administrateur de la base de données exécute ce script SQL sur le serveur qui contient la base de données de journalisation de la configuration. Exécutez ce script uniquement si cette base de données change (par exemple, après l'application d'un correctif logiciel).
   - `EnableServices.ps1` : l'utilisateur de Studio exécute le script PowerShell sur un Controller pour activer les services du produit.

   Une fois la mise à niveau de la base de données terminée, et les services du produit activés, Studio teste automatiquement l'environnement et la configuration, puis génère un rapport HTML. Si des problèmes sont identifiés, vous pouvez restaurer la sauvegarde de la base de données. Après avoir résolu les problèmes, vous pouvez effectuer la mise à niveau de la base de données à nouveau.
5. Après avoir effectué les tâches de la check-list, cliquez sur **Terminer la mise à niveau**.

#### Étape 10 : Mettre à niveau les Delivery Controller restants

Depuis la version de Studio nouvellement mise à niveau, sélectionnez **Citrix Studio** *nom-site* dans le volet de navigation. Sous l'onglet **Tâches courantes**, sélectionnez **Mettre à niveau les Delivery Controller restants**.

> **Remarque :**
>
> Pour afficher l'option **Mettre à niveau les Delivery Controller restants**, créez au moins un catalogue de machines et un groupe de mise à disposition pour le site.

Après avoir effectué la mise à niveau et confirmé l'achèvement, fermez puis rouvrez Studio. Studio peut demander une mise à niveau du site supplémentaire pour enregistrer les services du Controller sur le site ou pour créer un ID de zone s'il n'existe pas.

#### Étape 11 : Mettre à niveau les VDA

> **Important :**
>
> Si vous mettez à niveau un VDA vers la version 1912 ou ultérieure, reportez-vous à la section Mise à niveau des VDA vers 1912 ou version ultérieure.

Exécutez le programme d'installation du produit sur des machines contenant les VDA.

Si vous avez utilisé Machine Creation Services et une image principale pour créer des machines, accédez à votre hôte et mettez à niveau le VDA sur l'image principale. Vous pouvez utiliser n'importe lequel des programmes d'installation VDA disponibles.

- Pour obtenir des conseils sur l'interface graphique, consultez Installer des VDA.
- Pour obtenir des conseils sur la ligne de commande, consultez Installer à l'aide de la ligne de commande.

Si vous avez utilisé Citrix Provisioning pour créer des machines, consultez la documentation du produit Citrix Provisioning pour obtenir des conseils sur la mise à niveau.

#### Étape 12 : Mettre à jour les catalogues de machines et les groupes de mise à disposition

- Mettre à jour les catalogues qui utilisent des machines avec des VDA mis à niveau.
- Mettre à niveau les catalogues qui utilisent des machines avec des VDA mis à niveau.
- Mettre à niveau les groupes de mise à disposition qui utilisent des machines avec des VDA mis à niveau.

#### Étape 13 : Après la mise à niveau

Après avoir terminé une mise à niveau, vous pouvez tester le site récemment mis à niveau. À partir de Studio, sélectionnez **Citrix Studio nom-du-site** dans le volet de navigation. Sous l'onglet **Tâches courantes**, sélectionnez **Tester le site**. Ces tests sont exécutés automatiquement après que vous ayez mis à niveau la base de données, mais vous pouvez les exécuter à tout moment.

Les tests peuvent échouer pour un Controller sur Windows Server 2016, lorsqu'une instance locale de Microsoft SQL Server Express est utilisée pour la base de données du site, si le service SQL Server Browser ne démarre pas. Pour éviter ce problème :

- Activez le service SQL Server Browser (si nécessaire), puis démarrez-le.

- Redémarrez le service SQL Server (SQLEXPRESS).

Mettez à niveau d'autres composants de votre déploiement. Pour plus d'informations, consultez la documentation produit suivante :

- StoreFront
- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Profile Management
- Citrix Provisioning
- Enregistrement de session
- Workspace Environment Management

Si vous devez remplacer le logiciel Microsoft SQL Server Express LocalDB par une version ultérieure, consultez Remplacer SQL Server Express LocalDB.

### Mise à niveau de Dbschema

Lorsque vous mettez à jour votre déploiement, plusieurs schémas de base de données peuvent être mis à niveau. Le tableau suivant répertorie les schémas de base de données mis à niveau au cours de la procédure :

| From/To | 1912 CU1 | 1912 CU2 | 1912 CU3 | 1912 CU4 | 1912 CU5 | 2203 RTM | 2203 CU1 | 2203 CU2 | 2203 CU3 |
|---|---|---|---|---|---|---|---|---|---|
| 7.15 RTM/CU | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 RTM | Config | Site; Config | Site; Config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU1 | | Site | Site; Config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU2 | | | Site; Config | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU3 | | | | Site; Monitor; config | Site; Monitor; config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU4 | | | | | Site; Config | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU5 | | | | | | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU6 | | | | | | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 1912 CU7 | | | | | | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging | Site; Monitor; config;logging |
| 2203 RTM | | | | | | | Config | Config | Config |
| 2203 CU1 | | | | | | | | Config | Config |
| 2203 CU2 | | | | | | | | | Config |

Définition des termes :

- Site : magasin de données du site. La mise à jour Dbschema est effectuée dans le magasin de données du site.
- Monitor : magasin de données de surveillance. La mise à jour Dbschema est effectuée dans le magasin de données de surveillance.
- Config : table de configuration. La version de Desktop Studio, les informations sur les licences ou les deux sont mises à jour dans la table de configuration.
- Logging : magasin de données de journalisation. La mise à jour Dbschema est effectuée dans le magasin de données de journalisation.

### Mettre à niveau des VDA vers 2203 ou version ultérieure

Si le composant Personal vDisk (PvD) a déjà été installé sur un VDA, ce VDA ne peut pas être mis à niveau vers la version 2203 ou ultérieure. Pour utiliser le nouveau VDA, vous devez désinstaller le VDA actuel, puis installer le nouveau VDA.

Cette instruction s'applique même si vous n'avez jamais utilisé PvD.

Voici comment le composant PvD a pu être installé dans les versions antérieures :

- Dans l'interface graphique du programme d'installation du VDA, PvD était une option sur la page **Composants supplémentaires**.
- Sur la ligne de commande, l'option `/baseimage` installait PvD. Si vous avez spécifié cette option ou utilisé un script contenant cette option, PvD a été installé.

Si vous ne savez pas si PvD est installé sur votre VDA, exécutez le programme d'installation du nouveau VDA (2203 ou version ultérieure) sur la machine ou l'image.

- Si PvD est installé, un message s'affiche indiquant qu'il existe un composant incompatible.
  - Sur l'interface graphique, cliquez sur **Annuler** sur la page contenant le message, puis confirmez que vous souhaitez fermer le programme d'installation.
  - À partir de l'interface de ligne de commande, la commande échoue simplement avec l'affichage du message.
- Si PvD n'est pas installé, la mise à niveau se poursuit.

#### Que faire

Si PvD n'est pas installé sur le VDA, suivez la procédure de mise à niveau habituelle.

Si PvD est installé sur le VDA :

1. Désinstallez le VDA actuel.
2. Installez le nouveau VDA.

Si vous souhaitez continuer à utiliser PvD sur vos machines Windows 10 (1607 et versions antérieures, sans mises à jour), le VDA 7.15 LTSR est la dernière version prise en charge.

> **Remarque :**
>
> *Puis-je utiliser Personal vDisk avec des bureaux Windows 7 dans XenApp et XenDesktop 7.15 LTSR ?*
>
> Citrix a exclu Personal vDisk (PvD) de XenApp et XenDesktop 7.6 LTSR, ce qui a été annoncé en janvier 2016. En outre, Citrix a annoncé la dépréciation de la technologie PvD et recommande aux clients d'utiliser Citrix App Layering. Citrix App Layering (version 4.4 et ultérieure) est un composant compatible avec XenApp et XenDesktop 7.15 LTSR. Toutefois, pour aider les clients dis-

> posant de déploiements PvD existants sur Windows 7 à migrer vers la technologie Citrix App Layering, Citrix a décidé de fournir une prise en charge limitée dans le temps pour les déploiements PvD pour les bureaux Windows 7 via des mises à jour cumulatives (CU) de XenApp et XenDesktop 7.15 LTSR jusqu'au 14 janvier 2020. Le composant PvD sera supprimé des CU LTSR et ne sera plus pris en charge après le 14 janvier 2020. En outre, l'utilisation de PvD pour Windows 7 au-delà du 14 janvier 2020 rendra les sites LTSR non conformes. De plus, PvD pour Windows 10 continue d'être exclu de la version 7.15 LTSR. Par conséquent, les clients ne doivent pas l'utiliser avec leurs sites 7.15 LTSR.

### Suppression de PvD, AppDisks et d'hôtes non pris en charge

Les technologies et types d'hôte suivants ne sont pas pris en charge dans les déploiements Citrix Virtual Apps and Desktops 7 Current Release :

- **Personal vDisks (PvD)** pour stocker des données à côté des machines virtuelles des utilisateurs dans les catalogues. L'entité de couche de personnalisation de l'utilisateur gère désormais la persistance de l'utilisateur.
- **AppDisks** pour gérer les applications utilisées dans les groupes de mise à disposition.
- **Types d'hôtes :** Azure Classic, CloudPlatform (le produit Citrix d'origine).
  - Pour connaître les types d'hôtes pris en charge dans cette version, consultez la section Configuration système requise.
  - Pour plus d'informations sur d'autres façons de continuer à utiliser ARM et AWS, reportez-vous à la section CTX270373.

Si votre déploiement actuel utilise des PvD ou des AppDisks, ou si vous avez des connexions à des types d'hôtes non pris en charge (Microsoft Azure Classic, par exemple), vous pouvez effectuer une mise à niveau vers la version 2006 (ou les versions ultérieures prises en charge) uniquement après avoir supprimé les éléments qui utilisent ces technologies. Si votre déploiement actuel utilise des connexions hôtes de cloud public (par exemple, AWS), assurez-vous que vous disposez d'une licence de droits hybrides avant de procéder à la mise à niveau. Lorsque le programme d'installation détecte une ou plusieurs technologies ou connexions hôtes non prises en charge sans licence de droits hybrides, la mise à niveau est suspendue ou s'arrête et un message explicatif s'affiche. Les journaux du programme d'installation contiennent des détails.

Pour garantir une mise à niveau réussie, consultez et suivez les instructions applicables pour supprimer les éléments non pris en charge.

- Supprimer les PvD
- Supprimer les AppDisks
- Supprimer les éléments hôtes non pris en charge

Même si vous n'avez pas utilisé de PvD ou AppDisks dans votre déploiement, les MSI associés peuvent avoir été inclus dans une installation ou une mise à niveau de VDA antérieure. Avant de pouvoir mettre à niveau vos VDA vers la version 2006 (ou une version ultérieure prise en charge), vous devez supprimer ces logiciels, même si vous ne l'avez jamais utilisé. Lorsque vous utilisez l'interface graphique, cette suppression peut être effectuée pour vous ou vous pouvez inclure des options de suppression lors de l'utilisation de l'interface de ligne de commande. Pour plus d'informations, consultez la section Mise à niveau de VDA dotés de composants PvD ou AppDisks.

#### Supprimer les PvD

Une mise à niveau de déploiement ne peut pas réussir tant que vous n'avez pas supprimé toutes les machines configurées pour utiliser PvD. Cela affecte les catalogues et les groupes de mise à disposition.

Pour supprimer PvD des groupes et catalogues :

1. Dans Studio, si un groupe de mise à disposition contient des machines d'un catalogue qui utilise PvD, supprimez ces machines du groupe.
2. Dans Studio, supprimez tous les catalogues contenant des machines utilisant PvD.

**Mises à niveau de VDA :** la mise à niveau de déploiement ne détecte pas si les composants AppDisk ou PvD sont installés sur les VDA. Cependant, les programmes d'installation du VDA le font. Pour plus d'informations, consultez la section VDA dotés de composants PvD ou AppDisks.

Si vous prévoyez d'utiliser App Layering au lieu de PvD, reportez-vous à la section Migration de PvD vers App Layering pour plus d'informations sur le déplacement des données.

#### Supprimer les AppDisks

Une mise à niveau de déploiement ne peut pas se poursuivre tant que vous ne supprimez pas AppDisks de tous les groupes de mise à disposition qui les utilisent, puis supprimez les AppDisks eux-mêmes.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation de Studio.
2. Sélectionnez un groupe, puis cliquez sur **Gérer les AppDisks** dans le volet Action.
3. Cliquez sur l'action qui supprime AppDisk du groupe.
4. Répétez les étapes 2 et 3 pour chaque groupe de mise à disposition qui utilise AppDisks.
5. Sélectionnez **AppDisks** dans le volet de navigation de Studio.
6. Sélectionnez un AppDisk et cliquez sur l'action qui supprime l'AppDisk.
7. Répétez les étapes 5 et 6 pour chaque AppDisk.

**Mises à niveau de VDA :** la mise à niveau de déploiement ne détecte pas si les composants AppDisk ou PvD sont installés sur les VDA. Cependant, les programmes d'installation du VDA le font. Pour plus d'informations, consultez la section VDA dotés de composants PvD ou AppDisks.

#### Supprimer les éléments hôtes non pris en charge

Une mise à niveau de déploiement vers la version 2006 (ou une version ultérieure prise en charge) ne peut pas se poursuivre si le site possède des connexions à des types d'hôtes non pris en charge, tels que Citrix CloudPlatform ou Microsoft Azure Classic. Effectuez les tâches suivantes avant de tenter une mise à niveau.

À partir de Studio :

- Supprimez toutes les connexions aux hôtes non pris en charge.
- Si un groupe de mise à disposition contient des machines d'un catalogue créé avec une image principale à partir d'un hôte non pris en charge, supprimez ces machines du groupe.
- Supprimez tous les catalogues créés à l'aide d'une image principale à partir d'un hôte non pris en charge.

#### VDA dotés de composants PvD ou AppDisks

Si les composants qui activent les technologies PvD et AppDisks sont installés sur un VDA, ce VDA ne peut pas être mis à niveau tant que ces composants ne sont pas supprimés.

> **Remarque :**
>
> Lors de la mise à niveau vers la version 1912, vous deviez désinstaller le VDA actuel, puis installer le nouveau VDA. Dans cette version, il vous est demandé si vous souhaitez que Citrix supprime le composant, puis continue la mise à niveau.

Les composants AppDisk et PvD peuvent avoir été installés dans des versions VDA antérieures, même si vous n'avez jamais utilisé ces technologies :

- Interface graphique : dans les programmes d'installation de VDA, la page **Composants supplémentaires** contenait l'option **Citrix AppDisk/Personal vDisk**. Les versions 7.15 LTSR et 7.x antérieures activait cette option par défaut. Donc, si vous avez accepté les valeurs par défaut (ou activé explicitement l'option dans toute version qui l'offrait), ce composant a été installé.
- CLI : la spécification de l'option `/baseimage` installait le composant.

**Que faire** Si le programme d'installation du VDA ne détecte pas les AppDisks ou les composants PvD dans le VDA actuellement installé, la mise à niveau se poursuit comme d'habitude.

Si le programme d'installation détecte des composants AppDisks ou PvD dans le VDA actuellement installé :

- Interface graphique : la mise à niveau s'interrompt. Un message vous demande si vous souhaitez supprimer automatiquement les composants non pris en charge. Si vous cliquez sur **OK**, les composants sont supprimés automatiquement et la mise à niveau se poursuit.

- CLI : pour éviter l'échec de la commande, incluez les options suivantes dans la commande :
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

### Limitations

Les limites suivantes s'appliquent aux mises à niveau :

- **Installation sélective des composants :** si vous installez ou mettez à niveau les composants vers la nouvelle version, mais ne choisissez pas de mettre à niveau d'autres composants (sur différentes machines) qui nécessitent une mise à niveau, Studio vous le rappelle. Par exemple, supposons qu'une mise à niveau comprend de nouvelles versions de Controller et de Studio. Vous effectuez la mise à niveau du Controller, mais vous n'exécutez pas le programme d'installation sur la machine sur laquelle Studio est installé. Studio ne vous laissera pas continuer à gérer le site tant que vous n'aurez pas mis à niveau Studio.

  Vous n'avez pas besoin de mettre à niveau les VDA, mais Citrix vous recommande de mettre à niveau tous les VDA pour vous permettre d'utiliser toutes les fonctionnalités disponibles.
- **Versions préliminaires :** vous ne pouvez pas effectuer une mise à niveau à partir d'une version Early Release, Technology Preview ou Preview.
- **Composants sur les systèmes d'exploitation antérieurs :** vous ne pouvez pas installer les VDA actuels sur des systèmes d'exploitation qui ne sont plus pris en charge par Microsoft ou Citrix. Pour de plus amples informations, consultez la section Systèmes d'exploitation antérieurs.
- **Environnements/sites mixtes :** si vous devez continuer à exécuter des sites de version antérieure et des sites de version actuelle, consultez la section Considérations d'environnement mixte.
- **Sélection de produit :** lorsque vous effectuez une mise à niveau à partir d'une version antérieure, vous ne choisissez pas ni ne spécifiez le produit (Citrix Virtual Apps ou Citrix Virtual Apps and Desktops) qui a été défini lors de l'installation initiale.

### Considérations d'environnement mixte

Lorsque vous effectuez la mise à niveau, Citrix vous recommande de mettre à niveau tous les composants et les VDA, vous pouvez accéder à toutes ses nouvelles fonctionnalités dans votre édition et votre version.

Par exemple, bien que vous puissiez utiliser les VDA actuels dans les déploiements contenant des versions antérieures de Controller, les nouvelles fonctionnalités de la version actuelle peuvent ne pas

être disponibles. Des problèmes d'enregistrement de VDA peuvent aussi se produire lors de l'utilisation de versions antérieures.

Dans certains environnements, vous risquez de ne pas pouvoir mettre à niveau tous les VDA vers la version la plus récente. Dans ce cas, lorsque vous créez un catalogue de machines, vous pouvez spécifier la version du VDA installée sur les machines. (C'est ce qu'on appelle le niveau fonctionnel.) Par défaut, ce paramètre spécifie la version minimale recommandée du VDA. La valeur par défaut est suffisante pour la plupart des déploiements. Pensez à modifier le paramètre pour une version antérieure uniquement si le catalogue contient des VDA antérieurs à la valeur par défaut. Le mélange de versions VDA dans un catalogue de machines n'est pas recommandé.

Si un catalogue est créé avec le paramètre de valeur par défaut de VDA minimum, et une ou plusieurs machines possèdent une version de VDA antérieure à la version par défaut, ces machines ne peuvent pas s'enregistrer auprès du Controller et ne fonctionneront pas.

Pour de plus amples informations, consultez la section Versions VDA et niveaux fonctionnels.

#### Plusieurs sites avec différentes versions

Lorsque votre environnement contient des sites/batterie dont les versions de produits diffèrent (par exemple, si vous disposez d'un site XenDesktop 7.18 et d'un site Citrix Virtual Apps and Desktops 1909), Citrix recommande d'utiliser StoreFront pour regrouper les applications et les bureaux provenant de versions de produits différentes. Pour plus de détails, consultez la documentation StoreFront.

Dans un environnement mixte, continuez à utiliser les versions de Studio et de Director pour chaque version, mais assurez-vous que les différentes versions sont installées sur des machines distinctes.

### Systèmes d'exploitation antérieurs

Imaginons que vous ayez installé une version antérieure d'un composant sur une machine qui exécutait une version du système d'exploitation prise en charge. Maintenant, vous voulez utiliser une version de composant plus récente, mais ce système d'exploitation n'est plus pris en charge pour la version actuelle du composant.

Par exemple, supposons que vous avez installé un VDA serveur sur une machine Windows Server 2008 R2. Vous souhaitez maintenant mettre à niveau ce VDA vers la version actuelle, mais Windows Server 2008 R2 n'est pas pris en charge dans la version actuelle vers laquelle vous effectuez une mise à niveau.

Lorsque vous essayez d'installer ou de mettre à niveau un composant sur un système d'exploitation qui n'est plus autorisé, un message d'erreur s'affiche, tel que « Impossible d'installer sur ce système d'exploitation …».

Ces considérations s'appliquent à la mise à niveau des versions actuelles et LTSR. (Cela n'affecte pas l'application d'unités de stockage à une version LTSR.)

Suivez les liens pour savoir quels systèmes d'exploitation sont pris en charge :

- Citrix Virtual Apps and Desktops (Version actuelle) :
  - Delivery Controller, Studio, Director, VDA, Serveur d'impression universel
  - Service d'authentification fédérée
  - Pour StoreFront, la réinitialisation du mot de passe en libre-service et l'enregistrement de session, consultez l'article sur la configuration requise pour la version actuelle.
- Pour les versions LTSR, voir les listes de composants pour votre version LTSR et CU. (Sélectionnez votre version LTSR sur la page principale de la documentation du produit Citrix Virtual Apps and Desktops.)

#### Systèmes d'exploitation non valides

Le tableau suivant répertorie les systèmes d'exploitation antérieurs qui ne sont pas valides pour l'installation / la mise à niveau de composants dans la version actuelle. Il indique la dernière version de composant valide prise en charge pour chaque système d'exploitation répertorié et la version du composant lorsque l'installation et la mise à niveau sont devenues non valides.

Les systèmes d'exploitation du tableau incluent les service packs et les mises à jour.

| Système d'exploitation | Composant/fonctionnalité | Dernière version valide | Installation/mise à niveau |
|---|---|---|---|
| Windows 7 et Windows 8 | VDA | 7.15 LTSR | 7.16 |
| Windows 7 et Windows 8 | Autres composants du programme d'installation | 7.17 | 7.18 |
| Versions de Windows 10 antérieures à la version 1607 | VDA | 7.15 LTSR | 7.16 |
| Version Windows 10 x86 | VDA | 1906.2.0 | 1909 |
| Windows Server 2008 R2 | VDA | 7.15 LTSR | 7.16 |
| Windows Server 2008 R2 | Autres composants du programme d'installation | 7.17 | 7.18 |
| Windows Server 2012 | VDA | 7.15 LTSR | 7.16 |
| Windows Server 2012 | Autres composants du programme d'installation | 7.17 | 7.18 |
| Windows Server 2012 R2 | Autres composants du programme d'installation * | 1912 LTSR | 2003 |
| Windows Server 2012 R2 | Server VDI | 7.15 LTSR | 7.16 |

Windows XP et Windows Vista ne sont pas valides pour les composants ou technologies 7.x.

* S'applique à Delivery Controller, Studio, Director et VDA.

**Ce que vous pouvez faire**

Vous avez plusieurs solutions. Vous pouvez :

- Continuer avec le système d'exploitation actuel
- Réimager ou mettre à niveau la machine
- Ajouter de nouvelles machines, puis supprimer les anciennes machines

**Continuer avec le système d'exploitation actuel** Ces méthodes sont possibles pour les VDA. Si vous souhaitez continuer à utiliser des machines avec le système d'exploitation antérieur, vous pouvez choisir l'une des options suivantes :

- Continuer à utiliser la version du composant installé.
- Télécharger la dernière version de composant valide, puis mettre à niveau le composant vers cette version. (Cela suppose que la dernière version de composant valide n'est pas déjà installée.)

Par exemple, supposons que vous ayez un VDA 7.14 sur une machine Windows 7 SP1. La dernière version valide de VDA sur les machines Windows 7 est XenApp and XenDesktop 7.15 LTSR. Vous pouvez soit continuer à utiliser 7.14, soit télécharger un VDA LTSR 7.15, puis mettre à jour votre VDA vers cette version. Ces versions antérieures de VDA fonctionnent dans des déploiements contenant des Delivery Controller avec des versions plus récentes. Par exemple, un VDA 7.15 LTSR peut se connecter à un Controller Citrix Virtual Apps and Desktops 7 1808.

**Réimager ou mettre à niveau la machine** Ces méthodes sont possibles pour les VDA et autres machines qui n'ont pas de composants de base (tels que Delivery Controller) installés. Sélectionnez l'une des options suivantes :

- Après avoir mis la machine hors service (en activant le mode de maintenance et en permettant la fermeture de toutes les sessions), vous pouvez la réimager sur une version du système d'exploitation Windows prise en charge, puis installer la dernière version du composant.
- Pour mettre à niveau le système d'exploitation sans réimager, désinstallez le logiciel Citrix avant de mettre à niveau le système d'exploitation (cela inclut les mises à niveau internes de votre système d'exploitation. Par exemple, Windows 10 version 1903 à Windows 10 version 1909). Dans le cas contraire, le logiciel Citrix ne sera pas pris en charge. Ensuite, installez le nouveau composant.
- Pour mettre à niveau le système d'exploitation d'une machine VDA sans réimageage, vous devez d'abord installer une version du VDA prise en charge par le système d'exploitation vers lequel vous effectuez la mise à niveau ou mettre à niveau le VDA après la mise à niveau du système d'exploitation. Dans le cas contraire, le logiciel Citrix ne sera pas pris en charge. Vous

pouvez effectuer une mise à niveau vers les versions minimales du système d'exploitation suivantes lorsque vous effectuez une mise à niveau sur place sans désinstaller le VDA :

  - Windows 11 avec mise à jour cumulative 2023-07 pour Windows 11 (KB5028185) ou version ultérieure installée (build 22621.1992 ou version ultérieure).
  - Windows 10 avec mise à jour dynamique 2023-07 pour Windows 10 (KB5028311) installée.

- Si la version de Windows vers laquelle vous envisagez de procéder à la mise à niveau n'est pas conforme aux directives susmentionnées, vous devez désinstaller le VDA avant de mettre à niveau le système d'exploitation, puis installer une version de VDA prise en charge une fois la mise à niveau du système d'exploitation terminée.

**Ajouter de nouvelles machines, puis supprimer les anciennes machines** Cette méthode est possible si vous devez mettre à niveau le système d'exploitation sur des machines qui contiennent un Delivery Controller ou un autre composant principal.

Citrix recommande que tous les Controller d'un site aient le même système d'exploitation. La séquence de mise à niveau suivante minimise l'intervalle lorsque différents Controller ont des systèmes d'exploitation différents.

1. Prenez un instantané de tous les Delivery Controller sur le site, puis sauvegardez la base de données du site.
2. Installez les nouveaux Delivery Controller sur des serveurs vierges avec système d'exploitation pris en charge Par exemple, installez un Controller sur deux machines Windows Server 2016.
3. Ajoutez les nouveaux Controller au site.
4. Supprimez les Controller qui s'exécutent sur des systèmes d'exploitation qui ne sont pas valides pour la version actuelle. Par exemple, retirez deux Controller sur deux machines Windows Server 2008 R2. Suivez les recommandations pour supprimer les Controller dans Delivery Controller.

## Préparation

Avant de commencer une mise à niveau, consultez les informations suivantes et effectuez les tâches nécessaires.

> **Remarque :**
>
> Bien que la mise à niveau des VDA survienne plus tard dans la séquence de mise à niveau, il est conseillé de choisir un programme d'installation et de vérifier la procédure avant de commencer la mise à niveau, afin de savoir à quoi s'attendre.

### Choisir un programme d'installation et une interface

Utilisez le programme d'installation du produit entier depuis l'image ISO de produit pour mettre à niveau les composants. Vous pouvez mettre à niveau les VDA à l'aide du programme d'installation du produit entier ou de l'un des programmes d'installation de VDA autonomes. Tous les programmes d'installation offrent des interfaces graphique et de ligne de commande.

Pour de plus amples informations, consultez Programmes d'installation.

**Caractéristiques de l'installation :** une fois le travail de préparation terminé et que vous êtes prêt à démarrer le programme d'installation, l'article d'installation vous montre ce qui s'affiche sur l'écran (si vous utilisez l'interface graphique) ou ce qu'il faut taper (si vous utilisez l'interface de ligne de commande).

- Installer/mettre à niveau les composants principaux à l'aide de l'interface graphique
- Installer/mettre à niveau les composants principaux à l'aide de la ligne de commande
- Installer/mettre à niveau des VDA à l'aide de l'interface graphique
- Installer/mettre à niveau des VDA à l'aide de la ligne de commande

Si vous avez installé un VDA mono-session avec le programme d'installation `VDAWorkstationCoreSetup.exe`, Citrix vous recommande de mettre à niveau à l'aide de ce programme d'installation. Si vous utilisez le programme d'installation VDA du produit entier ou le programme d'installation `VDAWorkstationSetup.exe` pour mettre à niveau le VDA, il est possible que les composants initialement exclus soient installés, sauf si vous les ignorez/excluez expressément de la mise à niveau.

Lors de la mise à niveau d'un VDA vers la version actuelle, un redémarrage de l'ordinateur se produit pendant le processus de mise à niveau. (Cette exigence a commencé avec la version 7.17.) Ce processus ne peut pas être évité. La mise à niveau reprend automatiquement après le redémarrage (sauf si vous spécifiez `/noresume` sur la ligne de commande).

### Actions de base de données

Sauvegardez les bases de données de site, de contrôle et de journalisation de la configuration. Suivez les instructions de l'article CTX135207. Si vous rencontrez des problèmes après la mise à niveau, vous pouvez restaurer la sauvegarde.

Pour plus d'informations sur la mise à niveau des versions de SQL Server qui ne sont plus prises en charge, reportez-vous à la section Vérification de la version de SQL Server. (Cela fait référence à SQL Server qui est utilisé pour les bases de données de journalisation de site, de contrôle et de journalisation de la configuration.)

Microsoft SQL Server Express LocalDB est installé automatiquement pour une utilisation avec le cache d'hôte local. Si vous devez remplacer une version antérieure, la nouvelle version doit être SQL Server

Express LocalDB 2019. Pour plus d'informations sur le remplacement de SQL Server Express LocalDB par la nouvelle version après la mise à niveau des composants et du site, reportez-vous à la section Remplacer SQL Server Express LocalDB.

#### Assurez-vous que vos licences Citrix sont à jour

Pour un aperçu complet de la gestion du système de licences Citrix, consultez la section Activer, mettre à niveau et gérer les licences Citrix.

Vous pouvez utiliser le programme d'installation du produit complet pour effectuer la mise à niveau du serveur de licences. Vous pouvez également télécharger et mettre à niveau les composants de licence séparément. Consultez la section Mettre à niveau.

Avant la mise à niveau, assurez-vous que votre abonnement à Customer Success Services/Software Maintenance/Subscription Advantage est toujours valide pour la nouvelle version du produit. La date doit être au moins 2021.11.15.

#### Assurez-vous que votre serveur de licences Citrix est compatible

Assurez-vous que votre serveur de licences Citrix est compatible avec la nouvelle version. Il existe deux façons de procéder :

- Avant de procéder à la mise à niveau de tout autre composant Citrix, exécutez le programme d'installation `XenDesktopServerSetup.exe` depuis l'ISO sur la machine contenant un Delivery Controller. S'il y a des problèmes d'incompatibilité, le programme d'installation le signale avec les étapes recommandées pour les résoudre.
- À partir du répertoire `XenDesktop Setup` sur le support d'installation, exécutez la commande `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`. L'affichage indique si le serveur de licences est compatible. Si le serveur de licences est incompatible, mettez à niveau le serveur de licences.

#### Sauvegarder les modifications StoreFront

Avant une mise à niveau, si vous avez apporté des modifications aux fichiers dans `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, tels que *default.ica* et *usernamepassword.tfrm*, sauvegardez-les pour chaque magasin. Après la mise à niveau, vous pouvez les restaurer pour rétablir vos modifications.

#### Fermez les applications et les consoles

Avant de démarrer une mise à niveau, fermez tous les programmes qui pourraient entraîner des verrouillages de fichier, y compris les consoles d'administration et les sessions PowerShell.

Le redémarrage de la machine assure que tout verrouillage de fichier est annulé et qu'aucune mise à jour Windows n'est en attente.

Avant de démarrer une mise à niveau, arrêtez et désactivez tout service d'agent de surveillance tiers.

#### Vérifiez que vous disposez des autorisations adéquates

En plus d'être un utilisateur du domaine, vous devez être un administrateur local sur les machines sur lesquelles vous mettez à niveau les composants du produit.

La base de données du site et le site peuvent être mis à niveau automatiquement ou manuellement. Pour une mise à niveau automatique de la base de données, les autorisations de l'utilisateur de Studio doivent inclure la possibilité de mettre à jour le schéma de base de données SQL Server (par exemple, le rôle de base de données `db_securityadmin` ou `db_owner`). Pour de plus amples informations, veuillez consulter Bases de données.

Si l'utilisateur Studio ne possède pas ces autorisations, l'initiation de la mise à niveau manuelle d'une base de données générera des scripts. L'utilisateur Studio exécute certains des scripts à partir de Studio. L'administrateur de la base de données exécute d'autres scripts à l'aide d'un outil tel que SQL Server Management Studio.

#### Autres tâches de préparation

- Sauvegardez les modèles et mettez à niveau les hyperviseurs, le cas échéant
- Effectuez les tâches de préparation en fonction de votre plan de continuité des activités.

### Tests préliminaires du site

Lorsque vous mettez à niveau des Delivery Controller et un site, des tests préliminaires de site sont exécutés avant le début de la mise à niveau. Ces tests vérifient les points suivants :

- La base de données du site peut être contactée et a été sauvegardée
- Les connexions aux services Citrix essentiels fonctionnent correctement
- L'adresse du serveur de licences Citrix est disponible
- La base de données de journalisation de la configuration est accessible

- Assurez-vous de disposer d'une licence de droits hybrides si vous souhaitez ajouter des connexions hôtes de cloud public (par exemple, AWS). Dans le cas contraire, le test préliminaire sur site est suspendu ou s'arrête et un message explicatif s'affiche.

Une fois les tests exécutés, vous pouvez afficher un rapport des résultats. Vous pouvez alors résoudre tous les problèmes détectés et réexécuter les tests. Si vous ne parvenez pas à exécuter les tests de site préliminaires et à résoudre les problèmes, cela peut avoir un impact sur le fonctionnement de votre site.

Le rapport contenant les résultats du test est un fichier HTML (`PreliminarySiteTestResult.html`) dans le même répertoire que les journaux d'installation. Ce fichier est créé s'il n'existe pas. Si le fichier existe, son contenu est remplacé.

#### Exécuter les tests

- Lorsque vous utilisez l'interface graphique du programme d'installation pour effectuer la mise à niveau, l'assistant inclut une page dans laquelle vous pouvez démarrer les tests, puis afficher le rapport. Une fois que vous avez exécuté les tests, consulté le rapport et résolu les problèmes détectés, vous pouvez réexécuter les tests. Une fois les tests terminés, cliquez sur Suivant pour continuer avec l'assistant.
- Lorsque vous utilisez l'interface de ligne de commande pour mettre à niveau, les tests s'exécutent automatiquement. Par défaut, si un test échoue, la mise à niveau n'est pas effectuée. Après avoir affiché le rapport et résolu les problèmes, réexécutez la commande.

Citrix recommande de toujours exécuter les tests de site préliminaires, puis de résoudre les problèmes avant de poursuivre la mise à niveau du Controller et du site. Les bénéfices potentiels de ce processus justifient le temps passé à exécuter les tests. Cependant, vous pouvez ignorer cette action recommandée.

- Lors de la mise à niveau avec l'interface graphique, vous pouvez choisir d'ignorer les tests et de poursuivre la mise à niveau.
- Lors de la mise à niveau à partir de la ligne de commande, vous ne pouvez pas ignorer les tests. Par défaut, tout échec de test de site entraîne l'échec du programme d'installation, sans effectuer la mise à niveau. Dans la plupart des cas, si vous ajouter l'option `/ignore_site_test_failure`, les échecs de test de site sont ignorés et la mise à niveau continue. (Consultez la section Vérification de la version de SQL Server pour connaître les exceptions.)

#### Lors de la mise à niveau de plusieurs Controller

Lorsque vous démarrez une mise à niveau sur un Controller, puis démarrez une mise à niveau d'un autre Controller sur le même site (avant la fin de la première mise à niveau) :

- Si les tests de site préliminaires ont été effectués sur le premier Controller, la page des tests de site préliminaires n'apparaît pas dans l'assistant de l'autre Controller.
- Si les tests sur le premier Controller sont en cours lorsque vous démarrez la mise à niveau sur l'autre Controller, la page de tests de site apparaît dans l'assistant sur l'autre Controller. Cependant, si les tests sur le premier Controller se terminent, seuls les résultats des tests du premier Controller sont conservés.

#### Échecs de test non liés à l'intégrité du site

- Si les tests de site préliminaires échouent en raison d'une mémoire insuffisante, augmentez la mémoire disponible, puis réexécutez les tests.
- Si vous avez l'autorisation de mettre à niveau, mais pas d'exécuter des tests de site, les tests de site préliminaires échouent. Pour résoudre ce problème, réexécutez le programme d'installation avec un compte d'utilisateur autorisé à exécuter les tests.

### Vérification de la version de SQL Server

Le déploiement de Citrix Virtual Apps and Desktops nécessite une version prise en charge de Microsoft SQL Server pour les bases de données de journalisation du site, de contrôle et de configuration. La mise à niveau d'un déploiement Citrix avec une version de SQL Server qui n'est plus prise en charge peut entraîner des problèmes de fonctionnalité et le site ne sera pas pris en charge.

Pour savoir quelles versions de SQL Server sont prises en charge pour la version Citrix vers laquelle vous effectuez une mise à niveau, consultez l'article Configuration requise correspondant à cette version.

Lors de la mise à niveau d'un Controller, le programme d'installation Citrix vérifie la version SQL Server actuellement installée et utilisée pour les bases de données de journalisation du site, de contrôle et de configuration.

- Si la vérification détermine que la version de SQL Server actuellement installée n'est pas une version prise en charge dans la version Citrix vers laquelle vous effectuez une mise à niveau :
  - Interface graphique : la mise à niveau s'arrête avec un message. Cliquez sur **Je comprends**, puis cliquez sur **Annuler** pour fermer le programme d'installation de Citrix. (Vous ne pouvez pas poursuivre la mise à niveau.)
  - Interface de ligne de commande : la commande échoue (même si vous avez inclus l'option `/ignore_db_check_failure`avec la commande).

  Mettez à niveau la version de SQL Server, puis redémarrez la mise à niveau Citrix.

- Si la vérification ne peut pas déterminer la version de SQL Server qui est actuellement installée, vérifiez si votre version actuellement installée est prise en charge dans la version vers laquelle vous mettez à niveau (Configuration requise).
  - Interface graphique : la mise à niveau s'arrête avec un message.
    * Si la version de SQL Server actuellement installée est prise en charge, cliquez sur **Je comprends** pour fermer le message, puis cliquez sur **Suivant** pour continuer la mise à niveau Citrix.
    * Si la version de SQL Server actuellement installée n'est pas prise en charge, cliquez sur **Je comprends** pour fermer le message, puis cliquez sur **Annuler** pour mettre fin à la mise à niveau Citrix. Mettez à niveau votre SQL Server vers une version prise en charge, puis redémarrez la mise à niveau Citrix.
  - Interface de ligne de commande : la commande échoue avec un message. Après la fermeture du message :
    * Si la version de SQL Server actuellement installée est prise en charge, exécutez à nouveau la commande avec l'option `/ignore_db_check_failure`.
    * Si la version de SQL Server actuellement installée n'est pas prise en charge, mettez à niveau votre SQL Server vers une version prise en charge. Exécutez à nouveau la commande pour démarrer la mise à niveau de Citrix.

#### Mise à niveau de SQL Server

Si vous mettez en place de nouveaux serveurs SQL Server et migrez la base de données de site, les chaînes de connexion doivent être mises à jour.

Si le site utilise actuellement SQL Server Express pour la base de données du site (que Citrix a installé automatiquement lors de la création du site) :

1. Installez la dernière version de SQL Server Express.
2. Détachez la base de données.
3. Attachez la base de données au nouveau SQL Server Express.
4. Migrez les chaînes de connexion.

Pour plus d'informations, consultez Configuration des chaînes de connexion et la documentation du produit Microsoft SQL Server.

### Remplacer SQL Server Express LocalDB

Microsoft SQL Server Express LocalDB est une fonctionnalité de SQL Server Express que le cache d'hôte local utilise de manière autonome. Le cache d'hôte local ne nécessite aucun composant de SQL Server Express autre que SQL Server Express LocalDB.

Si vous avez installé une version Delivery Controller antérieure à 1912, puis mis à niveau votre déploiement vers la version 1912 ou ultérieure, Citrix ne met pas automatiquement à niveau la version de SQL Server Express LocalDB. Pourquoi ? Parce que vous pouvez avoir des composants non-Citrix qui reposent sur SQL Server Express LocalDB. Si vous avez des composants non-Citrix qui utilisent SQL Server Express LocalDB, assurez-vous que la mise à niveau de SQL Server Express LocalDB ne perturbe pas ces composants. Pour mettre à niveau (remplacer) la version de SQL Server Express LocalDB, suivez les instructions de cette section.

- **Lors de la mise à niveau des Delivery Controller vers Citrix Virtual Apps and Desktops version 1912 ou 2003 :** la mise à niveau de SQL Server Express LocalDB est facultative. Le cache d'hôte local fonctionne correctement, sans perte de fonctionnalité, que vous mettiez à niveau SQL Server Express LocalDB ou non. Nous avons ajouté la possibilité de passer à une version plus récente de SQL Server Express LocalDB en cas de préoccupations concernant la fin de la prise en charge par Microsoft de SQL Server Express LocalDB 2014.
- **Lors de la mise à niveau des Delivery Controller vers des versions Citrix Virtual Apps and Desktops antérieures à 2003 :** la version prise en charge est SQL Server Express LocalDB 2019. Si vous avez initialement installé un Delivery Controller antérieur à la version 1912 et que vous n'avez pas remplacé SQL Server Express LocalDB par la version plus récente depuis, vous devez remplacer ce logiciel de base de données maintenant. Sinon, le cache d'hôte local ne fonctionnera pas.

Ce dont vous avez besoin :

- Le support d'installation de Citrix Virtual Apps and Desktops (pour la version vers laquelle vous avez mis à niveau). Le support contient une copie de Microsoft SQL Server Express LocalDB 2019.
- Un outil Windows Sysinternals que vous téléchargez à partir de Microsoft.

Procédure :

1. Effectuez la mise à niveau de vos composants, bases de données et site Citrix Virtual Apps and Desktops. (Ces mises à niveau de la base de données affectent les bases de données de journalisation de la configuration, de surveillance et de site. Elles n'affectent pas la base de données du cache d'hôte local qui utilise SQL Server Express LocalDB.)
2. Sur le Delivery Controller, téléchargez `PsExec` depuis Microsoft. Consultez le document Microsoft PsExec v2.2.
3. Arrêtez Citrix High Availability Service.
4. À partir de l'invite de commandes, exécutez `PsExec` et basculez vers le compte de service réseau.

   ```
   psexec -i -u "NT AUTHORITY\NETWORKSERVICE"cmd
   ```

Le cas échéant, vous pouvez utiliser `whoami` pour confirmer que l'invite de commandes est exécutée en tant que compte de service réseau.

```
whoami
```

```
nt authority\networkservice
```

5. Accédez au dossier contenant SqlLocalDB.

```
cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
```

6. Arrêtez et supprimez `CitrixHA` (LocalDB).

```
SqlLocalDB stop CitrixHA
```

```
SqlLocalDB delete CitrixHA
```

7. Supprimez les fichiers associés dans `C:\Windows\ServiceProfiles\NetworkService`.

```
HADatabaseName.*
HADatabaseName_log.*
HAImportDatabaseName.*
HAImportDatabaseName_log.*
<!--NeedCopy-->
```

Conseil : votre déploiement peut ne pas avoir `HAImportDatabaseName.*` et `HAImportDatabaseNam.*`

8. Désinstallez SQL Server Express LocalDB 2014 du serveur, à l'aide de la fonctionnalité Windows de suppression des programmes.
9. Installez SQL Server Express LocalDB 2019. Dans le dossier `Support > SQLLocalDB` sur le support d'installation de Citrix Virtual Apps and Desktops, double-cliquez sur `sqllocaldb.msi`. Un redémarrage peut être requis pour terminer l'installation. (Le nouveau SQLLocalDB réside dans `C:\Program Files\Microsoft SQL Server\150\Tools\Binn`.)
10. Démarrez Citrix High Availability Service.
11. Assurez-vous que la base de données Cache hôte local a été créée sur chaque Delivery Controller. Cela confirme que le service haute disponibilité (broker secondaire) peut prendre le relais, si nécessaire.
    - Sur le serveur =Controller, accédez à `C:\Windows\ServiceProfiles\NetworkService`.
    - Vérifiez que `HaDatabaseName.mdf` et `HaDatabaseName_log.ldf` sont créés.

# Sauvegarder ou faire migrer votre configuration

June 27, 2024

Cette fonctionnalité vous permet d'effectuer une sauvegarde de vos configurations DaaS. Les sauvegardes facilitent le processus de migration des configurations d'un site cloud vers un autre. Elles facilitent également la récupération immédiate d'un site en cas d'urgence.
Vous pouvez utiliser les méthodes suivantes pour effectuer des sauvegardes :

1. Sauvegarde + Restauration
    a) Intégrée à WebStudio.
2. Outil de configuration automatisée (ACT)
    a) Outil basé sur PowerShell. Installez l'outil pour l'utiliser.

Les sauvegardes peuvent être utilisées pour :

1. Restauration
2. Migration

Citrix recommande les outils suivants pour les scénarios décrits.

## Sauvegarde

| Environnement | Cas d'utilisation | Outil recommandé | Considérations spéciales | Lien |
|---|---|---|---|---|
| DaaS | Sauvegardes planifiées et à la demande | Sauvegarde + Restauration | Citrix conserve la sauvegarde et l'utilisateur peut la télécharger si nécessaire | Sauvegarde + Restauration dans Studio |
| Local | Sauvegardes à la demande | ACT | L'utilisateur conserve la sauvegarde | Sauvegarder et restaurer à l'aide de l'outil de configuration automatisée |

## Migration

| Environnement | Cas d'utilisation | Outil recommandé | Considérations spéciales | Lien |
|---|---|---|---|---|
| Sur site ou dans le cloud | Faire migrer un site local vers un site DaaS | ACT | | Faire migrer un site local vers le cloud |
| | Consolider plusieurs sites locaux en un seul site DaaS | ACT | Fusion de sites | Fusionner plusieurs sites locaux en un seul site cloud |
| Site local vers site local | Faire migrer un site local vers un autre site local | ACT | | Guide de preuve de concept : Outil de configuration automatisée - Migration de site local vers site local |
| | Consolider plusieurs sites locaux en un autre site local | ACT | Fusion de sites | Guide de preuve de concept : Outil de configuration automatisée - Migration de site local vers site local |
| | | | | Fusionner plusieurs sites locaux en un seul site cloud |
| Cloud vers cloud | Faire migrer un site DaaS vers un autre site DaaS | ACT | | Faire migrer une configuration cloud vers le cloud |
| Consolider plusieurs sites DaaS en un seul site DaaS | ACT | Fusion de sites | | Faire migrer une configuration cloud vers le cloud |

| Environnement | Cas d'utilisation | Outil recommandé | Considérations spéciales | Lien |
|---|---|---|---|---|
| | | | | Faire migrer plusieurs sites locaux vers un seul site cloud |

## Sécuriser

June 27, 2024

Citrix Virtual Apps and Desktops offre une solution sécurisée de par sa conception qui vous permet de configurer votre environnement selon vos besoins en termes de sécurité.

Un problème de sécurité souvent rencontré en informatique concerne la perte ou le vol des données des travailleurs mobiles. En hébergeant les applications et les bureaux, Citrix Virtual Apps and Desktops sépare les données sensibles et la propriété intellectuelle des machines de point de terminaison de manière sécurisée en conservant les données dans un centre de données. Lorsque des stratégies sont activées pour autoriser le transfert des données, toutes les données sont cryptées.

Les centres de données Citrix Virtual Apps and Desktops facilitent également les réponses aux incidents avec un service de contrôle et de gestion centralisé. Director permet au département informatique de surveiller et d'analyser les données qui sont accédées sur le réseau et Studio permet au département informatique d'appliquer des correctifs logiciels et de remédier à la plupart des vulnérabilités dans le centre de données au lieu de résoudre les problèmes localement sur chaque machine utilisateur.

Citrix Virtual Apps and Desktops simplifie également les audits et assure la conformité à la règlementation car les enquêteurs peuvent utiliser une piste d'audit centralisée pour déterminer les personnes qui ont accès aux applications et aux données. Director collecte des données d'historique concernant les mises à jour du système et l'utilisation des données utilisateur en accédant à la journalisation de la configuration et l'API OData.

L'administration déléguée vous permet de configurer des rôles administrateur pour contrôler l'accès à Citrix Virtual Apps and Desktops à un niveau plus précis. Ceci permet une plus grande souplesse dans votre organisation pour fournir à certains administrateurs un accès complet aux tâches, opérations et étendues alors que d'autres administrateurs ont un accès limité.

Citrix Virtual Apps and Desktops fournit un contrôle plus précis aux administrateurs sur les utilisateurs en appliquant des stratégies à différents niveaux du réseau (à partir du niveau local de l'unité d'

organisation). Ce contrôle des stratégies détermine si un utilisateur, une machine ou des groupes d'utilisateurs et de périphériques peuvent se connecter, imprimer, copier/coller, ou mapper les lecteurs locaux, ce qui peut réduire les problèmes de sécurité causés par des travailleurs tiers intérimaires. Les administrateurs peuvent également utiliser la fonctionnalité Desktop Lock, les utilisateurs finaux peuvent alors uniquement utiliser le bureau virtuel tout en empêchant tout accès au système d'exploitation local de la machine utilisateur.

Les administrateurs peuvent améliorer la sécurité de Citrix Virtual Apps ou Citrix Virtual Desktops en configurant le site pour utiliser le protocole de sécurité TLS (Transport Layer Security) du Controller ou entre utilisateurs finaux et Virtual Delivery Agents (VDA). Le protocole peut également être activé sur un site pour fournir l'authentification de serveur, le cryptage du flux de données et le contrôle de l'intégrité des messages pour une connexion TCP/IP.

Citrix Virtual Apps and Desktops fournit également l'authentification multi-facteurs pour Windows ou une application spécifique. L'authentification multi-facteurs peut également être utilisée pour gérer toutes les ressources mises à disposition par Citrix Virtual Apps and Desktops. Ces méthodes comprennent :

- Jetons
- Cartes à puce
- RADIUS
- Kerberos
- Biométrie

Citrix Virtual Desktops peut être intégré à plusieurs des solutions de sécurité tierces, allant de la gestion de l'identité à un logiciel antivirus. Une liste des produits pris en charge peut être obtenue à l'adresse http://www.citrix.com/ready.

Les versions Premium de Citrix Virtual Apps and Desktops sont certifiées pour la norme des critères communs. Pour consulter la liste de ces normes, accédez à https://www.commoncriteriaportal.org/cc/.

## Authentification FIDO2 et WebAuthn

June 27, 2024

### Autorisation locale et authentification virtuelle à l'aide de FIDO2 et WebAuthn

Les utilisateurs peuvent s'authentifier auprès d'applications qui exploitent FIDO2 ou WebAuthn dans leur session virtuelle à l'aide de clés de sécurité FIDO2 et de la biométrie intégrée sur des appareils dotés du TPM 2.0 et de Windows Hello.

Pour plus d'informations sur FIDO2, consultez FIDO2 : WebAuthn et CTAP.

Pour plus d'informations sur l'utilisation de cette fonctionnalité, consultez Redirection FIDO2.

> **REMARQUE**
>
> Notez que cette fonctionnalité ne prend pas en charge la connexion à la session virtuelle à l'aide de WebAuthn ou FIDO2. Cette fonctionnalité permet uniquement d'utiliser ces méthodes d'authentification dans les applications de la session virtuelle.
>
> Cette fonctionnalité n'est pas prise en charge dans les scénarios double-hop.

### Prise en charge

| Système d'exploitation hôte de la session | Authentification des applications Web | Authentification des applications UWP |
|---|---|---|
| Windows Server 2016 | Pris en charge via la redirection USB | Non pris en charge |
| Windows Server 2019 | Pris en charge | Non pris en charge |
| Windows Server 2022 | Pris en charge | Pris en charge |
| Windows 10 | Pris en charge | Pris en charge |
| Windows 11 | Pris en charge | Pris en charge |

Pour plus d'informations, veuillez consulter les exigences ci-dessous.

### Authentification des applications Web

#### Exigences

Les exigences pour utiliser les authentifications FIDO2 et WebAuthn avec des applications Web sont les suivantes :

##### Plan de contrôle Citrix

- Citrix Virtual Apps and Desktops 2009 ou version ultérieure

##### Hôte de la session

- Système d'exploitation

  - Windows 10 1809 ou version ultérieure
  - Windows Server 2019 ou version ultérieure
- VDA
  - Windows : version 2009 ou ultérieure

#### Machine cliente

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Linux : veuillez vous référer à l'application Workspace pour connaître la configuration système requisepour Linux.
- Application Workspace
  - Windows : version 2009.1 ou ultérieure
  - Linux : 2303 ou version ultérieure

#### Exigences relatives au navigateur Web

- Navigateurs 64 bits uniquement

#### Méthodes d'authentification prises en charge

- Clé de sécurité FIDO2
- Windows Hello
  - TPM 2.0
  - Biométrie intégrée
    - Reconnaissance faciale
    - Scanner d'empreintes digitales
  - WebAuthn

### Authentification des applications UWP

Avec la publication de Citrix Virtual Apps and Desktops 2112, Citrix prend en charge les authentifications WebAuthn et FIDO2 dans les applications UWP.

Des applications telles que Microsoft Teams, Microsoft Outlook pour Office 365 et OneDrive utilisent une application UWP pour l'authentification en tant que lien vers Azure Active Directory. Citrix prend désormais en charge l'utilisation de FIDO2 pour authentifier ces applications.

### Exigences

Les exigences pour utiliser les authentifications FIDO2 et WebAuthn avec les applications UWP sont les suivantes :

#### Plan de contrôle Citrix

- Citrix Virtual Apps and Desktops 2112 ou version ultérieure

#### Hôte de la session

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Windows Server 2022 ou version ultérieure
- VDA
  - Windows : version 2112 ou ultérieure

#### Machine cliente

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Linux : veuillez vous référer à l'application Workspace pour connaître la configuration système requisepour Linux.
- Application Workspace
  - Windows : version 2009.1 ou ultérieure
  - Linux : 2303 ou version ultérieure

#### Méthodes d'authentification prises en charge

- Clé de sécurité FIDO2
- Windows Hello
  - TPM 2.0
  - Biométrie intégrée
    - Reconnaissance faciale
    - Scanner d'empreintes digitales
  - WebAuthn

> **Remarque :**
>
> Dans les scénarios où la redirection FIDO2 n'est pas disponible car la fonctionnalité n'est pas prise en charge par le client, le VDA ou le système d'exploitation, les clés FIDO2 basées sur USB peuvent être redirigées à l'aide de la redirection USB.
> Il est également possible d'utiliser la redirection USB pour rediriger les clés FIDO2 basées sur USB dans les scénarios où la redirection FIDO2 est disponible. Dans ce cas, vous devez désactiver la redirection FIDO2 et configurer les règles de redirection USB appropriées.
> Consultez la documentation sur les règles de redirection de périphérique USB pour plus de détails sur la façon de configurer les règles de redirection USB.

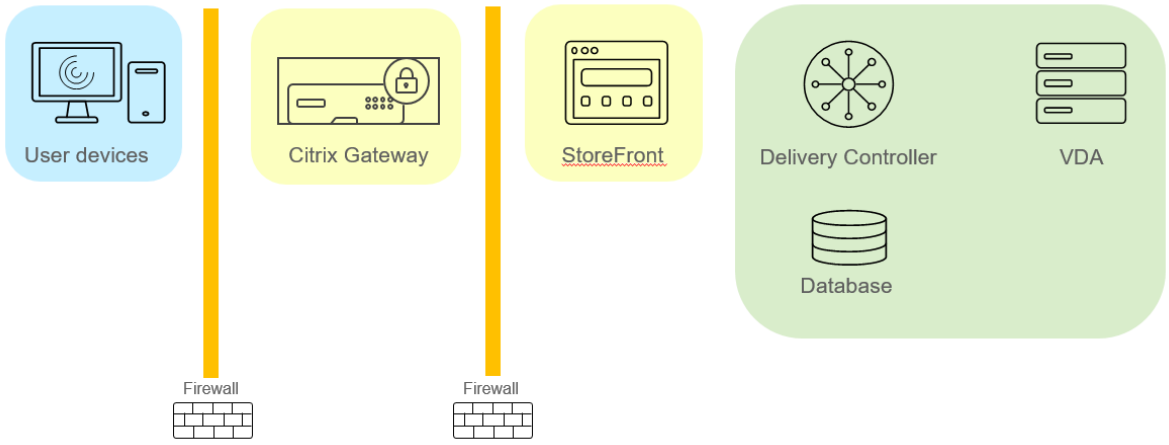
## Intégrer Citrix Virtual Apps and Desktops avec Citrix Gateway

June 27, 2024

Les serveurs StoreFront sont déployés et configurés pour gérer l'accès aux données et ressources publiées. Pour un accès distant, il est recommandé d'ajouter Citrix Gateway devant StoreFront.

> **Remarque :**
>
> Pour obtenir la procédure détaillée de configuration de l'intégration de Citrix Virtual Apps and Desktops avec Citrix Gateway, consultez la documentation de StoreFront.

Le diagramme suivant illustre un exemple d'un déploiement de Citrix simplifié qui inclut Citrix Gateway. Citrix Gateway communique avec StoreFront pour protéger les applications et les données fournies par Citrix Virtual Apps and Desktops. Les machines utilisateur exécutent l'application Citrix Workspace pour créer une connexion sécurisée et accéder à leurs applications, postes de travail et fichiers.



Les utilisateurs se connectent et s'authentifient à l'aide de Citrix Gateway. Citrix Gateway est déployé et sécurisé dans la DMZ. L'authentification à deux facteurs est configurée. En fonction des informations d'identification qu'ils saisissent, les utilisateurs recevront les ressources et applications auxquelles ils sont autorisés à accéder. Les applications et les données sont sur des serveurs appropriés (non illustrés dans le diagramme). Séparez les serveurs utilisés pour des applications et des données sensibles.

## Considérations de sécurité et meilleures pratiques

June 27, 2024

> **Remarque :**
>
> Votre entreprise peut être tenue de satisfaire à certaines normes de sécurité pour remplir ses obligations réglementaires. Ce document ne traite pas de ce sujet, car ces normes de sécurité évoluent continuellement. Pour obtenir les informations les plus récentes sur les normes de sécurité et les produits Citrix, consultez http://www.citrix.com/security/.

### Bonnes pratiques en matière de sécurité

Maintenez à jour toutes les machines de votre environnement avec des correctifs de sécurité. L'un des avantages est de pouvoir utiliser des clients légers comme terminaux, ce qui vous simplifie énormément la tâche.

Protégez toutes les machines de votre environnement avec un logiciel antivirus.

Envisagez d'utiliser un logiciel anti-programme malveillant spécifique à la plate-forme.

Lors de l'installation du logiciel, installez sur les chemins par défaut fournis.

- Si vous installez le logiciel dans un emplacement de fichiers autre que le chemin par défaut fourni, pensez à ajouter des mesures de sécurité supplémentaires, telles que des autorisations restreintes, à votre emplacement de fichiers.

Toutes les communications réseau doivent être correctement sécurisées et cryptées pour répondre à votre stratégie de sécurité. Vous pouvez sécuriser toutes les communications entre vos ordinateurs Microsoft Windows avec IPSec ; reportez-vous à la documentation de votre système d'exploitation pour plus d'informations à ce sujet. De plus, les communications entre les machines utilisateurs et les bureaux sont sécurisées via Citrix SecureICA, configuré par défaut sur un cryptage 128 bits. Vous pouvez configurer SecureICA lorsque vous créez ou mettez à jour un groupe de mise à disposition.

> **Remarque :**
>
> Citrix SecureICA fait partie du protocole ICA/HDX, mais n'est pas un protocole de sécurité réseau conforme aux normes comme TLS (Transport Layer Security). Vous pouvez également sécuriser les communications réseau entre les machines utilisateur et les postes de travail à l'aide de TLS. Pour configurer TLS, reportez-vous à la section TLS (Transport Layer Security).

Appliquez les recommandations Windows pour la gestion de comptes. Ne créez pas de compte sur un modèle ou une image avant sa duplication par Machine Creation Services ou Provisioning Services. Ne planifiez pas de tâches à l'aide de comptes de domaine privilégiés stockés. Ne créez pas manuellement de comptes de machines Active Directory partagés. Ces recommandations permettront d'éviter une attaque de machines par l'obtention des mots de passe de compte persistants locaux et leur utilisation pour se connecter à des images partagées MCS et PVS appartenant à d'autres utilisateurs.

#### Pare-feux

Protégez toutes les machines de votre environnement avec des pare-feu de périmètre, y compris aux limites des enclaves.

Toutes les machines de votre environnement devraient être protégées par un pare-feu personnel. Lorsque vous installez des composants principaux et des VDA (Virtual Delivery Agents), vous pouvez choisir que les ports requis pour le composant de la fonctionnalité de communication soient ouverts automatiquement si le service Pare-feu Windows est détecté (même si le pare-feu n'est pas activé). Vous pouvez également configurer ces ports de pare-feu manuellement. Si vous utilisez un autre pare-feu, vous devez le configurer manuellement.

Si vous faites migrer un environnement classique vers cette version, il peut être nécessaire de repositionner un pare-feu de périmètre existant ou d'en ajouter de nouveaux. Supposons, par exemple, qu'un pare-feu de périmètre soit positionné entre un client classique et un serveur de base de données dans le centre de données. Avec cette version, ce pare-feu de périmètre doit être positionné de façon telle que le bureau virtuel et la machine utilisateur se trouvent d'un côté du pare-feu, et les serveurs de bases de données et les Delivery Controller du centre de données de l'autre côté. Envisagez par conséquent de créer une enclave dans votre centre de données qui contiendra les serveurs de bases de données et les Controller. Il peut également être recommandé de mettre en place une protection entre la machine utilisateur et le bureau virtuel.

> **Remarque :**
>
> Les ports TCP 1494 et 2598 sont utilisés par les protocoles ICA et CGP. Ils sont donc susceptibles d'être ouverts afin que les utilisateurs se trouvant hors du centre de données puissent y accéder. Citrix vous recommande de ne pas utiliser ces ports à d'autres fins pour éviter tout risque d'attaque des interfaces d'administration. Les ports 1494 et 2598 sont officiellement enregistrés

> auprès de l'IANA (Internet Assigned Number Authority, voir http://www.iana.org/).

#### Sécurité des applications

Pour empêcher les actions malveillantes d'utilisateurs non administrateurs, nous vous recommandons de configurer les règles AppLocker Windows pour les programmes d'installation, les applications, les exécutables et les scripts sur l'hôte VDA et sur le client Windows local.

### Gérer les privilèges utilisateur

Accordez aux utilisateurs uniquement les droits qui leur sont nécessaires. Les privilèges Microsoft Windows sont toujours appliqués aux bureaux de la manière habituelle : vous configurez les privilèges à l'aide de l'attribution des droits utilisateur et de l'appartenance aux groupes via la stratégie de groupe. L'un des avantages de cette version est qu'il est possible d'octroyer à un utilisateur des droits d'administration sur un bureau sans lui accorder le contrôle physique de l'ordinateur qui héberge ce bureau.

Veuillez noter ce qui suit lors de la planification des privilèges des bureaux :

- Par défaut, lorsque des utilisateurs non privilégiés se connectent à un bureau, ils voient le fuseau horaire du système exécutant le bureau au lieu de celui de leur propre machine utilisateur. Pour savoir comment autoriser les utilisateurs à voir leur heure locale lorsqu'ils utilisent des bureaux, veuillez consulter l'article Gérer les groupes de mise à disposition.
- Un utilisateur qui est administrateur d'un bureau dispose d'un contrôle total sur ce dernier. S'il s'agit d'un bureau regroupé et non d'un bureau dédié, tous les autres utilisateurs de ce bureau, y compris les utilisateurs futurs, doivent lui faire confiance. Tous les utilisateurs doivent être conscients que ce genre de situation peut représenter un risque potentiel permanent pour la sécurité de leurs données. Cette remarque ne s'applique pas aux bureaux dédiés, qui n'ont qu'un seul utilisateur ; celui-ci ne doit être l'administrateur d'aucun autre bureau.
- Un utilisateur qui est administrateur d'un bureau peut généralement installer des logiciels sur ce bureau, y compris des logiciels potentiellement malveillants. Il a aussi la possibilité de surveiller ou de contrôler le trafic sur tout réseau connecté au bureau.

### Gérer les droits d'ouverture de session

Des droits d'ouverture de session sont requis pour les comptes d'utilisateur et les comptes d'ordinateur. À l'instar des privilèges Microsoft Windows, les droits d'ouverture de session sont toujours appliqués aux bureaux de la manière habituelle : vous configurez les droits d'ouverture de session à l'aide de l'attribution des droits utilisateur et de l'appartenance aux groupes via la stratégie de groupe.

Les droits d'ouverture de session Windows sont les suivants : ouverture de session locale, ouverture de session via les Services Bureau à distance, ouverture de session sur le réseau (accès à cet ordinateur depuis le réseau), ouverture de session en tant que traitement par lots et ouverture de session en tant que service.

Pour les comptes d'ordinateur, accordez aux ordinateurs uniquement les droits d'ouverture de session dont ils ont besoin. Le droit d'ouverture de session « Accéder à cet ordinateur à partir du réseau » est obligatoire :

- Sur les VDA, pour les comptes d'ordinateur des Delivery Controller.
- Sur les Delivery Controller, pour les comptes d'ordinateur des VDA. Voir Découverte de Controller basée sur unité d'organisation Active Directory.
- Sur les serveurs StoreFront, pour les comptes d'ordinateur des autres serveurs dans le même groupe de serveurs StoreFront.

Pour les comptes d'utilisateur, accordez aux utilisateurs uniquement les droits d'ouverture de session dont ils ont besoin.

Selon Microsoft, le droit d'ouverture de session « Autoriser l'ouverture de session par les services Bureau à distance » est accordé par défaut au groupe Utilisateurs du Bureau à distance (excepté sur les contrôleurs de domaine).

La stratégie de sécurité de votre organisation peut stipuler explicitement que ce groupe soit supprimé de ce droit d'ouverture de session. Considérez l'approche suivante :

- Le Virtual Delivery Agent (VDA) de l'OS multi-session utilise les Services Bureau à distance Microsoft. Vous pouvez configurer le groupe Utilisateurs du Bureau à distance en tant que groupe restreint, et contrôler l'appartenance au groupe via des stratégies de groupe Active Directory. Référez-vous à la documentation Microsoft pour plus d'informations.
- Pour les autres composants de Citrix Virtual Apps and Desktops, y compris le VDA pour OS mono-session, le groupe Utilisateurs du Bureau à distance n'est pas requis. Étant donné que le groupe Utilisateurs du Bureau à distance ne nécessite pas le droit d'ouverture de session « Autoriser l'ouverture de session au travers des services Bureau à distance » pour ces composants, vous pouvez le supprimer. Autres tâches :
  - Si vous administrez ces ordinateurs via les Services Bureau à distance, assurez-vous que tous les administrateurs sont déjà membres du groupe Administrateurs.
  - Si vous n'administrez pas ces ordinateurs via les Services Bureau à distance, vous pouvez désactiver les Services Bureau à distance sur ces ordinateurs.

Bien qu'il soit possible d'ajouter des utilisateurs et des groupes au droit d'ouverture de session « Interdire l'ouverture de session par les services Bureau à distance », l'interdiction de droits d'ouverture de session n'est généralement pas recommandée. Référez-vous à la documentation Microsoft pour plus d'informations.

### Configurer les droits des utilisateurs

L'installation de Delivery Controller crée les services Windows suivants :

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService Microsoft) : gère les comptes d'ordinateurs Active Directory pour les machines virtuelles.
- Citrix Analytics (NT SERVICE\CitrixAnalytics) : collecte des informations sur l'utilisation de la configuration du site, si cette collecte a été approuvée par l'administrateur du site. Ces informations sont ensuite envoyées à Citrix pour aider à améliorer le produit.
- Citrix App Library (NT SERVICE\CitrixAppLibrary) : prend en charge la gestion et le provisioning d'AppDisks, l'intégration d'AppDNA et la gestion d'App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService) : sélectionne les applications ou bureaux virtuels qui sont disponibles pour les utilisateurs.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging) : enregistre toutes les modifications de configuration et d'autres modifications apportées par les administrateurs du site.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService) : référentiel à l'échelle du site pour la configuration partagée.
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin) : gère les autorisations accordées aux administrateurs.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest) : gère les auto-tests des autres services Delivery Controller.
- Citrix Host Service (NT SERVICE\CitrixHostService) : stocke des informations sur les infrastructures d'hyperviseur utilisées dans un déploiement Citrix Virtual Apps ou Citrix Virtual Desktops, et offre également des fonctionnalités utilisées par la console pour énumérer les ressources dans un pool d'hyperviseurs.
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService) : orchestre la création de machines virtuelles de bureau.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor) : collecte des métriques pour Citrix Virtual Apps ou Citrix Virtual Desktops, stocke les données d'historique, et fournit une interface de requête pour la résolution des problèmes et les outils de reporting.
- Citrix Storefront Service (NT SERVICE\CitrixStorefront) : prend en charge la gestion de StoreFront. (Ne fait pas partie du composant StoreFront).
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService) : prend en charge les opérations d'administration privilégiée de StoreFront. (Ne fait pas partie du composant StoreFront).
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService) : propage les données de configuration depuis la base de données du site principal vers le cache d'hôte local.
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService) : sélectionne les applications ou bureaux virtuels qui sont disponibles pour les utilisateurs, lorsque la base de don-

nées du site principal n'est pas disponible.

L'installation de Delivery Controller crée également les services Windows suivants. Ces services sont également créés lorsqu'ils sont installés avec d'autres composants Citrix :

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc) : prend en charge la collecte d'informations de diagnostic destinées au support technique de Citrix.
- Service de télémétrie Citrix (NT SERVICE\CitrixTelemetryService) : collecte des informations de diagnostic à des fins d'analyse par Citrix, de façon à ce que les résultats de l'analyse et les recommandations puissent être consultés par les administrateurs pour diagnostiquer les problèmes avec le site.

L'installation de Delivery Controller crée également le service Windows suivant. Il n'est pas utilisé pour le moment. S'il est activé, désactivez-le.

- Citrix Remote Broker Provider (NT SERVICE\XaXdCloudProxy)

L'installation de Delivery Controller crée également les services Windows suivants. Ces derniers ne sont pas utilisés actuellement, mais doivent être activés. Ne les désactivez pas.

- Citrix Orchestration Service (NT SERVICE\CitrixOrchestration)
- Citrix Trust Service (NT SERVICE\CitrixTrust)

À l'exception du service Citrix Storefront Privileged Administration Service, le droit d'ouverture de session Ouvrir une session en tant que service et les privilèges Ajuster les quotas de mémoire pour un processus, Générer des audits de sécurité et Remplacer un jeton de niveau processus sont accordés à ces services. Vous n'avez pas besoin de changer ces droits d'utilisateur. Ces privilèges ne sont pas utilisés par le Delivery Controller et sont automatiquement désactivés.

### Configurer les paramètres du service

À l'exception du service Citrix StoreFront Privileged Administration Service et du Service de télémétrie Citrix, les services Windows Delivery Controller répertoriés ci-dessus dans la section Configurer les droits des utilisateurs sont configurés pour ouvrir une session sous l'identité NETWORK SERVICE. Ne modifiez pas ces paramètres de service.

Le service Citrix Config Synchronizer a besoin que le compte NETWORK SERVICE appartienne au groupe Administrateur local sur le Delivery Controller. Cela permet au cache d'hôte local de fonctionner correctement.

Le service Citrix StoreFront Privileged Administration Service est configuré pour ouvrir une session sous l'identité Système local (NT AUTHORITY\SYSTEM). Ceci est requis pour les opérations de Delivery Controller et de StoreFront qui ne sont normalement pas disponibles pour les services (y compris la création de sites IIS Microsoft). Ne modifiez pas ses paramètres de service.

Le Service de télémétrie Citrix est configuré pour ouvrir une session sous sa propre identité spécifique au service.

Vous pouvez désactiver le Service de télémétrie Citrix. Outre ce service, et les services qui sont déjà désactivés, ne désactivez aucun des autres services Windows Delivery Controller.

## Configurer les paramètres de registre

Il n'est plus nécessaire d'activer la création de noms de fichiers et de dossiers au format 8.3 sur le système de fichiers du VDA. La clé de registre **NtfsDisable8dot3NameCreation** peut être configurée pour désactiver la création de noms de fichiers et de dossiers au format 8.3. Vous pouvez également configurer ce comportement à l'aide de la commande **fsutil.exe behavior set disable8dot3**.

## Implications en termes de sécurité du scénario de déploiement

Votre environnement utilisateur peut se composer soit de machines utilisateur non gérées par votre entreprise et totalement sous le contrôle de l'utilisateur, soit de machines utilisateur gérées et administrées par votre entreprise. Les considérations de sécurité pour ces deux environnements sont généralement différentes.

### Machines utilisateur gérées

Les machines utilisateur gérées font l'objet d'un contrôle administratif ; elles sont soit sous votre propre contrôle, soit sous celui d'une autre organisation à laquelle vous faites confiance. Vous pouvez configurer et fournir directement aux utilisateurs les machines utilisateur ; vous pouvez également fournir des terminaux sur lesquels un seul bureau s'exécute en mode plein écran seulement. Suivez les bonnes pratiques générales en matière de sécurité décrites ci-dessous pour toutes les machines utilisateur gérées. Cette version présente l'avantage de n'exiger qu'un minimum de logiciels sur une machine utilisateur.

Une machine utilisateur gérée peut être configurée pour être utilisée en mode plein écran seulement ou en mode fenêtre.

- Mode plein écran uniquement : les utilisateurs ouvrent une session sur celle-ci à partir de l'écran d'ouverture de session Windows habituel. Les mêmes informations d'identification de l'utilisateur sont alors utilisées pour ouvrir automatiquement une session sur cette version.
- Les utilisateurs voient leur bureau dans une fenêtre : les utilisateurs doivent d'abord ouvrir une session sur la machine utilisateur, puis sur cette version via le site Web fourni avec le produit.

### Machines utilisateur non gérées

Les machines utilisateur qui ne sont pas gérées et administrées par une organisation de confiance ne peuvent pas être considérées comme des machines sous contrôle administratif. Vous pouvez, par exemple, autoriser les utilisateurs à se procurer et à configurer leurs propres machines, mais ceux-ci peuvent ne pas respecter les bonnes pratiques générales en matière de sécurité décrites ci-dessus. Cette version présente l'avantage de mettre, en toute sécurité, des bureaux à la disposition des machines utilisateur non gérées. Ces machines doivent tout de même disposer d'une protection antivirus de base capable d'arrêter les enregistreurs de frappes et les attaques similaires axées sur la saisie.

### Considérations sur le stockage de données

Lorsque vous utilisez cette version, vous pouvez empêcher les utilisateurs de stocker des données sur les machines utilisateur qui sont sous leur contrôle physique. Toutefois, vous devez encore envisager les conséquences de l'enregistrement, par les utilisateurs, de données sur leurs bureaux. Enregistrer des données sur les bureaux n'est pas une bonne pratique ; celles-ci doivent être stockées sur des serveurs de fichiers, des serveurs de bases de données ou d'autres référentiels où elles feront l'objet d'une protection appropriée.

Votre environnement peut être composé de différents types de bureaux, tels que des bureaux regroupés ou dédiés. Les utilisateurs ne doivent jamais stocker de données sur des bureaux partagés, tels que les bureaux regroupés. S'ils stockent des données sur des bureaux dédiés, celles-ci doivent être supprimées si les bureaux sont ensuite mis à la disposition d'autres utilisateurs.

### Environnements à versions mixtes

Les environnements à versions mixtes sont inévitables lors de certaines mises à niveau. Suivez les recommandations et réduisez la durée pendant laquelle les composants Citrix de versions différentes co-existent. Dans les environnements à versions mixtes, la stratégie de sécurité, par exemple, peut ne pas être appliquée de façon uniforme.

> **Remarque :**
>
> Ce comportement est caractéristique d'autres produits logiciels ; l'utilisation d'une version antérieure d'Active Directory n'applique que partiellement la stratégie de groupe avec les versions ultérieures de Windows.

Le scénario suivant décrit un problème de sécurité qui peut se produire dans un environnement Citrix à versions mixtes spécifique. Lorsque Citrix Receiver 1.7 est utilisé pour se connecter à un bureau virtuel exécutant le VDA dans XenApp et XenDesktop 7.6 Feature Pack 2, le paramètre de stratégie **Autoriser le transfert de fichiers entre les bureaux et le client** est activée dans le site, mais ne peut

pas être désactivée par un Delivery Controller exécutant XenApp et XenDesktop 7.1. Il ne reconnaît pas le paramètre de stratégie, qui est disponible dans la version ultérieure du produit. Ce paramètre de stratégie permet aux utilisateurs de télécharger des fichiers sur leur bureau virtuel, ce qui cause le problème de sécurité. Pour contourner ce problème, mettez à niveau le Delivery Controller ou une instance autonome de Studio vers la version 7.6 Feature Pack 2, puis utilisez la stratégie de groupe pour désactiver le paramètre de stratégie. Vous pouvez également utiliser la stratégie locale sur tous les bureaux virtuels concernés.

## Considérations de sécurité Remote PC Access

Remote PC Access implémente les fonctionnalités de sécurité suivantes :

- La carte à puce est prise en charge.
- Lorsqu'une session à distance se connecte, le moniteur du PC de bureau affiche un écran noir.
- Remote PC Access redirige toutes les entrées de claviers et de souris vers la session à distance, sauf la combinaison CTRL+ALT+SUPPR et les cartes à puce et les périphériques biométriques USB.
- SmoothRoaming est prise en charge uniquement pour un seul utilisateur.
- Lorsqu'un utilisateur a ouvert une session distante connectée à un PC de bureau, seul cet utilisateur peut reprendre l'accès local sur le PC de bureau. Pour reprendre l'accès local, l'utilisateur appuie sur Ctrl+Alt+Suppr sur le PC local et ouvre une session avec les mêmes informations d'identification utilisées par la session à distance. L'utilisateur peut également reprendre l'accès local en insérant une carte à puce ou en tirant parti de la biométrie, si votre système possède une intégration fournisseur des informations d'identification tierces appropriées. Ce comportement par défaut peut être substitué par l'activation de changement rapide d'utilisateur via des objets de stratégie de groupe (GPO) ou en modifiant le registre.

> **Remarque :**
>
> Citrix recommande de ne pas attribuer de privilèges d'administrateur VDA aux utilisateurs de sessions.

### Assignations automatiques

Par défaut, Remote PC Access prend en charge l'assignation automatique de plusieurs utilisateurs à un VDA. Dans XenDesktop 5.6 Feature Pack 1, les administrateurs peuvent modifier ce comportement en utilisant le script PowerShell RemotePCAccess.ps1. Cette version utilise une entrée du Registre pour autoriser ou interdire plusieurs attributions de PC distants automatiques, ce paramètre s'applique à l'intégralité du site.

> **Attention :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Pour restreindre les attributions automatiques pour un utilisateur unique :

Sur chaque Controller du site, définissez la clé de registre suivante :

```
HKEY\_LOCAL\_MACHINE\Software\Citrix|DesktopServer
Name: AllowMultipleRemotePCAssignments
Type: REG_DWORD
Data: 0 = Disable multiple user assignment, 1 = (Default) Enable
   multiple user assignment.
```

S'il existe une ou plusieurs attributions d'utilisateur, supprimez-les à l'aide des commandes du kit de développement afin que le VDA puisse ensuite être admissible pour une seule attribution automatique.

- Supprimez tous les utilisateurs affectés à partir du VDA : `$machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine`
- Supprimez le VDA du groupe de distribution : `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

Redémarrez le PC de bureau physique.

### Approbation XML

Le paramètre d'approbation XML s'applique aux déploiements qui utilisent :

- un magasin StoreFront local ;
- une technologie d'authentification d'abonné (utilisateur) qui ne nécessite pas de mots de passe. Ces technologies sont par exemple des solutions de transfert de domaine, de cartes à puce, de SAML et de Veridium.

L'activation du paramètre d'approbation XML permet aux utilisateurs de s'authentifier avec succès, puis de démarrer les applications. Le Delivery Controller approuve les informations d'identification envoyées par StoreFront. Activez ce paramètre uniquement lorsque vous avez sécurisé les communications entre votre Delivery Controller et StoreFront (à l'aide de pare-feu, d'IPsec ou d'autres recommandations de sécurité).

Cette option est désactivée par défaut.

Utilisez le kit SDK Citrix Virtual Apps and Desktops PowerShell pour vérifier, activer ou désactiver le paramètre d'approbation XML.

- Pour vérifier la valeur actuelle du paramètre d'approbation XML, exécutez `Get-BrokerSite` et inspectez la valeur de `TrustRequestsSentToTheXMLServicePort`.
- Pour activer l'approbation XML, exécutez `Set-BrokerSite -TrustRequestsSentToTheXmlServi $true`.
- Pour désactiver l'approbation XML, exécutez `Set-BrokerSite -TrustRequestsSentToTheXmlSe $false`.

## Cartes à puce

June 27, 2024

Les cartes à puce et les technologies équivalentes sont prises en charge selon les indications décrites dans cet article. Pour utiliser des cartes à puce avec Citrix Virtual Apps ou Citrix Virtual Desktops :

- Il est important de bien comprendre la stratégie de sécurité de votre organisation concernant l'utilisation des cartes à puce. Ces stratégies peuvent, par exemple, déterminer comment les cartes à puce sont délivrées et comment les utilisateurs doivent les protéger. Il peut être nécessaire de réévaluer certains aspects de ces stratégies dans un environnement Citrix Virtual Apps ou Citrix Virtual Desktops.
- Déterminez les types de machine utilisateur, les systèmes d'exploitation et les applications publiées qui doivent être utilisés avec des cartes à puce.
- Familiarisez-vous avec la technologie de carte à puce ainsi que le matériel et les logiciels de votre fournisseur de carte à puce.
- Déterminez comment déployer des certificats numériques dans un environnement distribué.

> **Remarque :**
>
> L'inscription par carte à puce n'est pas prise en charge avec la carte à puce rapide. L'inscription par carte à puce peut fonctionner lorsque la carte à puce rapide est désactivée, mais dépend du type de carte à puce et de middleware. Contactez votre fournisseur de cartes à puce et de middleware pour obtenir des informations sur leur intégration avec Citrix Virtual Apps and Desktops et la prise en charge de l'inscription par carte à puce sur des sessions virtuelles.

### Types de cartes à puce

Les cartes à puce d'entreprise et de consommateur ont les mêmes dimensions et connecteurs électriques et utilisent les mêmes lecteurs de carte à puce.

Les cartes à puce d'entreprise contiennent des certificats numériques. Ces cartes à puce prennent en charge l'ouverture de session Windows et peuvent également être utilisées avec des applications pour la signature numérique et le cryptage de documents et d'e-mails. Citrix Virtual Apps and Desktops prend en charge les utilisations suivantes :

Les cartes à puce de consommateur ne contiennent pas de certificats numériques ; elles contiennent un secret partagé. Ces cartes à puce peuvent prendre en charge les paiements (par carte de crédit avec puce et signature ou avec puce et code PIN). Elles ne prennent pas en charge l'ouverture de session Windows ou les applications Windows standard. Des applications Windows spécialisées et une infrastructure logicielle adaptée (notamment, par exemple, une connexion à un réseau de carte de paiement) sont requises pour utiliser ces cartes à puce. Contactez votre conseiller Citrix pour de plus amples informations sur la prise en charge de ces applications spécialisées sur Citrix Virtual Apps or Citrix Virtual Desktops.

Pour les cartes à puce d'entreprise, il existe des équivalents compatibles qui peuvent être utilisés de manière similaire.

- Un jeton USB équivalent à une carte à puce se connecte directement à un port USB. Ces jetons USB sont généralement de la taille d'un lecteur flash USB, mais peuvent être aussi petits qu'une carte SIM utilisée dans un téléphone mobile. Ils se présentent comme une combinaison d'une carte à puce et d'un lecteur de carte à puce USB.
- Une carte à puce virtuelle utilisant un module de plateforme sécurisée Windows (TPM) s'affiche en tant que carte à puce. Ces cartes à puce virtuelles sont prises en charge pour Windows 8 et Windows 10, à l'aide de l'application Citrix Workspace (Citrix Receiver 4.3 au minimum).
  - Les versions de Citrix Virtual Apps and Desktops (anciennement XenApp et XenDesktop) antérieures à XenApp et XenDesktop 7.6 FP3 ne prennent pas en charge les cartes à puce virtuelles.
  - Pour de plus amples informations sur les cartes à puce virtuelles, consultez la section Présentation des cartes à puce virtuelles.

  **Remarque :** le terme « carte à puce virtuelle » est également utilisé pour décrire un certificat numérique stocké sur l'ordinateur de l'utilisateur. Ces certificats numériques ne sont pas réellement similaires aux cartes à puce.

La prise en charge des cartes à puce de Citrix Virtual Apps and Desktops repose sur les spécifications standard PC/SC (Personal Computer/Smart Card) de Microsoft. La configuration minimale requise exige que les cartes à puce et les lecteurs de carte à puce soient pris en charge par le système d'exploitation Windows sous-jacent et soient certifiés WHQL (laboratoires Microsoft de contrôle qualité du matériel conçu pour Windows). Consultez la documentation Microsoft pour obtenir des informations supplémentaires sur le matériel PC/SC conformité. D'autres types de machines utilisateur peuvent respecter les normes PS/SC. Pour plus d'informations, reportez-vous au programme Citrix Ready.

En règle générale, un pilote de périphérique séparé est nécessaire pour la carte à puce ou équivalent de chaque fournisseur. Cependant, si des cartes à puce sont conformes à une norme telle que la norme NIST Personal Identity Verification (PIV), il est possible d'utiliser un seul pilote de périphérique pour une gamme de cartes à puce. Le pilote de périphérique doit être installé sur la machine utilisateur et le Virtual Delivery Agent (VDA). Le pilote de périphérique est souvent fourni dans le cadre du package de middleware de la carte à puce, disponible auprès d'un partenaire Citrix ; le package de middleware de carte à puce propose des fonctionnalités avancées. Le pilote de périphérique peut également être décrit comme fournisseur de service cryptographique (CSP), fournisseur de stockage de clés (KSP) ou minipilote.

Les combinaisons carte à puce et logiciel intermédiaire pour systèmes Windows suivantes ont été testées par Citrix comme exemples représentatifs de leur type. Cependant, d'autres cartes à puce et middleware peuvent également être utilisés. Pour de plus amples informations sur les cartes à puce et middleware compatibles avec Citrix, consultez http://www.citrix.com/ready.

| Logiciels intermédiaires | Correspondance des cartes |
|---|---|
| Gemalto Mini Driver pour carte .NET | Gemalto .NET v2+ |

Pour de plus amples informations sur l'utilisation de cartes à puce avec d'autres types de périphériques, consultez la documentation relative à l'application Citrix Workspace pour ce périphérique.

### Remote PC Access

Les cartes à puce sont uniquement prises en charge pour l'accès à distance vers les postes de travail physiques exécutant Windows 10, Windows 8 ou Windows 7.

Les cartes à puce suivantes ont été testées avec Remote PC Access :

| Logiciels intermédiaires | Correspondance des cartes |
|---|---|
| Minipilote Gemalto .NET | Gemalto .NET v2+ |

### Carte à puce rapide

La carte à puce rapide constitue une amélioration par rapport à la redirection de carte à puce PC/SC HDX existante. Elle améliore les performances lorsque les cartes à puce sont utilisées dans des situations WAN à latence élevée. Lorsque la latence est élevée, l'amélioration des performances peut être

significative (par exemple, 15 secondes pour une connexion rapide par carte à puce Windows contre plus d'une minute avec la redirection de carte à puce basée sur PC/SC).

La carte à puce rapide est activée par défaut sur les machines hôtes avec des VDA Windows actuellement pris en charge. Pour désactiver la carte à puce rapide côté hôte, par exemple à des fins de diagnostic, définissez le paramètre de registre correspondant à la 'désactivation de la redirection cryptographique'sur n'importe quelle valeur non nulle :

```
HKLM\SOFTWARE\Citrix\SmartCard
CryptographicRedirectionDisable (DWORD)
<!--NeedCopy-->
```

Côté client, pour activer la carte à puce rapide, incluez le paramètre ICA SmartCardCryptographicRedirection dans le fichier *default.ica* du site StoreFront associé :

```
[WFClient]
SmartCardCryptographicRedirection=On
```

En outre, côté client, la carte à puce rapide peut être activée ou désactivée de force (par exemple, à des fins de diagnostic) avec les paramètres de registre suivants :

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (en tant que DWORD différent de zéro)

Ou

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (en tant que DWORD différent de zéro)

La ruche de Registre 32 bits doit être spécifiée (à l'aide de `WOW6432Node`) si la machine cliente est 64 bits.

Limitations :

- Seule l'application Citrix Workspace pour Windows prend en charge les cartes à puce rapides. Si vous configurez des cartes à puce rapides dans le fichier default.ica, les applications Citrix Workspace non dédiées à Windows fonctionnent toujours avec la redirection PC/SC existante.
- Les seuls scénarios à double saut (double-hop) qui prennent en charge les cartes à puce rapides sont ICA > ICA avec une carte à puce rapide activée sur les deux sauts. Étant donné que la carte à puce rapide ne prend pas en charge les scénarios ICA > RDP à double saut, ces scénarios ne fonctionnent pas.
- La carte à puce rapide ne prend pas en charge Cryptography Next Generation. Une carte à puce rapide ne prend donc pas en charge les cartes à puce Elliptic Curve Cryptography (ECC).
- La carte à puce rapide ne prend en charge que les opérations sur les conteneurs de clés en lecture seule.
- La carte à puce rapide ne prend pas en charge la modification du code PIN de la carte à puce.

À partir de la version 2203 du VDA et de la version 2202 de l'application Citrix Workspace pour Windows (ou version ultérieure), la carte à puce rapide est compatible avec Cryptography Next Generation (CNG). En outre, les cartes à puce ECC (Elliptic Curve Cryptography) sont prises en charge avec les courbes suivantes : P-256, P-384, P-521 bits, pour ECDSA et ECDH.

À partir de la version 2203 du VDA, la carte à puce rapide permet de mettre en cache le code PIN de la carte à puce entre les applications à partir de la session d'ouverture de session du même utilisateur. Par exemple, si la **mise en cache du code PIN de session** est activée et que l'utilisateur a précédemment fourni le code PIN de sa carte à puce à Outlook, lorsque Word est ensuite utilisé pour signer un document, Word utilise le code PIN de carte à puce déjà mis en cache (envoyé à Outlook). La **mise en cache du code PIN de session** améliore l'expérience utilisateur en réduisant le nombre de fois où l'utilisateur doit entrer le code PIN de sa carte à puce. En outre, si la carte à puce est utilisée pour se connecter au VDA, le code PIN d'ouverture de session de la carte à puce Windows peut éventuellement être enregistré dans la **mise en cache du code PIN de session**. Cela peut encore améliorer l'expérience utilisateur.

**La mise en cache du code PIN de session** est désactivée par défaut. Elle peut être activée et contrôlée à l'aide des paramètres de registre suivants sur le VDA :

Dans HKLM\SOFTWARE\Citrix\SmartCard :

- `EnablePinSessionCache` en tant que DWORD (non nul pour activer)
- `EnableLogonPinSessionCache` en tant que DWORD (non nul pour activer)
- `PinSessionCacheEntryStaleTimeout` en tant que DWORD (nombre de secondes avant qu'une entrée ne devienne obsolète, la valeur par défaut est 1 heure)

### Types de lecteurs de carte à puce

Un lecteur de carte à puce peut être intégré à la machine utilisateur, ou être connecté séparément à la machine utilisateur (généralement via USB ou Bluetooth). Les lecteurs de carte avec contact qui sont conformes à la spécification USB CCID sont pris en charge. Ils contiennent une fente dans laquelle l'utilisateur insère la carte à puce. La norme Deutsche Kreditwirtschaft (DK) définit quatre catégories de lecteurs de carte de contact.

- Les lecteurs de carte à puce de classe 1 sont les plus courants et sont généralement dotés d'une seule fente. Les lecteurs de carte à puce de classe 1 sont pris en charge, généralement avec un pilote de périphérique CCID standard fourni avec le système d'exploitation.
- Les lecteurs de carte à puce de classe 2 présentent également un pavé numérique sécurisé qui n'est pas accessible par la machine utilisateur. Les lecteurs de carte à puce de classe 2 peuvent être intégrés à un clavier avec un pavé numérique sécurisé. Pour les lecteurs de carte à puce de classe 2, contactez votre conseiller Citrix ; un pilote de périphérique spécifique au lecteur peut être nécessaire pour activer la fonctionnalité de pavé numérique sécurisé.

- Les lecteurs de carte à puce de classe 3 contiennent également un écran sécurisé. Les lecteurs de carte à puce de classe 3 ne sont pas pris en charge.
- Les lecteurs de carte à puce de classe 4 contiennent également un module de transaction sécurisé. Les lecteurs de carte à puce de classe 4 ne sont pas pris en charge.

> **Remarque :**
>
> La classe du lecteur de carte à puce n'est pas liée à la classe du périphérique USB.

Les lecteurs de carte à puce doivent être installés avec un pilote de périphérique correspondant sur la machine utilisateur.

Pour plus d'informations sur les lecteurs de carte pris en charge, consultez la documentation correspondant à l'application Citrix Workspace que vous utilisez. Dans la documentation de l'application Citrix Workspace, les versions prises en charge sont répertoriées dans une section sur les cartes à puce où dans la section sur la configuration système requise.

### Expérience utilisateur

La prise en charge des cartes à puce est intégrée dans Citrix Virtual Apps and Desktops à l'aide d'un canal virtuel de carte à puce ICA/HDX spécifique qui est activé par défaut.

Important : n'utilisez pas la redirection USB générique pour les lecteurs de carte à puce. Cette option est désactivée par défaut pour les lecteurs de carte à puce et n'est pas prise en charge si elle est activée.

Il est possible d'utiliser plusieurs cartes à puce et plusieurs lecteurs sur la même machine utilisateur, mais si l'authentification unique est en service, une seule carte à puce doit être insérée lorsque l'utilisateur démarre une application ou un bureau virtuel. En cas d'utilisation d'une carte à puce dans une application (par exemple pour les fonctions de signature numérique ou de cryptage), d'autres messages invitant à insérer la carte à puce ou à saisir un code PIN peuvent s'afficher. Cela peut se produire si plusieurs cartes à puce sont insérées en même temps.

- Si les utilisateurs sont invités à insérer une carte à puce alors que celle-ci se trouve déjà dans le lecteur, ils doivent sélectionner Annuler.
- Si les utilisateurs sont invités à entrer le code PIN, ils doivent le saisir à nouveau.

Vous pouvez réinitialiser les codes confidentiels à l'aide d'un système de gestion de carte ou d'un outil du fournisseur.

> **Important :**
>
> Dans une session Citrix Virtual Apps ou Citrix Virtual Desktops. l'utilisation d'une carte à puce

> avec l'application Connexion Bureau à distance Microsoft n'est pas prise en charge. Ceci est parfois décrit comme un scénario « double-hop ».

### Avant de déployer les cartes à puce

- Vous devez vous procurer un pilote de périphérique pour le lecteur de carte à puce et l'installer sur la machine utilisateur. De nombreux lecteurs de carte à puce peuvent utiliser le pilote de périphérique CCID fourni par Microsoft.
- Vous devez vous procurer un pilote de périphérique et un logiciel de fournisseur de services de chiffrement (CSP) depuis votre fournisseur de carte à puce et les installer sur les machines utilisateur et les bureaux virtuels. Le pilote et le logiciel CSP doivent être compatibles avec Citrix Virtual Apps and Desktops. Consultez la documentation du fournisseur pour connaître leur compatibilité. Pour les bureaux virtuels utilisant des cartes à puce qui prennent en charge et utilisent le modèle minipilote, les minipilotes de carte à puce se téléchargent automatiquement, mais vous pouvez également les obtenir à partir de http://catalog.update.microsoft.com ou auprès votre fournisseur. En outre, si des middlewares PKCS #11 sont requis, obtenez-les auprès de votre fournisseur de carte.
- Important : Citrix recommande d'installer et de tester les pilotes et le logiciel CSP sur un ordinateur physique avant d'installer le logiciel Citrix.
- Ajoutez l'adresse URL de Citrix Receiver pour Web à la liste Sites de confiance pour les utilisateurs qui utilisent des cartes à puce dans Internet Explorer avec Windows 10. Dans Windows 10, Internet Explorer n'est pas exécuté par défaut en mode protégé pour les sites de confiance.
- Assurez-vous que votre infrastructure de clé publique (PKI) est configurée correctement. Cela assure que le mappage de certificat vers le compte est correctement configuré pour l'environnement Active Directory et que la validation du certificat utilisateur peut être effectuée avec succès.
- Assurez-vous que votre déploiement répond à la configuration système requise des autres composants Citrix utilisé avec des cartes à puce, y compris application Citrix Workspace et StoreFront.
- Vérifiez l'accès aux serveurs suivants de votre site :
  - Le contrôleur de domaine Active Directory pour le compte d'utilisateur associé à un certificat d'ouverture de session sur la carte à puce
  - Delivery Controller
  - Citrix StoreFront
  - Citrix Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Facultatif pour Remote PC Access) : Microsoft Exchange Server

### Activer l'authentification par carte à puce

**Étape 1.** Problème de cartes à puce pour les utilisateurs en fonction de votre stratégie d'émission de carte.

**Étape 2.** (Facultatif) Définissez des cartes à puce pour activer les utilisateurs pour Remote PC Access.

**Étape 3.** Installez et configurez le Delivery Controller et StoreFront (s'ils ne sont pas déjà installés pour l'utilisation des cartes à puce à distance).

**Étape 4.** Activez StoreFront pour l'utilisation des cartes à puce. Pour de plus amples informations, consultez la section Configurer l'authentification par carte à puce dans la documentation de StoreFront.

**Étape 5.** Activez Citrix Gateway/Access Gateway pour utiliser la carte à puce. Pour de plus amples informations, consultez la section Configuration de l'authentification et de l'autorisation et Configuration de l'accès par carte à puce avec l'Interface Web dans la documentation NetScaler.

**Étape 6.** Activez des VDA pour l'utilisation des cartes à puce.

- Assurez-vous que le VDA possède les applications et les mises à jour requises.
- Installez les logiciels intermédiaires.
- Définissez l'utilisation d'une carte à puce à distance, l'activation de la communication des données de carte à puce entre l'application Citrix Workspace sur une machine utilisateur et une session de bureau virtuel.

**Étape 7.** Activez les machines utilisateur (y compris les machines appartenant à un domaine ou non) pour utiliser la carte à puce. Consultez la section Configurer l'authentification par carte à puce dans la documentation de StoreFront pour plus de détails.

- Importez le certificat racine de l'autorité de certification et le certificat émis par l'autorité de certificat dans le magasin de clés de la machine.
- Installez le middleware de carte à puce de votre fournisseur.
- Installez et configurez application Citrix Workspace pour Windows, en vous assurant d'importer le fichier icaclient.adm à l'aide de la console de gestion des stratégies de groupe et d'activer l'authentification par carte à puce.

**Étape 8.** Testez le déploiement. Assurez-vous que votre déploiement est correctement configuré en démarrant un bureau virtuel avec une carte à puce d'utilisateur test. Testez tous les mécanismes d'accès possibles (par exemple, accès au bureau via Internet Explorer et l'application Citrix Workspace).

### Suivre le nombre d'insertion du lecteur de carte à puce

Avec l'accès distant par carte à puce et la fonction SCardGetStatusChange, vous pouvez suivre le nombre de fois qu'une carte à puce a été insérée ou retirée d'un lecteur. La fonction met à jour un tableau de structures de données SCARD_READERSTATE (un tableau par lecteur que vous surveillez). Le mot élevé (16 bits) du champ dwEventState de chaque tableau SCARD_READERSTATE contient le nombre de lecteurs. Pour de plus amples informations, consultez les articles Microsoft SCardGetStatusChangeA function et SCARD_READERSTATEA structure.

Par défaut, le paramètre de suivi du nombre d'insertions du lecteur de carte à puce (**Reader Insert Count Reporting**) est désactivé. Pour activer le paramètre de suivi, ajoutez la clé de registre suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

Nom : EnableReaderInsertCountReporting

Type : DWORD

Valeur : toute valeur autre que zéro

Lorsque la session se déconnecte, le nombre se réinitialise à zéro.

Le paramètre de suivi du nombre d'insertions du lecteur de carte à puce (**Reader Insert Count Reporting**) est compatible avec les logiciels intermédiaires de carte à puce tiers.

## Déploiements de carte à puce

June 27, 2024

Les types de déploiements de carte à puce suivants sont pris en charge par cette version du produit et par les environnements mixtes contenant cette version. D'autres configurations peuvent fonctionner mais ne sont pas prises en charge.

| Type | Connectivité StoreFront |
|---|---|
| Ordinateurs appartenant à un domaine local | Directement connectés |
| Accès à distance à partir d'ordinateurs appartenant à un domaine | Connecté via Citrix Gateway |
| Ordinateurs n'appartenant pas à un domaine | Directement connectés |
| Accès à distance depuis des ordinateurs n'appartenant pas à un domaine | Connecté via Citrix Gateway |

| Type | Connectivité StoreFront |
| --- | --- |
| Ordinateurs n'appartenant pas à un domaine et clients légers accédant au site Desktop Appliance | Connectés au travers des sites Desktop Appliance |
| Ordinateurs appartenant à un domaine et clients légers accédant à StoreFront au travers de l'adresse URL XenApp Services | Connectés via les adresses URL XenApp Services |

Les types de déploiement sont définis par les caractéristiques de la machine utilisateur sur laquelle le lecteur de carte à puce est connecté :

- Indique si la machine appartient à un domaine ou n'appartient pas à un domaine.
- Comment le périphérique est-il connecté à StoreFront.
- Quel logiciel est utilisé pour afficher les applications et les bureaux virtuels.

En outre, les applications compatibles avec les cartes à puce, telles que Microsoft Word et Microsoft Excel, peuvent être utilisées dans ces déploiements. Ces applications permettent aux utilisateurs de signer numériquement ou de crypter des documents.

### Authentification bimodale

Lorsque cela est possible dans chacun de ces déploiements, Receiver prend en charge l'authentification bimodale en offrant à l'utilisateur le choix d'utilisation d'une carte à puce ou de saisie de leur nom d'utilisateur et mot de passe. Ceci est utile si la carte à puce ne peut pas être utilisé (par exemple, si l'utilisateur l'a laissé chez lui, ou que le certificat d'ouverture de session a expiré).

Étant donné que les utilisateurs de machines n'appartenant pas à un domaine ouvrent une session sur Receiver pour Windows directement, vous pouvez autoriser les utilisateurs à revenir à l'authentification explicite. Si vous configurez l'authentification bimodale, les utilisateurs sont initialement invités à ouvrir une session à l'aide de leurs cartes à puce et codes PIN mais ont la possibilité de sélectionner l'authentification explicite s'ils rencontrent des problèmes avec leurs cartes à puce.

Si vous déployez Citrix Gateway, les utilisateurs ouvrent une session sur leurs machines et sont invités par Receiver pour Windows à s'authentifier auprès de Citrix Gateway. Cela s'applique aussi bien aux machines appartenant à un domaine qu'à celles n'appartenant pas à un domaine. Les utilisateurs peuvent ouvrir une session sur Citrix Gateway à l'aide de leurs cartes à puce et codes PIN, ou avec des informations d'identification explicites. Cela vous permet de fournir aux utilisateurs une authentification bimodale pour l'ouverture de session Citrix Gateway. Configurez l'authentification pass-through via Citrix Gateway à StoreFront et déléguez la validation des informations d'identification à Citrix Gateway pour les utilisateurs de cartes à puce de façon à ce que les utilisateurs soient authentifiés auprès de StoreFront de manière silencieuse.

### Considérations relatives à la forêt Active Directory

Dans un environnement Citrix, les cartes à puce sont prises en charge dans une forêt unique. Les ouvertures de session par carte à puce entre les forêts nécessitent une approbation de forêt bidirectionnelle pour tous les comptes d'utilisateur. Les déploiements plus complexes de forêts multiples impliquant des cartes à puce (c'est-à-dire, où les approbations sont uniquement à sens unique ou de types différents) ne sont pas pris en charge.

Vous pouvez utiliser des cartes à puce dans un environnement Citrix qui comprend des bureaux distants. Cette fonctionnalité peut être installée localement (sur la machine utilisateur à laquelle la carte à puce est connectée) ou à distance (sur le bureau distant à laquelle la machine utilisateur se connecte).

### Stratégie de retrait de carte à puce

La stratégie définie pour le retrait de la carte à puce sur le produit détermine ce qui se passe lorsque vous retirez la carte à puce du lecteur au cours d'une session. Cette stratégie est configurée et gérée par le système d'exploitation Windows.

| Paramètre de stratégie | Comportement du Bureau |
|---|---|
| Aucune action | Aucune action. |
| Verrouiller la station de travail | La session de bureau est déconnectée et le bureau virtuel est verrouillé. |
| Forcer la fermeture de session | L'utilisateur est obligé de fermer la session. Si la connexion réseau est interrompue et que ce paramètre est activé, la session peut être fermée et l'utilisateur peut perdre des données. |
| Déconnecter en cas de session Terminal Server | La session est déconnectée et le bureau virtuel est verrouillé. |

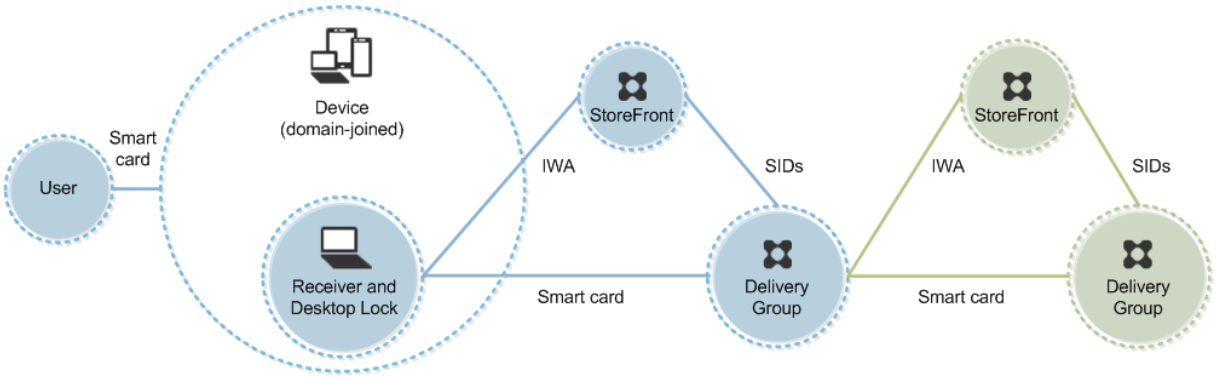
### Vérification de la révocation des certificats

Si la vérification de la révocation des certificats est activée et qu'un utilisateur insère une carte à puce avec un certificat non valide dans un lecteur de carte, l'utilisateur ne peut pas authentifier ou accéder au bureau ou à l'application associée à ce certificat. Par exemple, si le certificat non valide est utilisé pour le déchiffrement de messagerie, l'e-mail reste crypté. Si d'autres certificats sur la carte, tels que ceux utilisées pour l'authentification, sont toujours valides, ces fonctions restent actives.

### Exemple de déploiement : ordinateurs appartenant à un domaine

Ce déploiement implique des machines utilisateur appartenant à un domaine qui exécutent Desktop Viewer et se connectent directement à StoreFront.

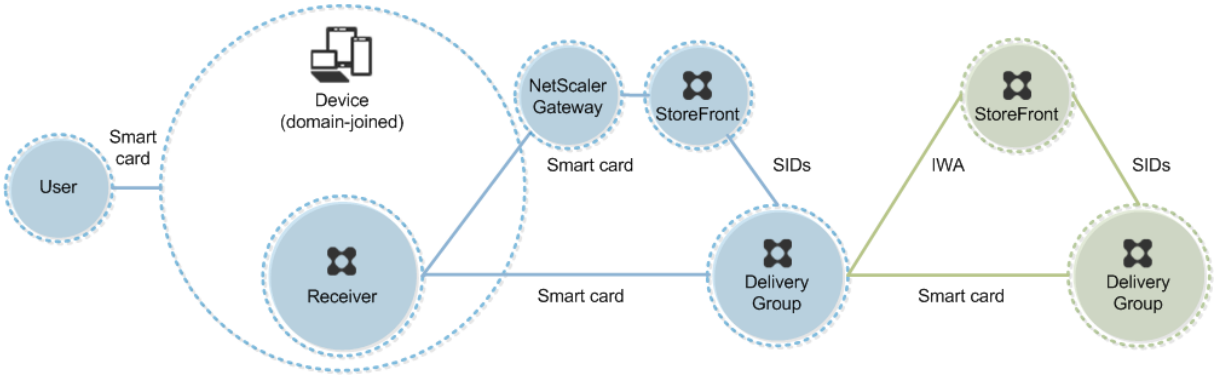



Un utilisateur ouvre une session sur une machine à l'aide d'une carte à puce et du code confidentiel. Receiver authentifie l'utilisateur à un serveur StoreFront à l'aide de l'authentification Windows intégrée (IWA). StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à Citrix Virtual Apps ou Citrix Virtual Desktops. Lorsque l'utilisateur démarre un bureau virtuel ou une application, l'utilisateur n'est pas invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique est configurée sur Receiver.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

### Exemple de déploiement : accès à distance à partir d'ordinateurs appartenant à un domaine

Ce déploiement implique des machines utilisateur appartenant à un domaine qui exécutent Desktop Viewer et se connectent à StoreFront via Citrix Gateway/Access Gateway.



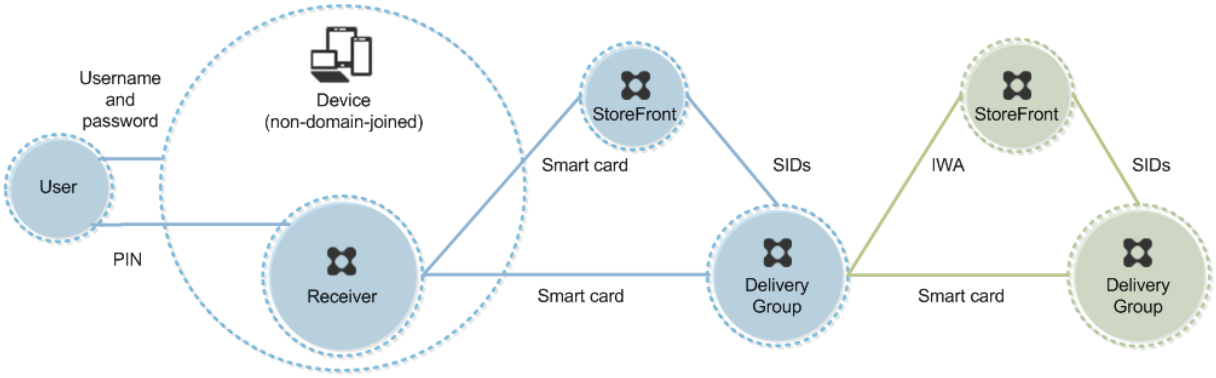
Un utilisateur ouvre une session sur une machine à l'aide d'une carte à puce et d'un code confidentiel, puis ouvre une session sur Citrix Gateway/Access Gateway. Cette seconde ouverture de session peut être effectuée avec la carte à puce et un code confidentiel ou un nom d'utilisateur et un mot de passe car Receiver permet l'authentification bimodale dans ce déploiement.

L'utilisateur ouvre automatiquement une session sur StoreFront, qui transmet les identificateurs de sécurité (SID) de l'utilisateur à Citrix Virtual Apps ou Citrix Virtual Desktops.. Lorsque l'utilisateur démarre un bureau ou une application virtuel(le), l'utilisateur n'est pas invité à entrer à nouveau un code confidentiel, car la fonctionnalité d'authentification unique est configurée sur Receiver.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

### Exemple de déploiement : ordinateurs n'appartenant pas à un domaine

Ce déploiement implique des machines utilisateur n'appartenant pas au domaine qui exécutent Desktop Viewer et se connectent directement à StoreFront.




Un utilisateur ouvre une session sur une machine. En général, l'utilisateur entre un nom d'utilisateur et un mot de passe, mais puisque la machine n'appartient pas à un domaine, les informations d'identification de cette ouverture de session sont facultatives. Comme l'authentification bimodale est possible dans ce déploiement, Receiver invite l'utilisateur à entrer une carte à puce et un code confidentiel ou un nom d'utilisateur et un mot de passe. Receiver s'authentifie ensuite auprès de StoreFront.

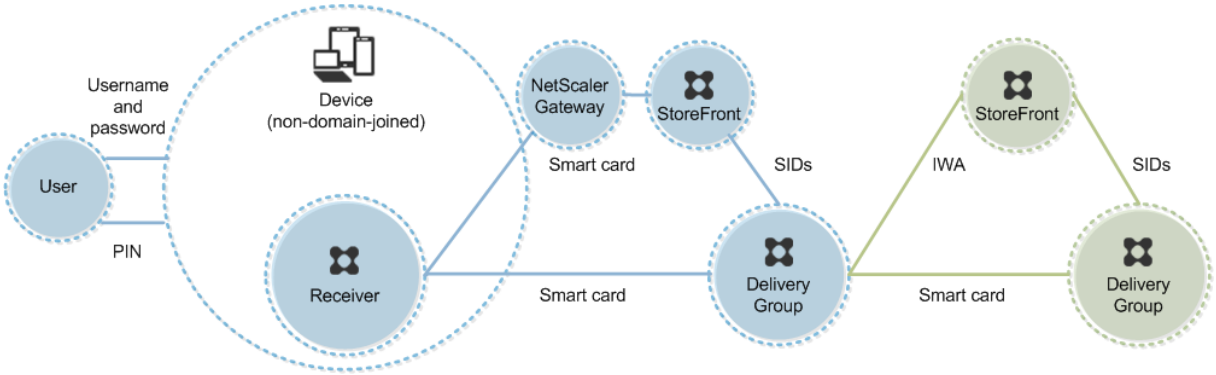
StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à Citrix Virtual Apps ou Citrix Virtual Desktops. Lorsque l'utilisateur démarre un bureau virtuel ou une application, l'utilisateur est invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique n'est pas disponible dans ce déploiement.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

### Exemple de déploiement : accès à distance à partir d'ordinateurs n'appartenant pas à un domaine

Ce déploiement implique des machines utilisateur n'appartenant pas au domaine qui exécutent Desktop Viewer et se connectent directement à StoreFront.




Un utilisateur ouvre une session sur une machine. En général, l'utilisateur entre un nom d'utilisateur et un mot de passe, mais puisque la machine n'appartient pas à un domaine, les informations d'identification de cette ouverture de session sont facultatives. Comme l'authentification bimodale est possible dans ce déploiement, Receiver invite l'utilisateur à entrer une carte à puce et un code confidentiel ou un nom d'utilisateur et un mot de passe. Receiver s'authentifie ensuite auprès de StoreFront.

StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à Citrix Virtual Apps ou Citrix Virtual Desktops. Lorsque l'utilisateur démarre un bureau virtuel ou une application, l'utilisateur est invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique n'est pas disponible dans ce déploiement.

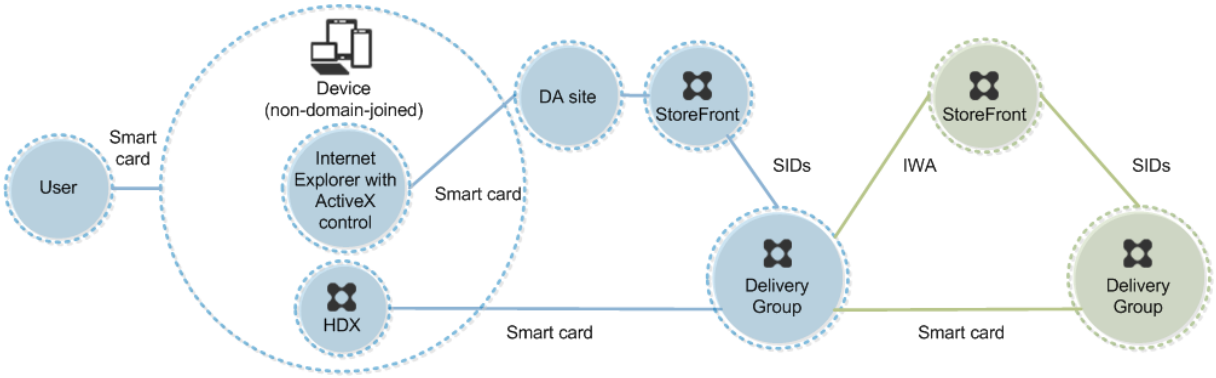
Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

### Exemple de déploiement : ordinateurs n'appartenant pas à un domaine et clients légers accédant au site Desktop Appliance

Ce déploiement implique des machines utilisateur n'appartenant pas au domaine pouvant exécuter Desktop Lock et se connecter à StoreFront via des sites Desktop Appliance.

Desktop Lock est un composant distinct fourni avec Citrix Virtual Apps, Citrix Virtual Desktops et VDI-in-a-Box. Il constitue une alternative à Desktop Viewer et il est conçu principalement pour les ordinateurs Windows réaffectés et les clients légers Windows. Desktop Lock remplace le shell Windows et le Gestionnaire des tâches dans ces machines utilisateur, ce qui empêche les utilisateurs d'accéder à des machines sous-jacentes. Grâce à Desktop Lock, les utilisateurs peuvent accéder aux bureaux Windows Server Machine et aux ordinateurs de bureau Windows. l'installation de Desktop Lock est facultative.




Un utilisateur ouvre une session sur une machine avec une carte à puce. Si Desktop Lock est en cours d'exécution sur la machine, celle-ci est configurée pour démarrer un site Desktop Appliance au travers d'Internet Explorer exécuté en mode Kiosque. Un contrôle ActiveX présent sur le site invite l'utilisateur à entrer un code confidentiel, et l'envoie à StoreFront. StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à Citrix Virtual Apps ou Citrix Virtual Desktops. Le premier bureau disponible de la liste alphabétique d'un groupe de bureaux attribué démarre.

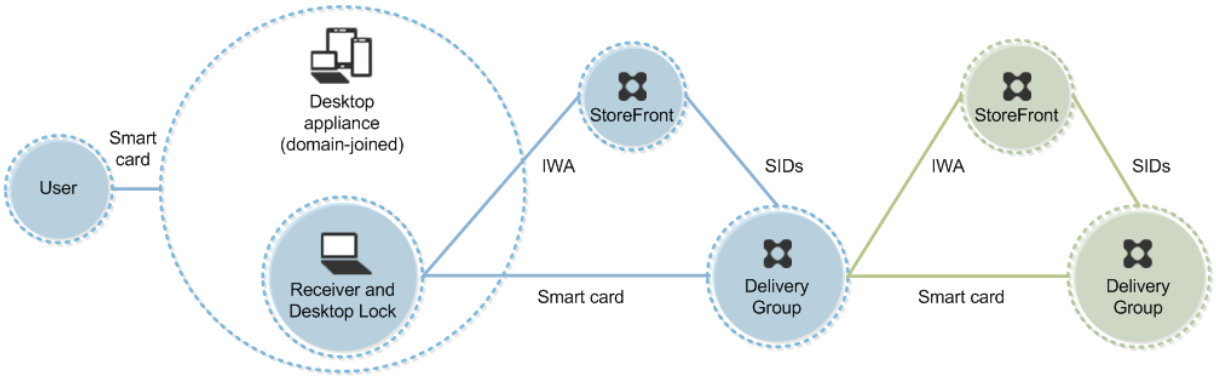
Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

### Exemple de déploiement : ordinateurs appartenant à un domaine et clients légers accédant à StoreFront via l'adresse URL XenApp Services

Ce déploiement implique des machines utilisateur appartenant à un domaine qui exécutent Desktop Lock et se connectent à StoreFront via les adresses URL XenApp Services.

Desktop Lock est un composant distinct fourni avec Citrix Virtual Apps, Citrix Virtual Desktops et VDI-in-a-Box. Il constitue une alternative à Desktop Viewer et il est conçu principalement pour les ordinateurs Windows réaffectés et les clients légers Windows. Desktop Lock remplace le shell Windows et le Gestionnaire des tâches dans ces machines utilisateur, ce qui empêche les utilisateurs d'accéder à des machines sous-jacentes. Grâce à Desktop Lock, les utilisateurs peuvent accéder aux bureaux Windows Server Machine et aux ordinateurs de bureau Windows. l'installation de Desktop Lock est facultative.




Un utilisateur ouvre une session sur une machine à l'aide d'une carte à puce et du code confidentiel. Si Desktop Lock est en cours d'exécution sur la machine, il authentifie l'utilisateur à un serveur StoreFront à l'aide de l'authentification Windows intégrée (IWA). StoreFront transmet les identificateurs de sécurité (SID) de l'utilisateur à Citrix Virtual Apps ou Citrix Virtual Desktops. Lorsque l'utilisateur démarre un bureau virtuel, l'utilisateur n'est pas invité à entrer un code confidentiel, car la fonctionnalité d'authentification unique est configurée sur Receiver.

Ce déploiement peut être étendu à une DMZ double avec l'ajout d'un deuxième serveur StoreFront et un serveur hébergeant des applications. Un Receiver depuis le bureau virtuel s'authentifie sur le deuxième serveur StoreFront. Toute méthode d'authentification peut être utilisée pour cette seconde connexion. La configuration indiquée pour le premier hop peut être réutilisée dans le deuxième hop ou utilisée dans le deuxième hop uniquement.

## Authentification pass-through et Single Sign-On avec des cartes à puce

June 27, 2024

### Authentification pass-through

L'authentification pass-through avec des cartes à puce sur les bureaux virtuels est prise en charge sur les machines utilisateur exécutant Windows 10, Windows 8 et Windows 7 SP1, éditions Enterprise et Professional.

L'authentification pass-through avec des cartes à puce sur les applications hébergées est prise en charge sur les serveurs exécutant Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 et Windows Server 2008 R2 SP1

Pour utiliser l'authentification unique avec des applications hébergées sur des cartes à puce, vous devez activer l'utilisation de Kerberos lorsque vous configurez Authentification unique avec carte à puce comme méthode d'authentification pour le site.

Remarque : la disponibilité de l'authentification pass-through avec des cartes à puce dépend de nombreux facteurs, notamment, mais pas exclusivement :

- les stratégies de sécurité de votre organisation concernant l'authentification pass-through.
- Type et configuration de logiciels intermédiaires.
- Types de lecteur de carte à puce.
- Stratégie de mise en cache du code confidentiel de logiciels intermédiaires.

L'authentification pass-through avec des cartes à puce est configurée sur Citrix StoreFront. Consultez la documentation StoreFront pour plus de détails.

### Single Sign-On

Citrix Single Sign-On est une fonctionnalité qui implémente l'authentification unique lors du lancement de bureaux virtuels et d'applications. Vous pouvez utiliser cette fonctionnalité dans des déploiements de carte à puce, appartenant à un domaine, direct-to-StoreFront et appartenant à un domaine, NetScaler-to-StoreFront pour réduire le nombre de fois où les utilisateurs entrent leur code confidentiel. Pour utiliser l'authentification unique dans ces types de déploiement, modifiez les paramètres suivants dans le fichier default.ica, qui se trouve sur le serveur StoreFront :

- Déploiements de carte à puce appartenant à un domaine, directement vers StoreFront : définissez DisableCtrlAltDel sur Off
- Déploiements de carte à puce appartenant à un domaine, NetScaler vers StoreFront : définissez UseLocalUserAndPassword sur On

Pour obtenir des instructions sur la configuration de ces paramètres, consultez la documentation de StoreFront ou Citrix Gateway.

La disponibilité de la fonctionnalité d'authentification unique dépend de nombreux facteurs, notamment, mais pas exclusivement :

- Les stratégies de sécurité de votre organisation relatives à l'authentification unique.
- Type et configuration de logiciels intermédiaires.
- Types de lecteur de carte à puce.
- Stratégie de mise en cache du code confidentiel de logiciels intermédiaires.

> **Remarque :**
>
> Lorsqu'un utilisateur ouvre une session sur Virtual Delivery Agent (VDA) sur une machine lorsqu'un lecteur de carte à puce est connecté, une mosaïque Windows peut sembler représenter le mode d'authentification précédent réussi, tel qu'une carte à puce ou un mot de passe. Par conséquent, lorsque l'authentification unique est activée, la mosaïque d'authentification unique peut s'afficher. Pour ouvrir une session, l'utilisateur doit sélectionner **Changer d'utilisateurs** pour sélectionner une autre mosaïque car la mosaïque d'authentification unique ne fonctionne pas.

## Transport Layer Security (TLS)

June 27, 2024

Citrix Virtual Apps and Desktops prend en charge le protocole TLS (Transport Layer Security) pour les connexions TCP entre composants. Citrix Virtual Apps and Desktops prend également en charge le protocole DTLS (Datagram Transport Layer Security) pour les connexions ICA/HDX basées sur UDP, en utilisant letransport adaptatif.

TLS et DTLS sont similaires et prennent en charge les mêmes certificats numériques. La configuration d'un site Citrix Virtual Apps ou Citrix Virtual Desktops pour utiliser TLS le configure également pour utiliser DTLS. Utilisez les procédures suivantes ; les étapes suivantes sont communes à TLS et DTLS sauf mention contraire :

- Obtenez, installez et enregistrez un certificat de serveur sur tous les Delivery Controller, et configurer un port avec le certificat TLS. Pour de plus amples informations, consultez la rubrique Installer les certificats de serveur TLS sur des Controller.

  Si vous le souhaitez, vous pouvez modifier les ports que le Controller utilise pour écouter le trafic HTTP et HTTPS.

- Activez les connexions TLS entre l'application Citrix Workspace et Virtual Delivery Agents (VDA) en renseignant les tâches suivantes :

  - Configurez TLS sur les machines où le VDA est installé. (Par commodité, les références supplémentaires aux machines sur lesquelles les VDA sont installés sont simplement appelées « VDA ».) Vous trouverez des informations générales dans la section Paramètres TLS sur les VDA. Il est fortement recommandé d'utiliser le script PowerShell fourni par Citrix pour configurer TLS/DTLS. Pour plus de détails, consultez la section Configurer TLS sur un VDA à l'aide du script PowerShell. Toutefois, si vous souhaitez configurer TLS/DTLS manuellement, veuillez consulter la section Configurer manuellement TLS sur un VDA.

- Configurez TSL dans les groupes de mise à disposition contenant les VDA en exécutant un jeu de cmdlets PowerShell dans Studio. Pour de plus amples informations, consultez la section Configurer TLS sur les groupes de mise à disposition.

  Configuration requise et considérations :

  * L'activation des connexions TLS entre les utilisateurs et les VDA est valide uniquement pour les sites XenApp 7.6 et XenDesktop 7.6, ainsi que les versions ultérieures prises en charge.
  * Configurez TLS dans les groupes de mise à disposition et le VDA après l'installation de composants, créez un site, créez des catalogues de machines, et créez des groupes de mise à disposition.
  * Pour configurer TLS dans les groupes de mise à disposition, vous devez disposer de l'autorisation de modification des règles d'accès de Controller. Un administrateur complet possède cette autorisation.
  * Pour configurer TLS sur les VDA, vous devez être un administrateur Windows sur la machine sur laquelle le VDA est installé.
  * Sur les VDA regroupés qui sont provisionnés par Machine Creation Services ou Provisioning Services, l'image de la machine VDA est réinitialisée au redémarrage, entraînant la perte des paramètres TLS précédents. Exécutez le script PowerShell chaque fois que le VDA est redémarré pour reconfigurer les paramètres TLS.

> **Avertissement :**
>
> Pour les tâches qui incluent l'utilisation du Registre Windows, la modification du Registre peut entraîner de sérieux problèmes qui pourraient nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Pour plus d'informations sur l'activation de TLS pour la base de données du site, consultez la section CTX137556.

### Installer les certificats de serveur TLS sur des Controller

Pour HTTPS, Le service XML prend en charge les fonctionnalités TLS par le biais de certificats de serveur mais pas de certificats de client. Cette section décrit l'acquisition et l'installation de certificats TLS dans des Delivery Controller. Les mêmes étapes peuvent être appliquées aux Cloud Connector pour chiffrer le trafic STA et XML.

Il existe différents types d'autorités de certification et méthodes pour demander un certificat, mais cet

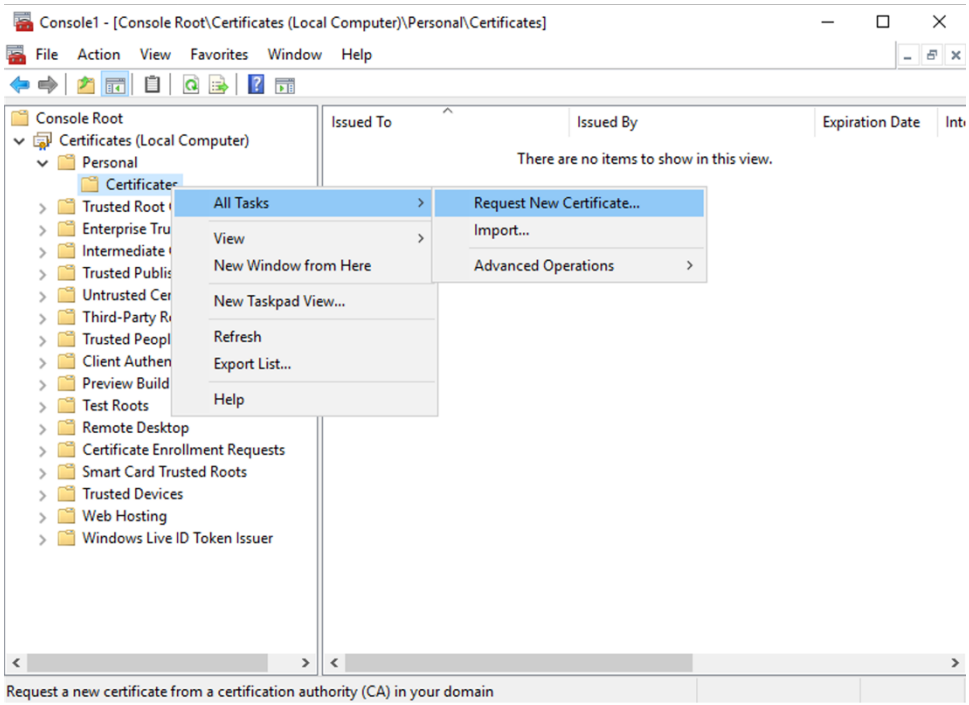
 

article décrit l'autorité de certification Microsoft. L'autorité de certification Microsoft doit disposer d'un modèle de certificat publié avec Authentification du serveur comme objectif.

Si l'autorité de certification Microsoft est intégrée à un domaine Active Directory ou à la forêt approuvée à laquelle les Delivery Controller sont joints, vous pouvez acquérir un certificat à partir de l'Assistant Inscription de certificats du composant logiciel enfichable MMC Certificats.

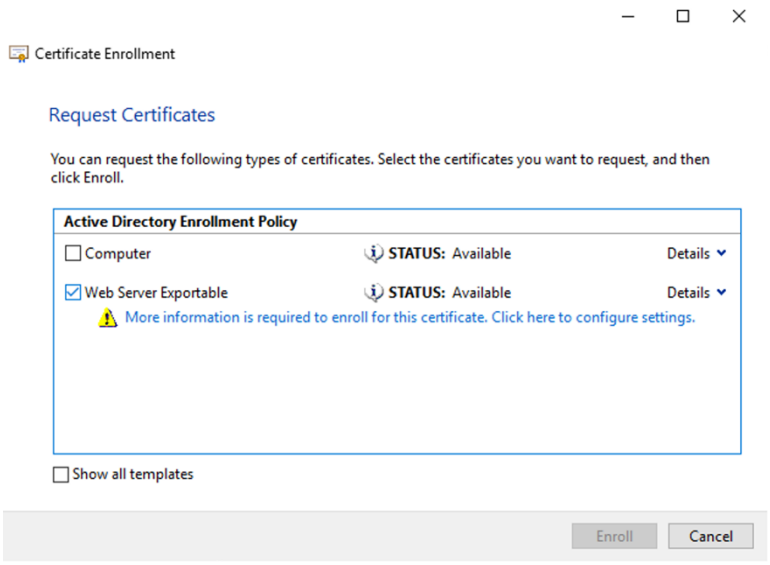
### Demande et installation d'un certificat

1. Sur le Delivery Controller, ouvrez la console MMC et ajoutez le composant logiciel enfichable Certificats. Lorsque vous y êtes invité, sélectionnez Un compte d'ordinateur.
2. Développez **Personnel > Certificats**, puis utilisez la commande de menu contextuel **Toutes les tâches > Demander un nouveau certificat**.




3. Cliquez sur **Suivant** pour commencer, puis sur **Suivant** pour confirmer que vous obtenez le certificat à partir de l'inscription Active Directory.
4. Sélectionnez le modèle de certificat d'authentification du serveur. Si le modèle a été configuré pour fournir automatiquement les valeurs du sujet, vous pouvez cliquer sur **Inscrire** sans fournir plus de détails.

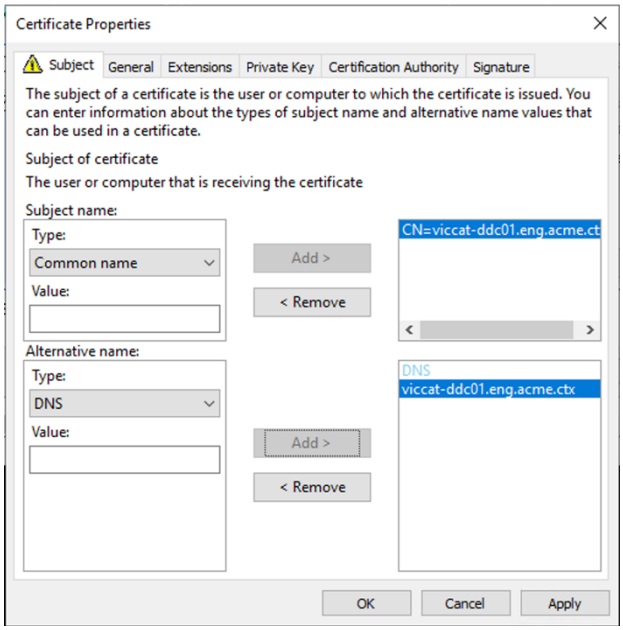
 




5. Pour fournir plus de détails sur le modèle de certificat, cliquez sur le bouton flèche **Détails** et configurez les éléments suivants :

   **Nom du sujet** : sélectionnez Nom commun et ajoutez le nom de domaine complet du Delivery Controller.

   **Autre nom** : sélectionnez DNS et ajoutez le nom de domaine complet du Delivery Controller.




### Configuration du port de l'écouteur SSL/TLS

1. Ouvrez une fenêtre de commande PowerShell en tant qu'administrateur de la machine.
2. Exécutez les commandes suivantes pour obtenir le GUID de l'application du service Broker :

```
New-PSDrive -Name HKCR -PSProvider Registry -Root
    HKEY_CLASSES_ROOT

$Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -
    Ea 0 | Where-Object {
  $key = $_; $_.GetValueNames() | ForEach-Object {
  $key.GetValue($_)  }
  | Where-Object {
  $_ -like 'Citrix Broker Service'  }
   }
  | Select-Object Name

$Service_Guid.Name -match "[A-Z0-9]*$"

$Guid = $Matches[0]

[GUID]$Formatted_Guid = $Guid

Remove-PSDrive -Name HKCR

Write-Host "Broker Service Application GUID: $($Formatted_Guid)" -
    ForegroundColor Yellow
<!--NeedCopy-->
```

3. Exécutez les commandes suivantes dans la même fenêtre PowerShell pour obtenir l'empreinte numérique du certificat que vous avez installé précédemment :

```
$HostName = ([System.Net.Dns]::GetHostByName(($env:computerName)))
    .Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-
    Object {
 $_.Subject -match ("CN=" + $HostName) }
 ).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $(
    $Thumbprint)" -Foreground Yellow
<!--NeedCopy-->
```

4. Exécutez les commandes suivantes dans la même fenêtre PowerShell pour configurer le port SSL/TLS du service Broker et utiliser le certificat pour le chiffrement :

```
$IPV4_Address = Test-Connection -ComputerName $HostName -Count 1
    | Select-Object -ExpandProperty IPV4Address

$IPPort = "$($IPV4_Address):443"

$SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
    appid={
 $Formatted_Guid }
 "

```

```
$SSLxml | netsh

. netsh http show sslcert
<!--NeedCopy-->
```

Lorsqu'elle est correctement configurée, la sortie de la dernière commande `.netsh http show sslcert` indique que l'écouteur utilise le bon `IP:port` et que `Application ID` correspond au GUID de l'application du service Broker.

Si les serveurs approuvent le certificat installé sur les Delivery Controller, vous pouvez désormais configurer les Delivery Controller StoreFront et les liaisons STA Citrix Gateway pour utiliser HTTPS au lieu de HTTP.

> **Remarque :**
>
> Si le Controller est installé sur Windows Server 2016 et que StoreFront est installé sur Windows Server 2012 R2, une modification de la configuration est nécessaire au niveau du Controller, pour modifier l'ordre des suites de chiffrement TLS. Cette modification de la configuration n'est pas nécessaire pour le Controller et StoreFront avec d'autres combinaisons de versions de Windows Server.

La liste d'ordre de la suite de chiffrement doit inclure les suites de chiffrement `TLS_ECDHE_RSA_WITH_AES_256` ou `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` (ou les deux) ; ces suites de chiffrement doivent précéder toutes les suites de chiffrement `TLS_DHE_`.

1. Dans l'éditeur de stratégie de groupe Microsoft, accédez à **Configuration ordinateur > Modèles d'administration > Réseau > Paramètres de configuration SSL**.
2. Modifiez la stratégie « Ordre des suites de chiffrement SSL ». Par défaut, cette stratégie est définie sur Non configuré. Définissez cette stratégie sur Activé.
3. Organisez les suites dans l'ordre approprié ; supprimez les suites de chiffrement que vous ne souhaitez pas utiliser.

Assurez-vous que `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` ou `TLS_ECDHE_RSA_WITH_AES_128_` précèdent les suites de chiffrement `TLS_DHE_`.

Sur Microsoft MSDN, consultez également Priorité des suites de chiffrement Schannel.

### Modifier les ports HTTP ou HTTPS

Par défaut, le service XML du Controller écoute le trafic HTTP sur le port 80 et le trafic HTTPS sur le port 443. Bien que vous puissiez utiliser des ports différents de ceux par défaut, n'oubliez pas les risques de sécurité relatifs à l'exposition d'un Controller à des réseaux non approuvés. Le déploiement d'un serveur StoreFront autonome est préférable à la modification des valeurs par défaut.

Pour modifier la valeur par défaut des ports HTTP ou HTTPS utilisés par le Controller, exécutez la commande suivante à partir de Studio :

```
BrokerService.exe -WIPORT \<http-port> -WISSLPORT \<https-port>
```

où <http-port> est le numéro de port pour le trafic HTTP et <https-port> le numéro de port pour le trafic HTTPS.

> **Remarque :**
>
> Après avoir modifié un port, il se peut que Studio affiche un message sur la compatibilité et la mise à niveau des licences. Pour résoudre le problème, ré-enregistrez les instances de service à l'aide de la séquence de l'applet de commande PowerShell suivante :

```
1 Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
     XML_HTTPS |
2 Unregister-ConfigRegisteredServiceInstance
3 Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
4 Register-ConfigServiceInstance
5 <!--NeedCopy-->
```

#### Appliquer le trafic HTTPS uniquement

Si vous souhaitez que le service XML ignore le trafic HTTP, créez le paramètre de registre suivant sur le Controller dans HKLM\Software\Citrix\DesktopServer\ et redémarrez le service Broker.

Pour ignorer le trafic HTTP, créez un DWORD XmlServicesEnableNonSsl et définissez-le sur 0.

Il existe une valeur de registre DWORD correspondante que vous pouvez créer pour ignorer le trafic HTTPS : DWORD XmlServicesEnableSsl. Assurez-vous qu'elle n'est pas définie sur 0.

### Paramètres TLS sur les VDA

Un groupe de mise à disposition ne peut pas avoir un mélange d'un VDA avec TLS configuré et d'autres VDA sans TLS configuré. Avant de configurer le protocole TLS pour un groupe de mise à disposition, vous devez avoir déjà configuré TLS pour tous les VDA dans ce groupe de mise à disposition.

Lorsque vous configurez le protocole TLS sur les VDA, les autorisations sur le certificat TLS installé sont modifiées, offrant au service ICA un accès en lecture à la clé privée du certificat, et informant le service ICA des opérations suivantes :

- **Quel certificat du magasin de certificats utiliser pour TLS**.
- **Quel numéro de port TCP utiliser pour les connexions TLS**.

  Le Pare-feu Windows (s'il est activé) doit être configuré pour autoriser les connexions entrantes sur ce port TCP. Cette configuration est effectuée pour vous si vous utilisez le script PowerShell.

- **Versions du protocole TLS à autoriser.**

  > **Important :**
  >
  > Citrix vous recommande de vérifier leur utilisation de SSLv3 et de reconfigurer ces déploiements pour supprimer la prise en charge de SSLv3, le cas échéant. Consultez l'article CTX200238.

  Les versions prises en charge du protocole TLS suivent une hiérarchie (de la plus basse à la plus élevée) : SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 et TLS 1.3. Spécifiez la version minimale autorisée ; toutes les connexions de protocole utilisant cette version ou une version supérieure sont autorisées.

  Par exemple, si vous spécifiez TLS 1.1 comme version minimale, les connexions de protocole TLS 1.1 et TLS 1.3 sont autorisées. Si vous spécifiez SSL 3.0 en tant que version minimale, les connexions pour toutes les versions prises en charge sont alors autorisées. Si vous spécifiez TLS 1.3 comme version minimale, seules les connexions TLS 1.3 sont autorisées.

  DTLS 1.0 correspond à TLS 1.1, et DTLS 1.3 correspond à TLS 1.3.

- **Suites de chiffrement TLS à autoriser.**

  Une suite de chiffrement sélectionne le cryptage qui sera utilisé pour une connexion. Les clients et les VDA peuvent prendre en charge plusieurs ensembles de suites de chiffrement. Lorsqu'un client (app Citrix Workspace ou StoreFront) se connecte et envoie une liste des suites de chiffrement TLS pris en charge, le VDA fait correspondre une des suites de chiffrement du client avec l'une de suites de chiffrement de sa liste configurée et accepte la connexion. S'il n'existe aucune correspondance de suite de chiffrement, le VDA rejette la connexion.

  Le VDA prend en charge trois ensembles de suites de chiffrement (également appelés modes de conformité) : GOV (gouvernement), COM (commercial) et ALL (tout). Les suites de chiffrement acceptables dépendent du mode FIPS Windows ; voir http://support.microsoft.com/kb/811833 pour plus d'informations sur le mode FIPS Windows. Le tableau suivant répertorie les suites de chiffrement compris dans chaque ensemble :

| **Suite de chiffrement TLS/DTLS** | **TOUT** | **COM** | **GOV** | **TOUT** | **COM** | **GOV** |
|---|---|---|---|---|---|---|
| **Mode FIPS** | Désactivé | Désactivé | Désactivé | On | On | On |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384* | X | | | X | | X |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | X | | | X | | X |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | X | | | X | X | |

| Suite de chiffrement TLS/DTLS | TOUT | COM | GOV | TOUT | COM | GOV |
|---|---|---|---|---|---|---|

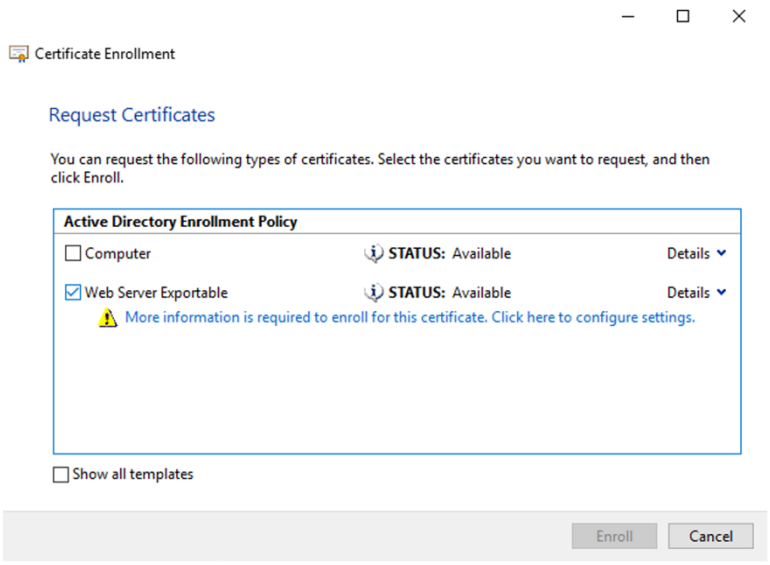
* Non pris en charge dans Windows Server 2012 R2.

> **Remarque :**
>
> Le VDA ne prend pas en charge les suites de chiffrement DHE (par exemple, TLS_DHE_RSA_WITH_AES_256_GCM_ TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 et TLS_DHE_RSA_WITH_AES_128_CBC_SHA). Si elles sont sélectionnées par Windows, elles ne peuvent pas être utilisées par Receiver.
>
> Si vous utilisez Citrix Gateway, reportez-vous à la documentation Citrix ADC pour plus d'informations sur la prise en charge de suite de chiffrement pour les communications back-end. Pour plus d'informations sur la prise en charge de la suite de chiffrement TLS, consultez la section Suites de chiffrement disponibles sur les appliances Citrix ADC. Pour plus d'informations sur la prise en charge de la suite de chiffrement DTLS, reportez-vous à la section Prise en charge du chiffrement DTLS.

#### Demande et installation d'un certificat

1. Sur le VDA, ouvrez la console MMC et ajoutez le composant logiciel enfichable Certificats. Lorsque vous y êtes invité, sélectionnez Un compte d'ordinateur.
2. Développez **Personnel > Certificats**, puis utilisez la commande de menu contextuel **Toutes les tâches > Demander un nouveau certificat**.
3. Cliquez sur **Suivant** pour commencer, puis sur **Suivant** pour confirmer que vous obtenez le certificat à partir de l'inscription Active Directory.
4. Sélectionnez le modèle de certificat d'authentification du serveur. L'**ordinateur** Windows par défaut ou le **serveur Web exportable** sont tous deux acceptables. Si le modèle a été configuré pour fournir automatiquement les valeurs du sujet, vous pouvez cliquer sur **Inscrire** sans fournir plus de détails.

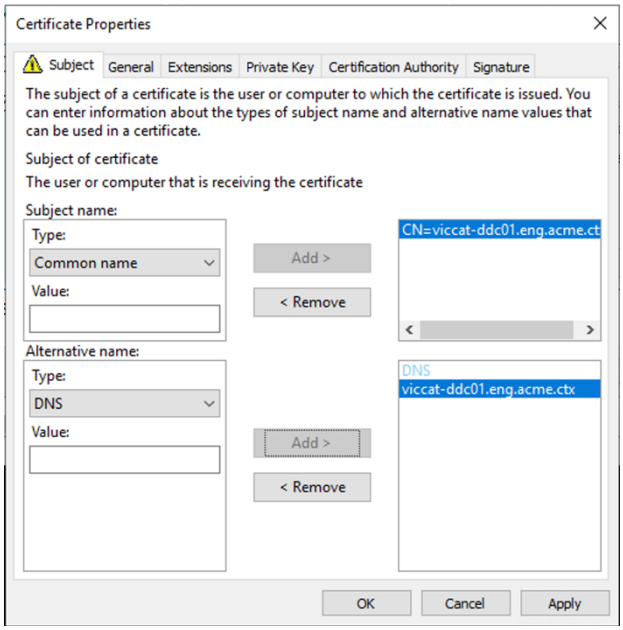
 




5. Pour fournir plus de détails sur le modèle de certificat, cliquez sur **Détails** et configurez les éléments suivants :

   **Nom du sujet** : sélectionnez le type **Nom commun** et ajoutez le nom de domaine complet du VDA

   **Autre nom** : sélectionnez le type **DNS** et ajoutez le nom de domaine complet du VDA



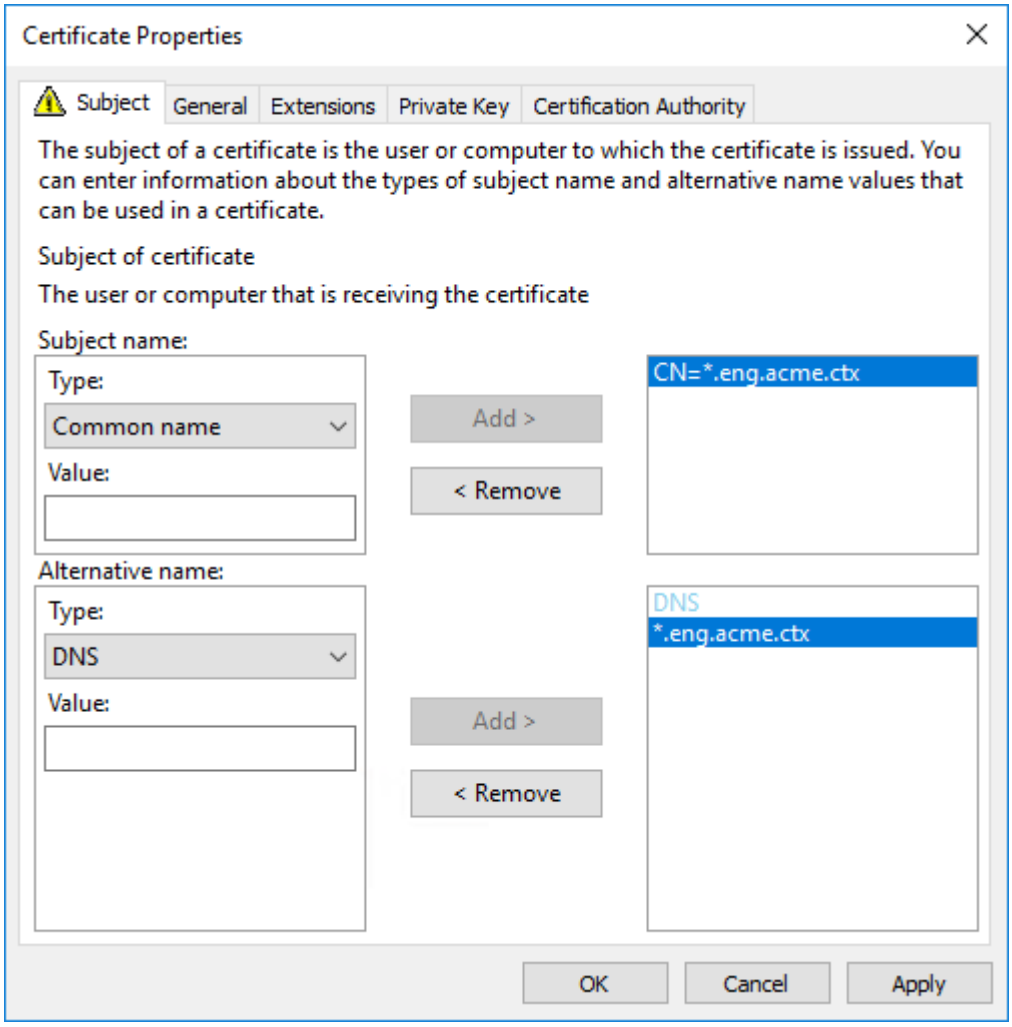

> **Remarque :**
>
> Utilisez l'inscription automatique des certificats des services de certificats Active Directory pour automatiser l'émission et le déploiement de certificats sur les VDA. Elle est décrite dans la section https://support.citrix.com/article/CTX205473.

Vous pouvez utiliser des certificats génériques pour autoriser un seul certificat à sécuriser plusieurs VDA :

**Nom du sujet** : sélectionnez le type **Nom commun** et ajoutez le *.domaine.complet des VDA

**Autre nom** : sélectionnez le type **DNS** et ajoutez le *.domaine.complet des VDA

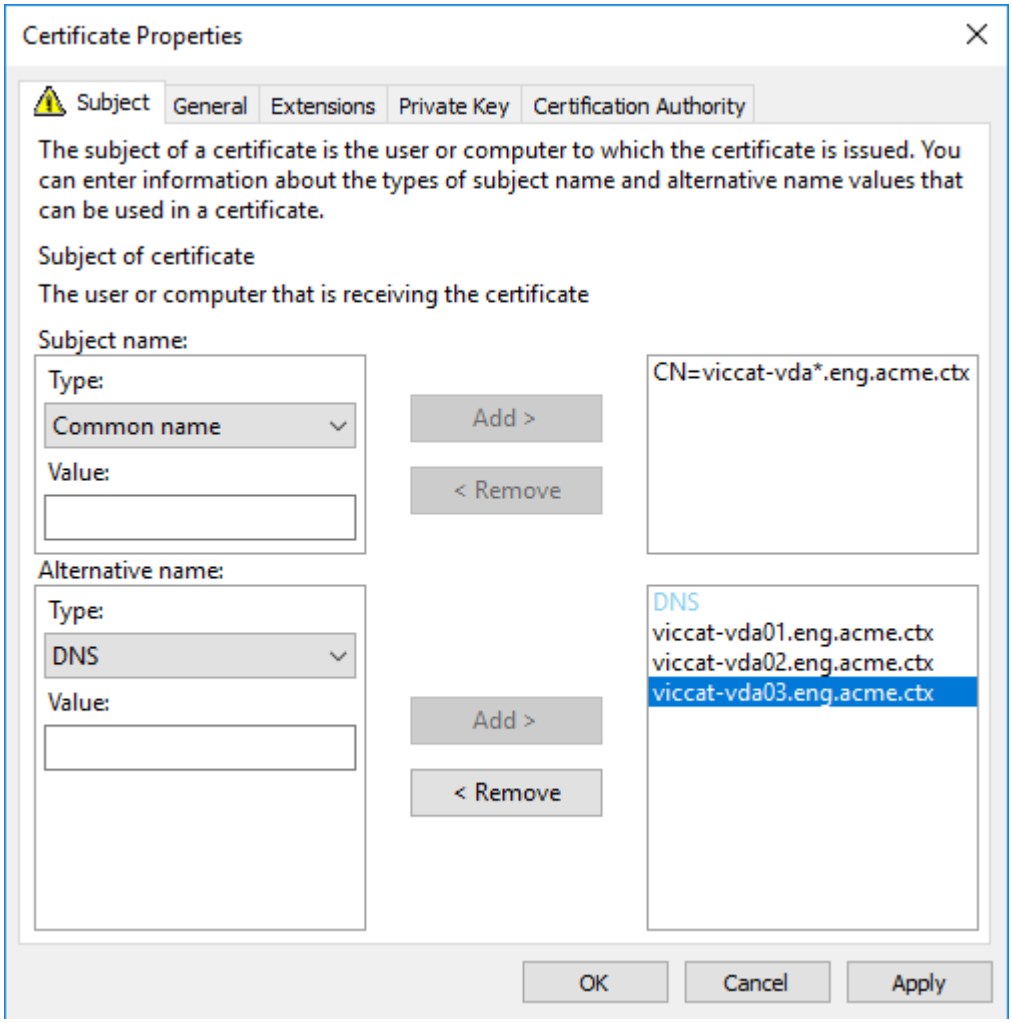



Vous pouvez utiliser des certificats SAN pour autoriser un seul certificat à sécuriser plusieurs VDA spécifiques :

**Nom du sujet** : sélectionnez le type **Nom commun** et entrez une chaîne pour identifier l'utilisation du certificat

**Autre nom** : sélectionnez le type **DNS** et ajoutez une entrée pour le nom de domaine complet de chaque VDA. Limitez le nombre de noms alternatifs au minimum pour garantir une négociation TLS optimale.

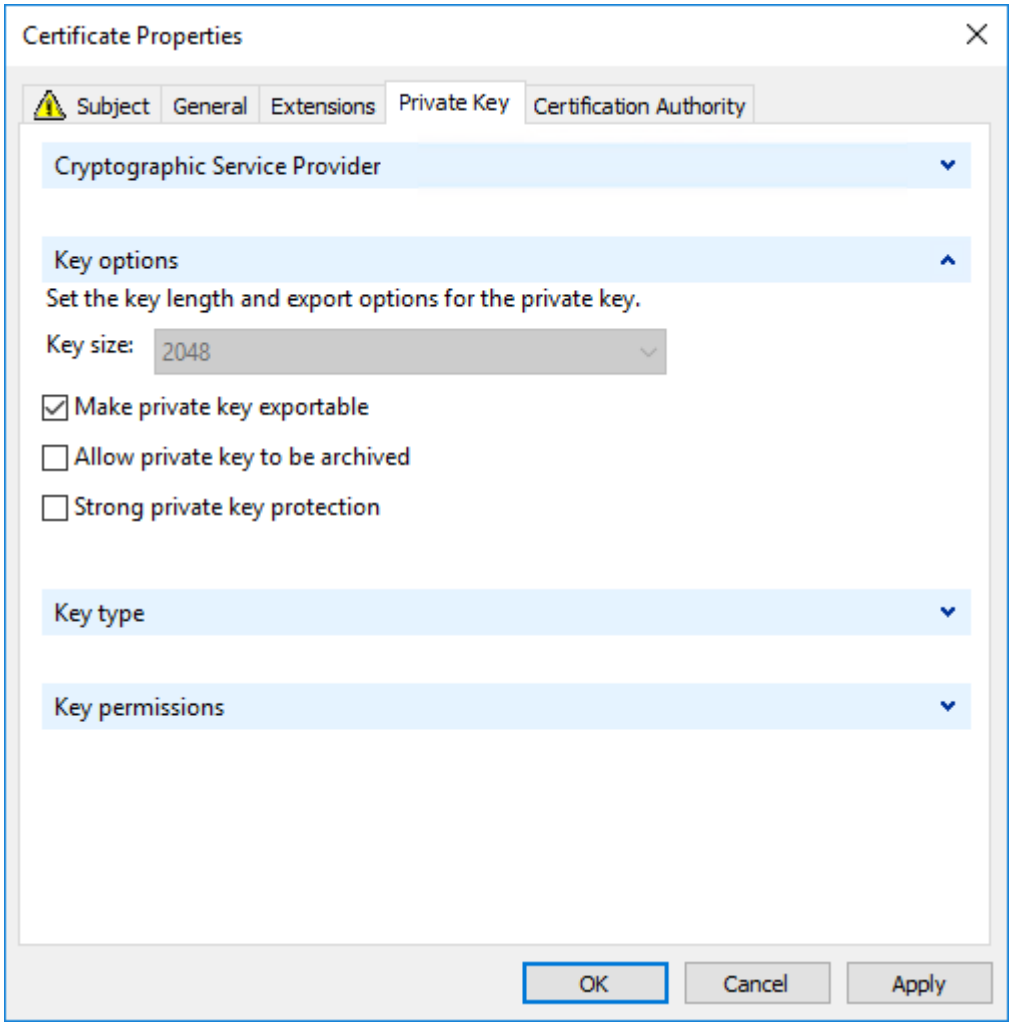
 




**Remarque :**

Les certificats génériques et SAN nécessitent que l'option **Permettre l'exportation de la clé privée** de l'onglet Clé privée soit sélectionnée :




**Configurer TLS sur un VDA à l'aide du script PowerShell**

Installez le certificat TLS dans la zone Ordinateur local > Personnel > Certificats du magasin de certificats. Si plusieurs certificats résident à cet emplacement, fournissez l'empreinte numérique du certificat au script PowerShell.

> **Remarque :**
>
> À compter de XenApp et XenDesktop 7.16 LTSR, le script PowerShell trouve le certificat approprié en fonction du nom de domaine complet du VDA. Vous n'avez pas besoin de fournir l'empreinte si un seul certificat est présent pour le nom de domaine complet du VDA.

Le script Enable-VdaSSL.ps1 active ou désactive l'écouteur TLS sur un VDA. Ce script est disponible dans le dossier *Support* > *Tools* > *SslSupport* sur le support d'installation.

Lorsque vous activez TLS, les suites de chiffrement DHE sont désactivées. Les suites de chiffrement ECDHE ne sont pas affectées.

Lorsque vous activez le protocole TLS, le script désactive toutes les règles de pare-feu Windows existantes pour le port TCP spécifié. Ensuite, il ajoute une règle qui permet au service ICA d'accepter les connexions entrantes uniquement sur les ports TLS TCP et UDP. Cela désactive également les règles du Pare-feu Windows pour :

- Citrix ICA (valeur par défaut : 1494)
- Citrix CGP (valeur par défaut : 2598)
- Citrix WebSocket (valeur par défaut : 8008)

Les utilisateurs peuvent uniquement se connecter en utilisant TLS ou DTLS. Ils ne peuvent pas utiliser ICA/HDX, ICA/HDX avec fiabilité de session ou HDX sur WebSocket, sans TLS ou DTLS.

> **Remarque :**
>
> DTLS n'est pas pris en charge avec ICA/HDX Audio via UDP Real-time Transport ou avec ICA/HDX Framehawk.

Consultez Ports réseau.

Le script contient des descriptions de la syntaxe suivante, ainsi que d'autres exemples ; vous pouvez utiliser un outil tel que le Bloc-notes++ pour consulter ces informations.

> **Important :**
>
> Spécifiez soit le paramètre Enable ou Disable de même que le paramètre CertificateThumbPrint. Les autres paramètres sont facultatifs.

**Syntaxe** `Enable-VdaSSL { -Enable | -Disable } -CertificateThumbPrint "<thumbprint>"[-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite"\<suite>"]`

| Paramètre | Description |
|---|---|
| Activer | Installe et active l'écouteur TLS sur le VDA. Soit ce paramètre ou le paramètre Disable est requis. |
| Désactiver | Désactive l'écouteur TLS sur le VDA. Soit ce paramètre ou le paramètre Enable est requis. Si vous spécifiez ce paramètre, aucun autre paramètre n'est valide. |

| Paramètre | Description |
| --- | --- |
| CertificateThumbPrint “” | Empreinte numérique du certificat TLS dans le magasin de certificats, entourée de guillemets. Le script utilise l’empreinte numérique spécifiée pour sélectionner le certificat que vous voulez utiliser. Si ce paramètre est omis, un certificat incorrect est sélectionné. |
| SSLPort | Port TLS. Valeur par défaut : 443 |
| SSLMinVersion “” | Version minimale du protocole TLS, entourés de guillemets. Valeurs valides : « TLS_1.0 » (par défaut), « TLS_1.1 » et « TLS_1.3 ». |
| SSLCipherSuite “” | Suite de chiffrement TLS, entourés de guillemets. Les valeurs valides sont : « GOV », « COM » et « ALL » (par défaut). |

**Exemples** Le script suivant installe et active la version de protocole TLS. L’empreinte numérique (représentée en tant que « 12345678987654321 » dans cet exemple) est utilisée pour sélectionner le certificat à utiliser.

```
Enable-VdaSSL -Enable -CertificateThumbPrint "12345678987654321"
```

Le script suivant installe et active l’écouteur TLS et spécifie le port TLS 400, la suite de chiffrement GOV et une valeur de protocole minimale de TLS 1.2. L’empreinte numérique (représentée en tant que « 12345678987654321 » dans cet exemple) est utilisée pour sélectionner le certificat à utiliser.

```
Enable-VdaSSL -Enable
-CertificateThumbPrint "12345678987654321"
-SSLPort 400 -SSLMinVersion "TLS_1.3"
-SSLCipherSuite "All"
```

Le script suivant désactive l’écouteur TLS sur le VDA.

```
Enable-VdaSSL -Disable
```

#### Configurer manuellement TLS sur un VDA

Lors de la configuration manuelle de TLS sur un VDA, vous offrez un accès en lecture générique à la clé privée du certificat TLS pour le service approprié sur chaque VDA : NT SERVICE\PorticaService pour un VDA pour OS mono-session Windows, ou NT SERVICE\TermService pour un VDA pour OS multi-session Windows. Sur la machine sur laquelle le VDA est installé :

**ÉTAPE 1**. Lancez la console MMC (Microsoft Management Console) : Démarrer > Exécuter > mmc.exe.

**ÉTAPE 2**. Ajouter le composant logiciel enfichable Certificats à la console MMC :

1. Sélectionnez Fichier > Ajouter/Supprimer un composant logiciel enfichable.
2. Sélectionnez Certificats et cliquez sur Ajouter.
3. Lorsque vous y êtes invité par « Ce composant logiciel enfichable gérera toujours les certificats pour : », choisissez « Le compte d'ordinateur », puis cliquez sur Suivant.
4. Lorsque vous y êtes invité par « Sélectionnez l'ordinateur à gérer par ce composant logiciel enfichable », choisissez « Ordinateur local », puis cliquez sur Terminer.

**ÉTAPE 3**. Sous Certificats (Ordinateur local) > Personnel > Certificats, cliquez avec le bouton droit de la souris sur le certificat, puis sélectionnez Toutes les tâches > Gérer les clés privées.

**ÉTAPE 4.** L'Éditeur de liste de contrôle d'accès affiche « Autorisations pour les clés privées (NomConvivial) » où (NomConvivial) est le nom de votre certificat TLS. Ajoutez l'un des services suivants et accordez-lui un accès en lecture :

- Pour un VDA pour OS mono-session Windows, « PORTICASERVICE »
- Pour un VDA pour OS multi-session Windows, « TERMSERVICE »

**ÉTAPE 5.** Cliquez deux fois sur le certificat TLS installé. Dans la boîte de dialogue du certificat, sélectionnez l'onglet Détails, puis faites défiler vers le bas. Cliquez sur Empreinte numérique.

**ÉTAPE 6.** Exécutez la commande regedit et rendez-vous sur HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.

1. Modifier la clé d'empreinte numérique SSL et copiez la valeur de l'empreinte numérique du certificat TLS dans cette valeur binaire. Vous pouvez ignorer sans risque les éléments inconnus dans la boîte de dialogue Modifier la valeur binaire (tels que '0000'et les caractères spéciaux).
2. Modifier la clé SSLEnabled et modifiez la valeur DWORD sur 1. (Pour désactiver SSL ultérieurement, changez la valeur DWORD sur 0).
3. Si vous souhaitez modifier les paramètres par défaut (facultatif), utilisez les informations suivantes dans le même chemin d'accès du Registre :

   SSLPort DWORD : numéro de port SSL. Valeur par défaut : 443.

   SSLMinVersion DWORD : 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.3. Valeur par défaut : 2 (TLS 1.0).

   SSLCipherSuite DWORD : 1 = GOV, 2 = COM, 3 = ALL. Valeur par défaut : 3 (ALL).

**ÉTAPE 7.** Assurez-vous que les ports TLS TCP et UDP sont ouverts dans le Pare-feu Windows s'il ne s'agit pas de la valeur par défaut (443). (Lors de la création de la règle de trafic entrant dans le Pare-feu

Windows, assurez-vous que ses propriétés possèdent les entrées sélectionnées « Autoriser la connexion » et « Activé ».)

**ÉTAPE 8.** Assurez-vous qu'aucune autre application ou service (tel que IIS) utilisent le port TCP TLS.

**ÉTAPE 9.** Pour les VDA pour OS multi-session Windows, redémarrez la machine pour que les modifications prennent effet. (Il n'est pas nécessaire de redémarrer les machines contenant des VDA pour OS mono-session Windows).

> **Important :**
>
> Une étape supplémentaire est nécessaire lorsque le VDA se trouve sur un serveur Windows Server 2012 R2, Windows Server 2016 ou Windows 10 Anniversary Edition ou une version ultérieure prise en charge. Cela affecte les connexions à partir de Citrix Receiver pour Windows (version 4.6 à 4.9), l'application Citrix Workspace pour HTML5 et l'application Citrix Workspace pour Chrome. Cela inclut également les connexions utilisant Citrix Gateway.
>
> Cette étape est également requise pour toutes les connexions utilisant Citrix Gateway, pour toutes les versions de VDA, si TLS est configuré entre Citrix Gateway et le VDA. Cela affecte toutes les versions de Citrix Receiver.

Sur le VDA (Windows Server 2012 R2, Windows Server 2016 ou Windows 10 Anniversary Edition ou version ultérieure), à l'aide de l'éditeur de stratégie de groupe, accédez à Configuration ordinateur > Stratégies > Modèles d'administration > Réseau > Paramètres de configuration SSL > Ordre des suites de chiffrement SSL. Sélectionnez l'ordre suivant :

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

> **Remarque :**
>
> Les six premiers éléments spécifient également la courbe elliptique, P384 ou P256. Assurez-vous que l'option « curve25519 » n'est pas sélectionnée. Le mode FIPS n'empêche pas l'utilisation de l'option « curve25519 ».

Lorsque ce paramètre de stratégie de groupe est configuré, le VDA sélectionnera une suite de chiffrement uniquement si elle apparaît dans les deux listes : la liste Stratégies de groupe et la liste pour le mode de conformité sélectionné (COM, GOV ou ALL). La suite de chiffrement doit également s'afficher dans la liste envoyée par le client (application Citrix Workspace ou StoreFront).

Cette configuration de stratégie de groupe affecte également d'autres applications et services TLS sur le VDA. Si vos applications requièrent des suites de chiffrement spécifiques, vous devez les ajouter à la liste Stratégie de groupe.

> **Important :**
>
> Même si les modifications de stratégie de groupe sont affichées lorsqu'elles sont appliquées, les modifications de stratégie de groupe pour la configuration TLS ne prennent effet qu'après le redémarrage du système d'exploitation. Par conséquent, pour les bureaux regroupés, appliquez les modifications de stratégie de groupe pour la configuration TLS à l'image de base.

#### Configurer TLS sur les groupes de mise à disposition

Effectuez cette procédure pour chaque groupe de mise à disposition qui contient les VDA vous avez configurés pour les connexions TLS.

1. À partir de Studio, ouvrez la console PowerShell.
2. Exécutez **asnp Citrix.*** pour charger les applets de commande du produit Citrix.
3. Exécutez **Get-BrokerAccessPolicyRule -DesktopGroupName '*<groupe-mise-à-disposition>*' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true**.
4. Exécutez **Set-BrokerSite -DnsResolutionEnabled $true**.

#### Dépannage

Si une erreur de connexion se produit, consultez le journal des événements système du VDA.

Lorsque vous utilisez l'application Citrix Workspace pour Windows, si vous recevez une erreur de connexion qui indique une erreur TLS, désactivez Desktop Viewer et essayez de vous reconnecter. Bien que la connexion échoue encore, une description du problème TLS sous-jacent peut être fournie. Par exemple, vous avez spécifié un modèle incorrect lors de la demande d'un certificat à partir de l'autorité de certification.

La plupart des configurations utilisant HDX Adaptive Transport fonctionnent avec DTLS, y compris celles qui utilisent les dernières versions de application Citrix Workspace, Citrix Gateway et VDA. Certaines configurations qui utilisent DTLS entre application Citrix Workspace et Citrix Gateway et qui utilisent DTLS entre Citrix Gateway et le VDA requièrent des actions supplémentaires.

Des actions supplémentaires sont nécessaires si :

- la version Citrix Receiver prend en charge HDX Adaptive Transport et DTLS : Receiver pour Windows (4.7, 4.8, 4.9), Receiver pour Mac (12.5, 12.6, 12.7), Receiver pour iOS (7.2, 7.3.x) ou Receiver pour Linux (13.7)

et l'une des conditions suivantes s'applique également :

- la version Citrix Gateway prend en charge DTLS sur le VDA, mais la version VDA ne prend pas en charge DTLS (version 7.15 ou antérieure),

- la version VDA prend en charge DTLS (version 7.16 ou ultérieure), mais la version Citrix Gateway ne prend pas en charge DTLS sur le VDA.

Pour éviter l'échec des connexions de Citrix Receiver, effectuez l'une des opérations suivantes :

- mettre à jour Citrix Receiver vers Receiver pour Windows version 4.10 ou ultérieure, Receiver pour Mac 12.8 ou version ultérieure ou Receiver pour iOS version 7.5 ou ultérieure ; ou,
- mettre à jour Citrix Gateway vers une version qui prend en charge DTLS vers le VDA ; ou,
- mettre à jour le VDA vers la version 7.16 ou ultérieure ; ou,
- désactiver DTLS sur le VDA ; ou,
- désactiver HDX Adaptive Transport.

> **Remarque :**
>
> Une mise à jour appropriée pour Receiver pour Linux n'est pas encore disponible. Receiver pour Android (version 3.12.3) ne prend pas en charge HDX Adaptive Transport et DTLS via Citrix Gateway et n'est donc pas affecté.
>
> Pour désactiver DTLS sur le VDA, modifiez la configuration du pare-feu VDA pour désactiver le port UDP 443. Voir Ports réseau.

### Communications entre le Controller et le VDA

La protection des messages de Windows Communication Framework (WCF) sécurise les communications entre le Controller et le VDA. Une protection supplémentaire au niveau du transport à l'aide de TLS n'est pas requise. La configuration WCF utilise Kerberos pour l'authentification mutuelle entre le Controller et le VDA. Le cryptage utilise AES en mode CBC avec une clé 256 bits. L'intégrité des messages est assurée par SHA-1.

Selon Microsoft, les protocoles de sécurité utilisés par WCF sont conformes aux normes OASIS (Organization for the Advancement of Structured Information Standards), y compris la stratégie WS-SecurityPolicy 1.2. En outre, Microsoft indique que WCF prend en charge tous les jeux d'algorithmes répertoriés dans la stratégie de sécurité 1.2.

Les communications entre les Controller et les VDA utilisent le jeu d'algorithmes basic256, dont les algorithmes sont indiqués ci-dessus.

#### Redirection vidéo TLS et HTML5 / Redirection du contenu du navigateur

Vous pouvez utiliser la redirection vidéo HTML5 et la redirection du contenu du navigateur pour rediriger les sites Web HTTPS. Le code JavaScript injecté sur ces sites Web doit établir une connexion TLS avec le service de redirection vidéo Citrix HDX HTML5 qui s'exécute sur le VDA. Pour ce faire,

le service de redirection vidéo HTML5 génère deux certificats personnalisés dans le magasin de certificats sur le VDA. L'arrêt de ce service supprime les certificats.

La redirection vidéo HTML5 est désactivée par défaut.

La redirection du contenu du navigateur est activée par défaut.

Pour plus d'informations sur la redirection de la vidéo pour HTML5, consultez la section Paramètres de stratégie multimédia.

## Transport Layer Security (TLS) sur le serveur d'impression universelle

June 27, 2024

Le protocole TLS (Transport Layer Security) est pris en charge pour les connexions basées sur TCP entre le Virtual Delivery Agent (VDA) et le serveur d'impression universelle.

> **Avertissement :**
>
> Pour les tâches qui incluent l'utilisation du registre Windows, la modification du registre peut entraîner de sérieux problèmes qui peuvent nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

### Types de connexions d'impression entre le VDA et le serveur d'impression universelle

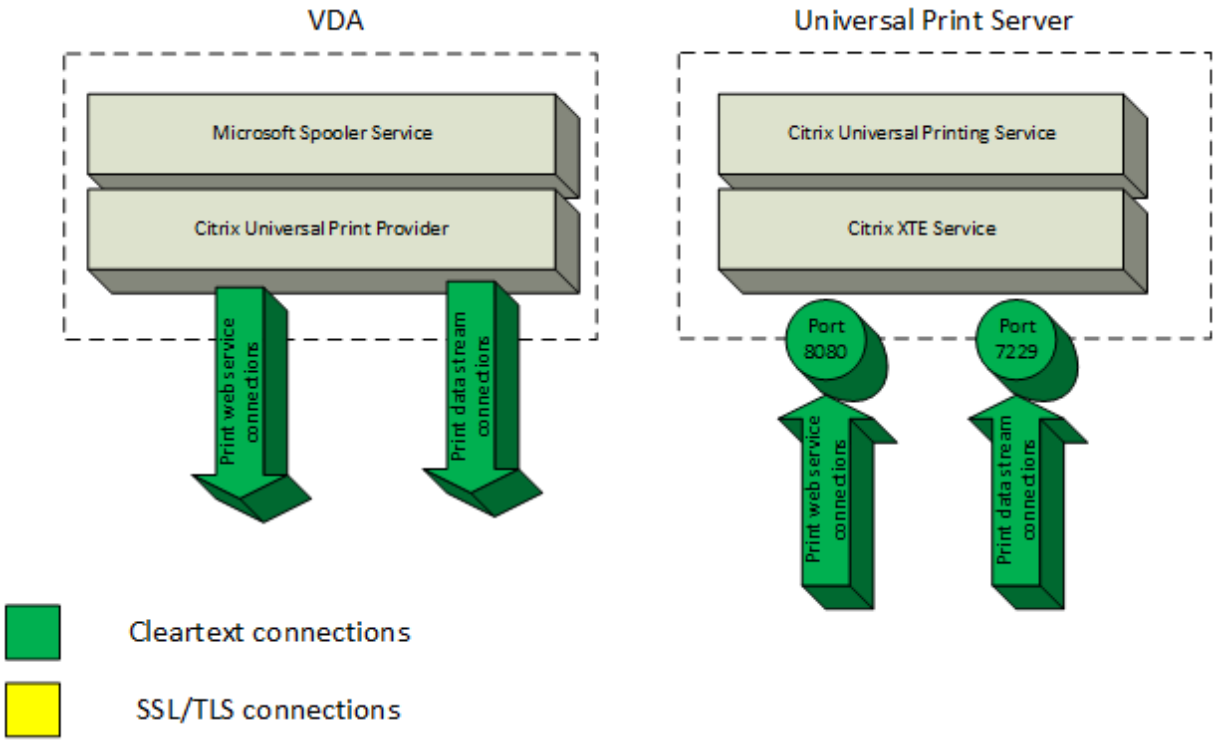
#### Connexions en texte clair (cleartext)

Les connexions suivantes, relatives à l'impression, proviennent du VDA et se connectent aux ports du serveur d'impression universelle. Ces connexions sont effectuées uniquement lorsque le paramètre de stratégie **SSL activé** est défini sur **Désactivé** (valeur par défaut).

- Connexions de service Web d'impression en texte clair (port TCP 8080)
- Connexions de flux de données d'impression en texte clair (CGP) (port TCP 7229)

L'article de support Microsoft Vue d'ensemble des services et exigences de ports réseau pour Windows décrit les ports utilisés par le service de spouleur d'impression Microsoft Windows. Les paramètres SSL/TLS de ce document ne s'appliquent pas aux connexions NetBIOS et RPC effectuées par le Print Spooler Service de Windows. Le VDA utilise le fournisseur d'impression réseau Windows (win32spl.dll) comme solution de secours si le paramètre de stratégie **Activer le serveur d'impression universelle** est défini sur **Activé avec retour à l'impression distante native de Windows**.

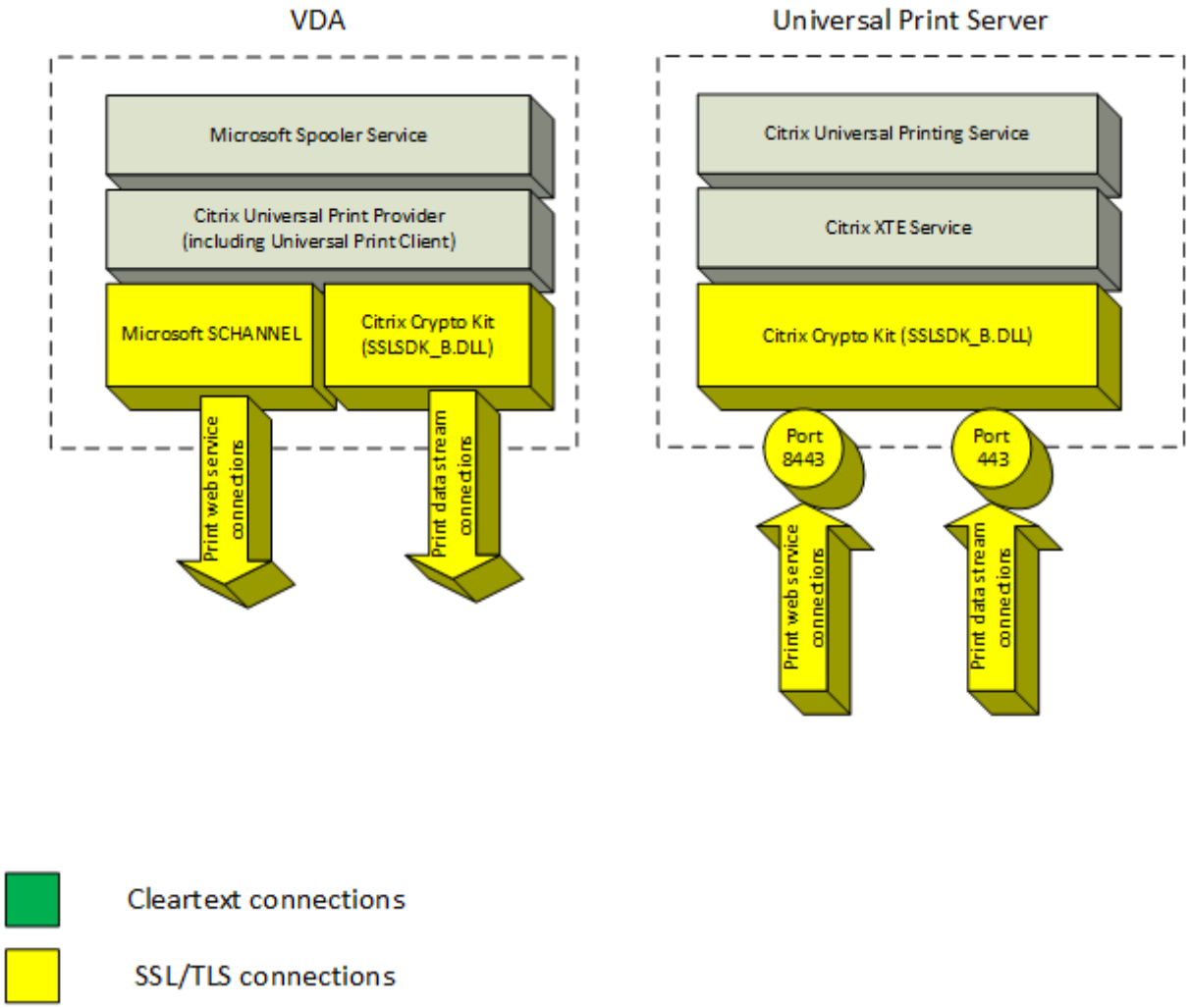



**Connexions cryptées**

Ces connexions SSL/TLS, relatives à l'impression, proviennent du VDA et se connectent aux ports du serveur d'impression universelle. Ces connexions sont effectuées uniquement lorsque le paramètre de stratégie **SSL activé** est défini sur **Activé**.

- Connexions du service Web d'impression cryptées (port TCP 8443)
- Connexions du flux de données d'impression cryptées (CGP) (port TCP 443)




**Configuration du client SSL/TLS**

Le VDA fonctionne en tant que client SSL/TLS.

Utilisez la stratégie de groupe Microsoft et le Registre pour configurer Microsoft SCHANNEL SSP pour les connexions de service Web d'impression cryptées (port TCP 8443). L'article de support Microsoft Paramètres de Registre TLS décrit les paramètres de Registre de Microsoft SCHANNEL SSP.

À l'aide de l'éditeur de stratégie de groupe du VDA, cliquez sur **Configuration ordinateur > Modèles d'administration > Réseau > Paramètres de configuration SSL > Ordre de la suite de chiffrement SSL**. Sélectionnez l'ordre suivant avec TLS 1.3 :

TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256

Sélectionnez l'ordre suivant avec TLS 1.2 :

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256

> **Remarque :**
>
> Lorsque ce paramètre de stratégie de groupe est configuré, le VDA sélectionne une suite de chiffrement pour les connexions de service Web d'impression chiffrées (port par défaut : 8443) uniquement si les connexions apparaissent dans les deux listes de suites de chiffrement SSL :
>
> - Liste des suites de chiffrement SSL de stratégie de groupe
> - Liste correspondant au paramètre de stratégie Suite de chiffrement SSL (COM, GOV ou ALL) sélectionné
>
> Cette configuration de stratégie de groupe affecte également d'autres applications et services TLS sur le VDA. Si vos applications requièrent des suites de chiffrement spécifiques, vous devez les ajouter à la liste des suites de chiffrement de la stratégie de groupe.
>
> **Important :**
>
> Les modifications de stratégie de groupe pour la configuration TLS ne prennent effet qu'après le redémarrage du système d'exploitation.
>
> Utilisez une stratégie Citrix pour configurer les paramètres SSL/TLS pour les connexions CGP (port TCP 443).

#### Configuration du serveur SSL/TLS

Le serveur d'impression universelle fonctionne en tant que serveur SSL/TLS.

Utilisez le script PowerShell `Enable-UpsSsl.ps1` pour configurer les paramètres SSL/TLS.

#### Installer le certificat du serveur TLS sur le serveur d'impression universelle

Pour HTTPS, le service d'impression universelle prend en charge les fonctionnalités TLS par le biais de certificats de serveur. Les certificats client ne sont pas utilisés. Utilisez les services de certificats Microsoft Active Directory ou une autre autorité de certification pour demander un certificat pour le serveur d'impression universelle.

Prenez note des considérations suivantes lors de l'inscription ou de la demande d'un certificat à l'aide des services de certificats Microsoft Active Directory :

1. Placez le certificat dans le magasin de certificats **personnel** de l'ordinateur local.
2. Définissez l'attribut **Nom commun** du nom unique de l'objet (DN) du certificat sur le nom de domaine complet (FQDN) du serveur d'impression universelle. Spécifiez cette information dans le modèle de certificat.
3. Définissez le fournisseur de services cryptographiques (CSP) utilisé pour générer la demande de certificat et la clé privée sur **Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**. Spécifiez cette information dans le modèle de certificat.
4. Définissez la taille de la clé sur au moins 2048 bits. Spécifiez cette information dans le modèle de certificat.

### Configuration de SSL sur le serveur d'impression universelle

Le service XTE sur le serveur d'impression universelle écoute les connexions entrantes. Il fonctionne comme un serveur SSL lorsque SSL est activé. Les connexions entrantes sont de deux types : les connexions de service Web d'impression, qui contiennent les commandes d'impression, et les connexions de flux de données d'impression, qui contiennent les travaux d'impression. SSL peut être activé sur ces connexions. SSL protège la confidentialité et l'intégrité de ces connexions. Par défaut, SSL est désactivé.

Le script PowerShell utilisé pour configurer SSL se trouve sur le support d'installation et porte le nom de fichier suivant : `\Support\Tools\SslSupport\Enable-UpsSsl.ps1`.

### Configuration des numéros de port d'écoute sur le serveur d'impression universelle

Les ports par défaut pour le service XTE sont :

- Port TCP de service Web d'impression en texte clair (HTTP) : 8080
- Port TCP de flux de données d'impression en texte clair (CGP) : 7229
- Port TCP de service Web d'impression cryptée (HTTPS) : 8443
- Port TCP de flux de données d'impression crypté (CGP) : 443

Pour modifier les ports utilisés par le service XTE sur le serveur d'impression universelle, exécutez les commandes suivantes dans PowerShell en tant qu'administrateur (voir la section suivante pour obtenir des notes sur l'utilisation du script PowerShell Enable-UpsSsl.ps1) :

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` ou `Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

### Paramètres TLS sur le serveur d'impression universelle

Si vous disposez de plusieurs serveurs d'impression universelle dans une configuration à charge équilibrée, assurez-vous que les paramètres **TLS** sont configurés de manière cohérente sur tous les serveurs d'impression universelle.

Lorsque vous configurez le protocole TLS sur le serveur d'impression universelle, les autorisations sur le certificat TLS installé sont modifiées, offrant au service d'impression universelle un accès en lecture à la clé privée du certificat, et fournissant au service d'impression universelle les informations suivantes :

- Quel certificat utiliser dans le magasin de certificat à utiliser pour TLS.
- Quels numéros de port TCP utiliser pour les connexions TLS.

Le Pare-feu Windows (s'il est activé) doit être configuré pour autoriser les connexions entrantes sur ces ports TCP. Cette configuration est effectuée pour vous si vous utilisez le script PowerShell Enable-UpsSsl.ps1.

- Versions du protocole TLS à autoriser.

Le serveur d'impression universelle prend en charge les versions 1.3 et 1.2 du protocole TLS. Spécifiez la version minimale autorisée.

La version du protocole TLS par défaut est 1.2.

> **Remarque :**
>
> Les protocoles TLS 1.1 et 1.0 ne sont plus pris en charge depuis la version 2311 de Citrix Virtual Apps and Desktops.

- Suites de chiffrement TLS à autoriser.

Une suite de chiffrement sélectionne les algorithmes cryptographiques utilisés pour une connexion. Le serveur d'impression universelle et les VDA peuvent prendre en charge plusieurs ensembles de suites de chiffrement. Lorsqu'un VDA se connecte et envoie une liste des suites de chiffrement TLS prises en charge, le serveur d'impression universelle fait correspondre une des suites de chiffrement du client avec l'une de suites de chiffrement de sa liste configurée et accepte la connexion. S'il n'existe aucune correspondance de suite de chiffrement, le serveur d'impression universelle rejette la connexion.

Le serveur d'impression universel prend en charge les ensembles suivants de suites de chiffrement nommés GOV (gouvernement), COM (commercial) et ALL (tous) pour les modes de kit de chiffrement natifs OPEN, FIPS et SP800-52. Les suites de chiffrement acceptables dépendent aussi du paramètre de stratégie **Mode FIPS SSL** et du mode FIPS Windows. Consultez cet article de support Microsoft pour plus d'informations sur le mode FIPS Windows.

| Suite de chiffrement (par ordre de priorité décroissant) | OPEN ALL | OPEN COM | OPEN GOV | FIPS ALL | FIPS COM | FIPS GOV | SP800-52 ALL | SP800-52 COM | SP800-52 GOV |
|---|---|---|---|---|---|---|---|---|---|
| TLS_ECDHE_RSA_AES256_GCM_SHA384 | X | | X | X | | X | X | | X |
| TLS_ECDHE_RSA_AES256_CBC_SHA384 | X | | X | X | | X | X | | X |
| TLS_ECDHE_RSA_AES256_CBC_SHA | X | X | | X | X | | X | X | |

#### Configurer TLS sur un serveur d'impression universelle à l'aide du script PowerShell

Installez le certificat TLS dans la zone **Ordinateur local > Personnel > Certificats** du magasin de certificats. Si plusieurs certificats résident à cet emplacement, fournissez l'empreinte numérique du certificat au script PowerShell `Enable-UpsSsl.ps1`.

> **Remarque :**
>
> Le script PowerShell trouve le certificat correct en se basant sur le nom de domaine complet du serveur d'impression universelle. Vous n'avez pas besoin de fournir l'empreinte du certificat si un seul certificat est présent pour le nom de domaine complet du serveur d'impression universelle.

Le script `Enable-UpsSsl.ps1` active ou désactive les connexions TLS depuis le VDA vers le serveur d'impression universelle. Ce script est disponible dans le dossier **Support > Tools > SslSupport** sur le support d'installation.

Lorsque vous activez le protocole TLS, le script désactive toutes les règles de pare-feu Windows existantes pour les ports TCP du serveur d'impression universelle. Ensuite, il ajoute des règles qui permettent au service XTE d'accepter les connexions entrantes uniquement sur les ports TLS TCP et UDP. Cela désactive également les règles du Pare-feu Windows pour :

- Connexions de service Web d'impression en texte clair (par défaut : 8080)
- Connexions de flux de données d'impression en texte clair (CGP) (par défaut : 7229)

Par conséquent, le VDA ne peut effectuer ces connexions que lors de l'utilisation de TLS.

> **Remarque :**
>
> L'activation de TLS n'affecte pas les connexions RPC/SMB du Spouleur d'impression Windows depuis le VDA vers le serveur d'impression universelle.
>
> **Important :**
>
> Spécifiez **Activer** ou **Désactiver** comme premier paramètre. Le paramètre CertificateThumbPrint est facultatif si un seul certificat dans le magasin de certificats Ordinateur local possède le nom de domaine complet du serveur d'impression universelle. Les autres paramètres sont facultatifs.

### Syntaxe

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-FIPSMode <Boolean>] [-ComplianceMode <mode>]
Enable-UpsSSL.ps1 -Disable [-HTTPPort <portnum>] [-CGPPort <portnum>]
```

| Paramètre | Description |
|---|---|
| Activer | Active SSL/TLS sur le serveur XTE. Soit ce paramètre ou le paramètre Disable est requis. |
| Désactiver | Désactive SSL/TLS sur le serveur XTE. Soit ce paramètre ou le paramètre Enable est requis. |
| CertificateThumbprint "<thumbprint>" | Empreinte numérique du certificat TLS dans le magasin de certificats personnel de l'ordinateur local, entourée de guillemets. Le script utilise l'empreinte numérique spécifiée pour sélectionner le certificat que vous voulez utiliser. |
| HTTPPort <port> | Port de service Web d'impression en texte clair (HTTP/SOAP). Valeur par défaut : 8080 |
| CGPport<port> | Port de flux de données d'impression en texte clair (CGP). Valeur par défaut : 7229. |
| HTTPSPort <port> | Port de service Web d'impression cryptée (HTTPS/SOAP). Valeur par défaut : 8443 |
| CGPSSLPort <port> | Port de flux de données d'impression cryptée (CGP). Valeur par défaut : 443 |
| SSLMinVersion "<version>" | Version minimale du protocole TLS, entourés de guillemets. Valeurs valides : « TLS_1.2 » et « TLS_1.3 ». Valeur par défaut : TLS_1.2. |

| Paramètre | Description |
| --- | --- |
| SSLCipherSuite "<name>" | Nom du package de la suite de chiffrement TLS, entre guillemets. Les valeurs valides sont : « GOV », « COM » et « ALL » (par défaut). |
| FIPSMode <Boolean> | Active ou désactive le mode FIPS 140 dans le serveur XTE. Les valeurs valides sont : $true pour activer le mode FIPS 140, $false pour désactiver le mode FIPS 140. |

#### Exemples

Le script suivant active TLS. L'empreinte numérique (représentée en tant que « 12345678987654321 » dans cet exemple) est utilisée pour sélectionner le certificat à utiliser.

```
Enable-UpsSsl.ps1 –Enable -CertificateThumbprint "12345678987654321"
```

Le script suivant désactive TLS.

```
Enable-UpsSsl.ps1 –Disable
```

### Configuration du mode FIPS

L'activation du mode US FIPS (Federal Information Processing Standards) garantit que seule la cryptographie conforme à la norme FIPS 140 est utilisée pour les connexions chiffrées du serveur d'impression universelle.

Configurez le mode FIPS sur le serveur avant de configurer le mode FIPS sur le client.

Consultez le site de documentation de Microsoft pour activer ou désactiver le mode FIPS Windows.

#### Activation du mode FIPS sur le client

Sur le Delivery Controller, exécutez Web Studio et définissez le paramètre de stratégie Citrix **Mode FIPS SSL** sur **Activé**. Activez la stratégie Citrix.

Procédez comme suit sur chaque VDA :

1. Activez le mode FIPS Windows.
2. Redémarrez le VDA.

#### Activation du mode FIPS sur le serveur

Procédez comme suit sur chaque serveur d'impression universelle :

1. Activez le mode FIPS Windows.
2. Exécutez cette commande PowerShell en tant qu'administrateur : `stop-service CitrixXTEServer, UpSvc`
3. Exécutez le script `Enable-UpsSsl.ps1` avec les paramètres `-Enable -FIPSMode $true`.
4. Redémarrez le serveur d'impression universelle.

#### Désactivation du mode FIPS sur le client

Dans Web Studio, définissez le paramètre de stratégie Citrix **Mode FIPS SSL** sur **Désactivé**. Activez la stratégie Citrix. Vous pouvez également supprimer le paramètre de stratégie Citrix **Mode FIPS SSL**.

Procédez comme suit sur chaque VDA :

1. Désactivez le mode FIPS Windows.
2. Redémarrez le VDA.

#### Désactivation du mode FIPS sur le serveur

Procédez comme suit sur chaque serveur d'impression universelle :

1. Désactivez le mode FIPS Windows.
2. Exécutez cette commande PowerShell en tant qu'administrateur : `stop-service CitrixXTEServer, UpSvc`
3. Exécutez le script `Enable-UpsSsl.ps1` avec les paramètres `-Enable -FIPSMode $false`.
4. Redémarrez le serveur d'impression universelle.

> **Remarque :**
>
> Le mode FIPS n'est pas pris en charge lorsque la version du protocole SSL est définie sur TLS 1.3.

### Configuration de la version du protocole SSL/TLS

La version du protocole SSL/TLS par défaut est TLS 1.2. TLS 1.2 et TLS 1.3 sont les versions de protocole SSL/TLS recommandées pour une utilisation en production. Pour le dépannage, il peut être nécessaire de modifier temporairement la version du protocole SSL/TLS dans un environnement hors production.

SSL 2.0 et SSL 3.0 ne sont pas pris en charge sur le serveur d'impression universelle.

#### Configuration de la version du protocole SSL/TLS sur le serveur

Procédez comme suit sur chaque serveur d'impression universelle :

1. Exécutez cette commande PowerShell en tant qu'administrateur : `stop-service CitrixXTEServer, UpSvc`
2. Exécutez le script `Enable-UpsSsl.ps1` avec les paramètres de version `-Enable -SSLMinVersion`. N'oubliez pas de revenir à TLS 1.2 ou TLS 1.3 lorsque vous avez terminé le test.
3. Redémarrez le serveur d'impression universelle.

#### Configuration de la version du protocole SSL/TLS sur le client

Procédez comme suit sur chaque VDA :

1. Sur le Delivery Controller, définissez le paramètre de stratégie **Version du protocole SSL** sur la version de protocole souhaitée et activez la stratégie.
2. L'article de support Microsoft Paramètres de Registre TLS décrit les paramètres de Registre de Microsoft SCHANNEL SSP. Activez **TLS 1.2 ou TLS 1.3** côté client à l'aide des paramètres du registre.

   > **Important :**
   >
   > N'oubliez pas de restaurer les valeurs d'origine des paramètres du Registre lorsque vous avez terminé le test.

3. Redémarrez le VDA.

### Dépannage

En cas d'erreur de connexion, vérifiez le fichier journal C:\Program Files (x86)\Citrix\XTE\logs\error.log sur le serveur d'impression universelle.

Le message d'erreur **SSL handshake from client failed** figure dans ce fichier journal si le handshake SSL/TLS échoue. De tels échecs peuvent se produire si les versions du protocole SSL/TLS sur le VDA et sur le serveur d'impression universelle ne correspondent pas.

Utilisez le nom de domaine complet du serveur d'impression universelle dans les paramètres de stratégie suivants, qui contiennent les noms d'hôte du serveur d'impression universelle :

- Imprimantes de session

- Attributions d'imprimantes
- Serveurs d'impression universelle d'équilibrage de la charge

Vérifiez que l'horloge système (date, heure et fuseau horaire) est correcte sur les serveurs d'impression universelle et les VDA.

## Liste verte des canaux virtuels

June 27, 2024

La liste verte des canaux virtuels est une fonctionnalité qui vous permet de contrôler les canaux virtuels non-Citrix autorisés dans votre environnement. Par défaut, la fonctionnalité de liste verte des canaux virtuels est activée. Par conséquent, seuls les canaux virtuels Citrix sont autorisés à s'ouvrir dans les sessions Citrix Virtual Apps and Desktops. S'il est nécessaire d'utiliser des canaux virtuels personnalisés, qu'ils soient locaux ou provenant d'un tiers, ils doivent être explicitement ajoutés à la liste d'autorisation.

### Configuration

La liste verte des canaux virtuels est activée par défaut. Vous pouvez configurer cette fonctionnalité à l'aide des paramètres suivants de la stratégie Citrix :

- **Liste verte des canaux virtuels** : pour activer ou désactiver la fonctionnalité et ajouter des canaux virtuels à la liste.
- **Limitation de journalisation de la liste verte des canaux virtuels** : définit la période de limitation pour la journalisation des événements de la liste verte des canaux virtuels.
- **Journalisation de la liste verte des canaux virtuels** : définit le niveau de journalisation de la liste verte des canaux virtuels.

### Ajout de canaux virtuels à la liste d'autorisation

Pour ajouter une chaîne virtuelle à la liste verte, vous avez besoin des informations suivantes :

1. Le nom du canal virtuel tel que défini dans le code, qui peut contenir jusqu'à sept caractères. Par exemple, `CTXCVC1`.
2. Les chemins d'accès aux processus qui ouvrent le canal virtuel sur la machine VDA. Par exemple, `C:\Program Files\Application\run.exe`.

Une fois que vous avez les informations requises, vous devez ajouter le canal virtuel à la liste d'autorisation à l'aide du paramètre de stratégie Liste d'autorisation des canaux virtuels. Pour ajouter un canal virtuel à la liste, entrez le nom du canal virtuel suivi d'une virgule, puis le chemin d'accès au processus qui accède au canal virtuel. S'il existe plusieurs processus, vous pouvez les ajouter en séparant chaque processus par des virgules.

#### Dans le cas de processus uniques

En utilisant les exemples précédents, ajoutez les éléments suivants à la liste :

```
CTXCVC1,C:\Program Files\Application\run.exe
```

#### Dans le cas de plusieurs processus

S'il y a plusieurs processus, ajoutez l'entrée suivante à la liste :

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

#### Caractères génériques

L'utilisation de caractères génériques (*) est prise en charge. Vous pouvez utiliser des caractères génériques lorsque les noms des répertoires ou des exécutables changent en fonction de la version de l'application ou si le composant tiers est installé dans les profils des utilisateurs.

Vous pouvez utiliser des caractères génériques dans les scénarios suivants :

- Pour remplacer le nom complet du répertoire.
  Par exemple : `C:\Program Files\Application\*\run1.exe`
- Pour remplacer une partie du nom du répertoire.
  Par exemple : `C:\Program Files\Application\v*\run1.exe`
- Pour remplacer le nom de l'exécutable.
  Par exemple : `C:\Program Files\Application\v1.2\*.exe`
- Pour remplacer une partie du nom de l'exécutable.
  Par exemple : `C:\Program Files\Application\v1.2\run*.exe`

Les restrictions suivantes s'appliquent :

- Le caractère générique ne peut être utilisé que pour remplacer un seul répertoire. Par exemple, si l'exécutable se trouve dans `C:\Program Files\Application\v1.2\run1.exe`
  - Autorisé : `C:\Program Files\Application\*\run1.exe`
  - Non autorisée : `C:\Program Files\*\run1.exe`

- Les entrées doivent contenir l'extension de fichier.
  - Autorisé : `C:\Program Files\Application\v1.2\*.exe`
  - Non autorisée : `C:\Program Files\Application\v1.2\*`
- Tous les chemins doivent être locaux.

> **Remarque :**
>
> - Les chemins réseau ne sont pas autorisés.
> - La prise en charge des caractères génériques est disponible à partir de Citrix Virtual Apps and Desktops 2206.
> - La prise en charge des caractères génériques est disponible dans Citrix Virtual Apps and Desktops 2203 LTSR à partir de la version CU2.

#### Utilisation des variables d'environnement système

Vous pouvez utiliser des variables d'environnement système pour simplifier la définition des processus approuvés dans la liste verte. Vous pouvez utiliser toutes les variables prêtes à l'emploi, telles que `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` et `%systemroot%`.

Vous pouvez également utiliser des variables d'environnement personnalisées tant qu'elles sont définies au niveau du système.

Les exemples suivants présentent les variables d'environnement prêtes à l'emploi :

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application\*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

L'exemple suivant décrit une variable d'environnement système personnalisée :

- Nom de variable personnalisé : `app`
- Valeur de variable personnalisée : `%programfiles%\Application\`
- Entrée dans la liste d'autorisation : `CTXCVC1,%app%\run.exe`

> **Remarque :**
>
> Les variables d'environnement utilisateur ne sont pas prises en charge.
>
> La prise en charge des variables d'environnement est disponible à partir de la version 2209 de Citrix Virtual Apps and Desktops.

### Obtenir des noms et des processus de canaux virtuels

Le moyen le plus simple d'obtenir le nom du canal virtuel et le processus qui l'ouvre sur la machine VDA est de demander ces informations au développeur ou au fournisseur tiers qui a fourni le canal virtuel.

Vous pouvez également obtenir ces informations en appliquant les journaux de la fonctionnalité et en procédant comme suit :

1. Une fois que les composants client et serveur du canal virtuel personnalisé sont en place, lancez une application virtuelle ou un bureau virtuel.
2. Dans le journal des événements système de la machine VDA, recherchez le nom du canal virtuel personnalisé et le processus qui a essayé de l'ouvrir. Pour plus d'informations sur les événements disponibles, consultez la section Journaux d'événements.
3. Déconnectez-vous de la session.
4. Ajoutez une entrée dans les paramètres de la stratégie de liste verte des canaux virtuels pour le canal virtuel et le processus identifiés.
5. Redémarrez la machine.
6. Une fois le VDA enregistré, exécutez l'application virtuelle ou le bureau virtuel pour vérifier que les canaux virtuels personnalisés s'ouvrent correctement.

### Considérations relatives aux canaux virtuels Citrix

Tous les canaux virtuels Citrix intégrés sont approuvés et peuvent s'ouvrir sans autre configuration. Toutefois, les deux fonctionnalités suivantes nécessitent des entrées explicites dans la liste verte en raison de dépendances externes :

- Redirection multimédia
- Pack d'optimisation HDX RealTime pour Skype Entreprise

#### Redirection multimédia

Si vous utilisez un lecteur multimédia autre que Windows Media Player comme lecteur multimédia de votre système, vous devez l'ajouter à la liste verte en tant que processus approuvé. Les informations suivantes sont requises pour l'entrée dans la liste verte :

- Nom du canal virtuel : `CTXMM`
- Processus : chemin d'accès au lecteur multimédia utilisé sur votre machine VDA. Par exemple, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Entrée dans la liste d'autorisation : `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

#### Pack d'optimisation HDX RealTime pour Skype Entreprise

Les informations suivantes sont requises pour l'entrée dans la liste verte :

- Nom du canal virtuel : `CTXRMEP`
- Processus : chemin d'accès à l'exécutable Skype Entreprise sur votre machine VDA, qui peut varier en fonction de la version de Skype Entreprise ou si vous avez utilisé un chemin d'installation personnalisé. Par exemple, `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.
- Entrée dans la liste d'autorisation : `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

## Communication WebSocket entre VDA et Delivery Controller

June 27, 2024

Cet article explique comment configurer une connexion WebSocket pour la communication entre les VDA et les Delivery Controller.

### Vue d'ensemble

Le protocole WebSocket fonctionne via Citrix Brokering Protocol et facilite une communication stable entre les Delivery Controller et les VDA.
L'utilisation du protocole WebSocket pour la communication offre les avantages suivants :

- Requiert uniquement le port TLS 443 pour la communication entre le VDA et le Delivery Controller.
- Fournit des canaux de communication fluides et fiables entre les VDA et les Delivery Controller.

### Fonctionnement

La section suivante décrit le workflow pour la connexion WebSocket entre un Delivery Controller et un VDA :

1. Les administrateurs de Citrix Virtual Apps and Desktops lancent le processus en provisionnant des VDA à l'aide de Machine Creation Service (MCS).
2. Au cours du processus de provisioning MCS, MCS génère des paires de clés publique-privée pour chaque VDA et enregistre les clés publiques auprès du Trust Service FMA sur le Delivery Controller. MCS enregistre la paire de clés publique-privée sous forme de fichier sous le disque d'identité sur les VDA.

3. Lorsque la machine VDA démarre, l'agent MCS installé sur celle-ci lit la paire de clés depuis le disque d'identité et écrit ces informations dans l'emplacement de registre du VDA.
4. L'agent broker installé sur le VDA lit les paires de clés du registre et génère une demande WebSocket compatible SSL auprès du Delivery Controller avec la clé de service signée par la clé privée.
5. Le Delivery Controller vérifie l'en-tête d'autorisation de clé de service signé avec la clé publique du Trust Service FMA.
6. Une fois la vérification terminée, le système établit la connexion WebSocket entre le VDA et le Delivery Controller.

## Prise en charge de WebSocket pour les VDA joints à AD

### Avant de commencer

1. Configurez votre site. Pour plus d'informations, consultez la section Créer un site.
2. Installez des certificats TLS sur les Delivery Controller. Pour plus d'informations, consultez Installer les certificats de serveur TLS sur des Controller.
3. Installez l'autorité de certification racine et l'autorité de certification intermédiaire sur le VDA pour approuver le Delivery Controller.

### Procédure

Pour configurer une connexion WebSocket, procédez comme suit :

1. Activez la connexion WebSocket sur le Delivery Controller. Exécutez la commande suivante sur chaque Delivery Controller présent sur votre site :

   ```
   New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy
   "-Name "WebSocket_Enabled"-PropertyType "DWord"-Value 1 -Force
   ```

   > **Remarque :**
   >
   > Assurez-vous de redémarrer les Delivery Controller après avoir activé le WebSocket.

2. Créez un catalogue de machines pour les VDA joints à AD avec le provisioning MCS. Pour de plus amples informations, consultez l'article Créer un catalogue de machines.
3. Créez un groupe de mise à disposition et ajoutez-y votre VDA. Pour plus d'informations, consultez la section Créer des groupes de mise à disposition.
4. Activez la connexion WebSocket sur le VDA. Exécutez la commande suivante sur le VDA :

```
New-ItemProperty "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
    Services\CitrixBrokerAgent\WebSocket" -Name "Enabled" -
    PropertyType "DWord" -Value 1 -Force
<!--NeedCopy-->
```

- Pour vérifier si le VDA est connecté au serveur via WebSocket, vérifiez la valeur de la clé de registre suivante.

  Clé :

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
      CitrixBrokerAgent\WebSocket
  <!--NeedCopy-->
  ```

  Nom : Connecté

  Type : REG_DWORD

  Valeur : 1 ou 0

  1 : VDA connecté au serveur à l'aide de WebSocket.

  0 : le VDA ne parvient pas à communiquer avec le serveur via WebSocket ou WebSocket n'est pas activé.

- Pour vérifier si WebSocket est activé, vérifiez la valeur de la clé de registre suivante. La valeur de `Enabled` doit être 1.

  Clé :

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
      CitrixBrokerAgent\WebSocket
  <!--NeedCopy-->
  ```

  Nom : Enabled

  Type : REG_DWORD

  Valeur : 1

## Connectivité HDX

June 27, 2024

Citrix HDX représente un large ensemble de technologies qui offrent une expérience haute définition aux utilisateurs d'applications et de bureaux centralisés, sur tout périphérique et sur tout réseau.

HDX est conçu autour de trois principes techniques :

- Redirection intelligente
- Compression adaptative
- Déduplication des données

Appliqués selon différentes combinaisons, ils optimisent l'expérience du service informatique et des utilisateurs, réduisent la consommation de bande passante et augmentent la densité utilisateur par serveur d'hébergement.

Dans le cadre de l'offre HDX, vous pouvez vous connecter via un protocole de transport propriétaire unique, utiliser le maximum d'unités de transmission lors de l'établissement de sessions et optimiser la connectivité avec Citrix SD-WAN.

## Transport adaptatif

June 27, 2024

Le transport adaptatif est un mécanisme de Citrix Virtual Apps and Desktops qui permet d'établir des connexions pour les sessions HDX à l'aide d'un protocole de transport préféré tout en fournissant une solution de retour au protocole TCP si la connectivité avec le protocole préféré n'est pas disponible.

Les protocoles de transport suivants sont pris en charge :

- Enlightened Data Transport (EDT)
- Transmission Control Protocol (TCP)

### Configuration

Le transport adaptatif est activé par défaut. Vous pouvez configurer le transport adaptatif pour qu'il fonctionne dans les modes suivants :

- **Préféré** : (par défaut) le client tente de se connecter avec le protocole préféré et revient au protocole TCP si la connectivité avec le protocole préféré n'est pas disponible.
- **Mode de diagnostic** : le client tente de se connecter uniquement à l'aide du protocole préféré. Le retour vers TCP est désactivé.
- **Désactivé** : le client tente uniquement de se connecter via le protocole TCP.

### Fonctionnement

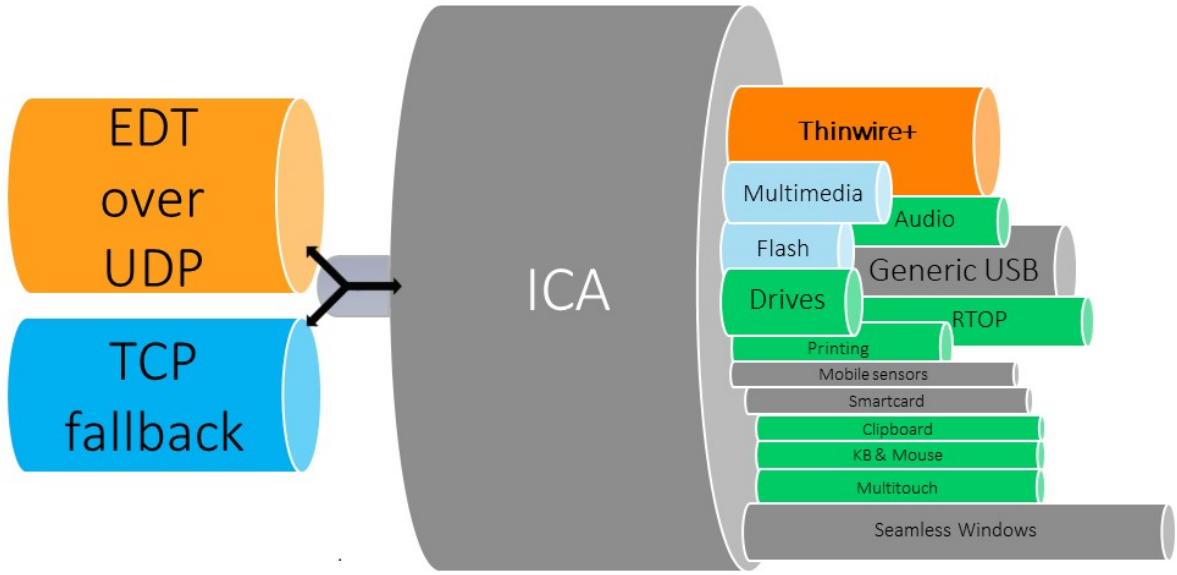
Lorsque l'option **Transport adaptatif** est définie sur `Preferred`, le client tente de se connecter à la session avec le protocole préféré et le protocole TCP en parallèle. Cela permet d'optimiser le temps de

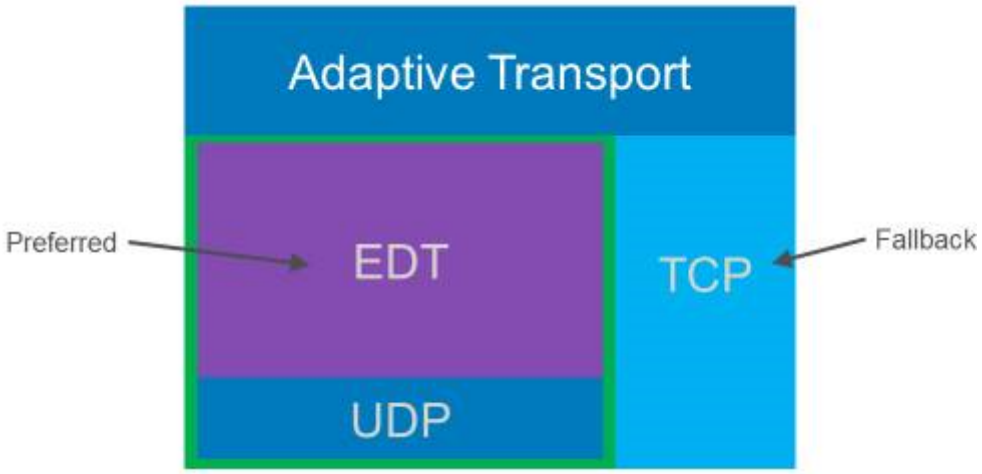
 

connexion s'il n'est pas possible de se connecter avec le protocole préféré et que le client doit revenir à l'utilisation du protocole TCP. Si la connexion est établie à l'aide du protocole TCP, le client tente de se connecter avec le protocole préféré en arrière-plan toutes les cinq minutes.

Lorsque l'option **Transport adaptatif** est définie sur `Diagnostic mode`, le client se connecte à la session uniquement avec le protocole préféré. Si le client ne parvient pas à établir une connexion à l'aide du protocole préféré, il ne revient pas au protocole TCP et la connexion échoue.

Lorsque l'option **Transport adaptatif** est définie sur `Off`, le **transport adaptatif** est désactivé et le client se connecte à la session via TCP uniquement.




### Configuration système requise

Les exigences suivantes sont requises pour utiliser le transport adaptatif et EDT :

- Plan de contrôle
  - Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops : version actuellement prise en charge
- Virtual Delivery Agent
  - Windows : version actuellement prise en charge (version 2402 ou ultérieure recommandée)
  - Linux : version actuellement prise en charge (version 2402 ou ultérieure recommandée)
- Application Citrix Workspace
  - Windows : version actuellement prise en charge (version 2402 ou ultérieure recommandée)
  - Linux : version actuellement prise en charge (version 2402 ou ultérieure recommandée)
  - Mac : version actuellement prise en charge (version 2402 ou ultérieure recommandée)
  - iOS : dernière version disponible dans l'App Store Apple
  - Android : dernière version disponible dans Google Play
- Citrix NetScaler Gateway
  - 14.1.12.30 ou version ultérieure (recommandé)
  - 13.1.17.42 ou version ultérieure (13.1-52.19 ou version ultérieure recommandée)

> **Remarque :**
>
> Pour plus d'informations sur Linux VDA, consultez la documentation de Linux Virtual Delivery Agent.

## Configuration réseau requise

Les sections suivantes décrivent la configuration réseau requise pour utiliser EDT avec le transport adaptatif :

### Hôtes de sessions

Si vos hôtes de session disposent d'un pare-feu tel que le pare-feu Windows Defender, vous devez autoriser le trafic entrant suivant pour les connexions internes.

| Description | Source | Protocole | Port |
|---|---|---|---|
| Connexion interne - Fiabilité de session activée | Client | UDP | 2598 |
| Connexion interne - Fiabilité de session désactivée | | | 1494 |
| Connexion interne - HDX Direct ou VDA SSL | | | 443 |

> **Remarque :**
>
> Le programme d'installation du VDA ajoute les règles entrantes appropriées au pare-feu Windows Defender. Si vous utilisez un autre pare-feu, vous devez ajouter les règles ci-dessus.

**Réseau interne**

Le tableau suivant décrit les règles de pare-feu requises pour utiliser EDT sur votre réseau :

| Description | Protocole | Source | Destination | Port de destination |
|---|---|---|---|---|
| Connexion interne directe - Fiabilité de session activée | UDP | Réseau client | Réseau VDA | 2598 |
| Connexion interne directe - Fiabilité de session désactivée | | | | 1494 |
| Connexion interne directe - HDX Direct ou VDA SSL | | | | 443 |
| NetScaler Gateway | | SNIP NetScaler | | 2598 |
| NetScaler Gateway - VDA SSL | | | | 443 |

> **Remarque :**
>
> Si vous utilisez Citrix Gateway Service, vous devez activer **Rendezvous** pour utiliser EDT comme protocole de transport. Consultez la documentation de Rendezvous pour connaître la configuration système et réseau requise.

### Réseau client

Le tableau suivant décrit la configuration requise pour la connectivité des machines clientes :

| Description | Protocole | Source | Destination | Port de destination |
|---|---|---|---|---|
| Connexion interne - Fiabilité de session activée | UDP | IP client | Réseau VDA | 2598 |
| Connexion interne - Fiabilité de session désactivée | | | | 1494 |
| Connexion interne - HDX Direct ou VDA SSL | | | | 443 |
| Connexion externe - NetScaler Gateway | | | Adresse IP publique de NetScaler Gateway | 443 |
| Connexion externe - Citrix Gateway Service | | | Citrix Gateway Service | 443 |

> **Remarque :**
>
> Si vous utilisez Citrix Gateway Service, les clients doivent être en mesure de contacter https://*.*.nssvc.net. Si vous ne pouvez pas autoriser tous les sous-domaines à l'aide de https://*.*.nssvc.net, vous pouvez utiliser https://*.c.nssvc.net et https://*.g.nssvc.net. Pour obtenir davantage d'informations, veuillez consulter l'article CTX270584 du centre de connaissances.

# Enlightened Data Transport

June 27, 2024

Enlightened Data Transport (EDT) est un protocole de transport propriétaire de Citrix basé sur le protocole UDP (User Datagram Protocol). Il offre une expérience utilisateur supérieure sur les connexions longue distance difficiles tout en maintenant la capacité à monter en charge du serveur. EDT améliore le débit de données de tous les canaux virtuels ICA sur des réseaux peu fiables, offrant ainsi une expérience utilisateur plus performante et plus cohérente.

Lorsque le **transport adaptatif** est activé, EDT est le protocole préféré.

## Ce qu'il faut savoir

- La **Fiabilité de session** doit être activée pour utiliser la **découverte MTU** et EDT avec NetScaler Gateway et Citrix Gateway Service.
- La fragmentation des paquets peut entraîner une dégradation des performances, voire l'impossibilité d'ouvrir des sessions dans certains cas. Pour éviter cela, vous devez régler le MTU EDT à une valeur adaptée à vos réseaux. Vous pouvez utiliser la découverte MTU EDT ou la solution manuelle décrite dans l'article How to configure MSS when using EDT on networks with non-standard MTU.
- Pour plus d'informations sur l'activation de l'utilisation de l'EDT avec NetScaler Gateway, consultez Configuration de NetScaler Gateway pour prendre en charge Enlightened Data Transport.

## Découverte MTU EDT

La découverte MTU permet à EDT de déterminer automatiquement l'unité de transmission maximale (MTU) lors de l'établissement d'une session. Cela empêche la fragmentation des paquets EDT, qui pourrait entraîner une dégradation des performances ou l'échec de l'établissement d'une session.

La découverte MTU est activée par défaut. Si vous devez la désactiver, consultez la section Fonctions HDX gérées via le registre pour plus de détails.

> **Remarque :**
>
> - La **Fiabilité de session** doit être activée pour que la découverte MTU fonctionne.
> - La découverte MTU avec ICA Multi-Stream est disponible avec les versions 2209 et ultérieures du VDA.

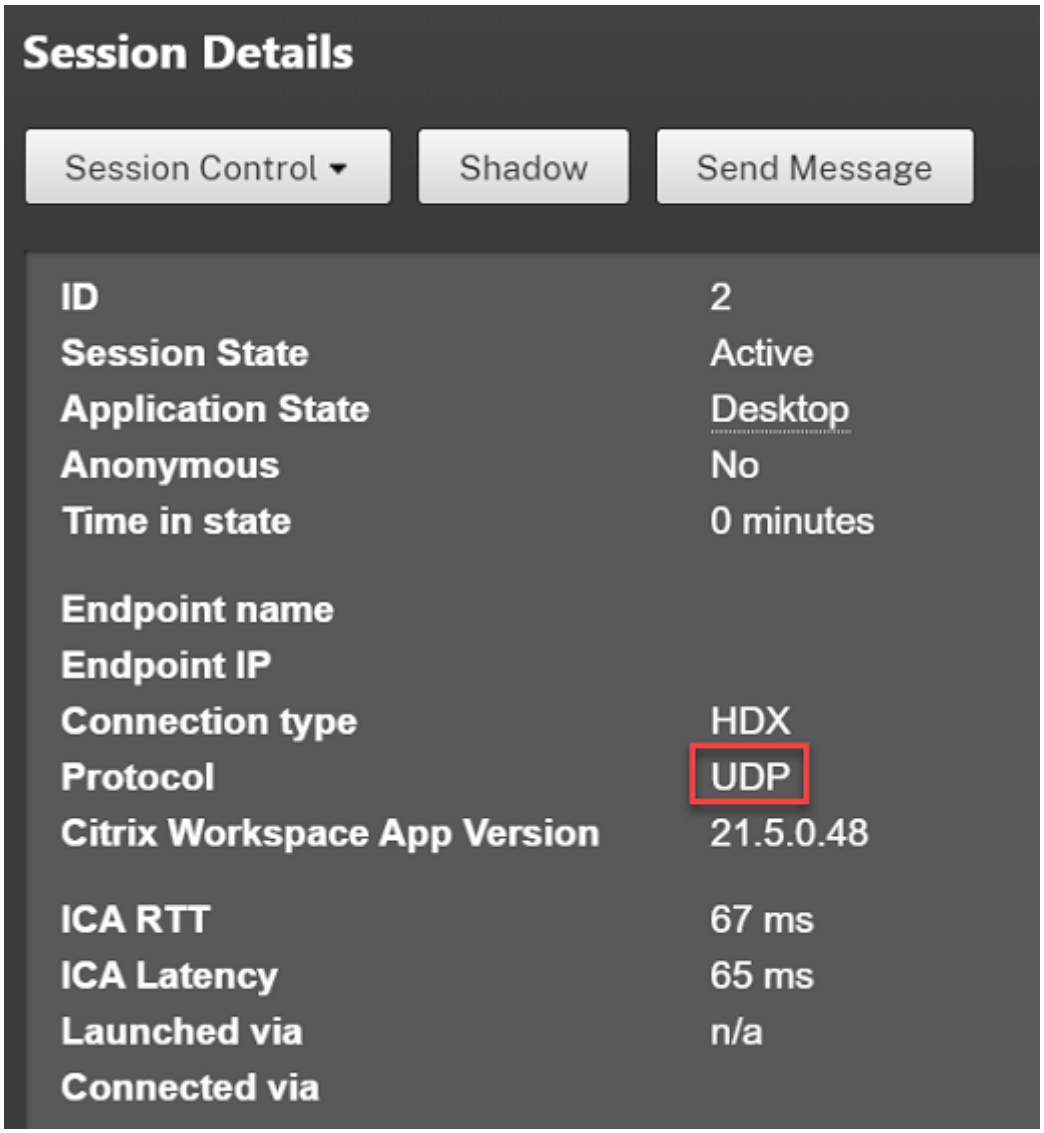
 

## Dépannage

June 27, 2024

Pour confirmer qu'EDT est utilisé comme protocole de transport pour la session, vous pouvez utiliser Director ou l'utilitaire de ligne de commande `CtxSession.exe` sur le VDA.

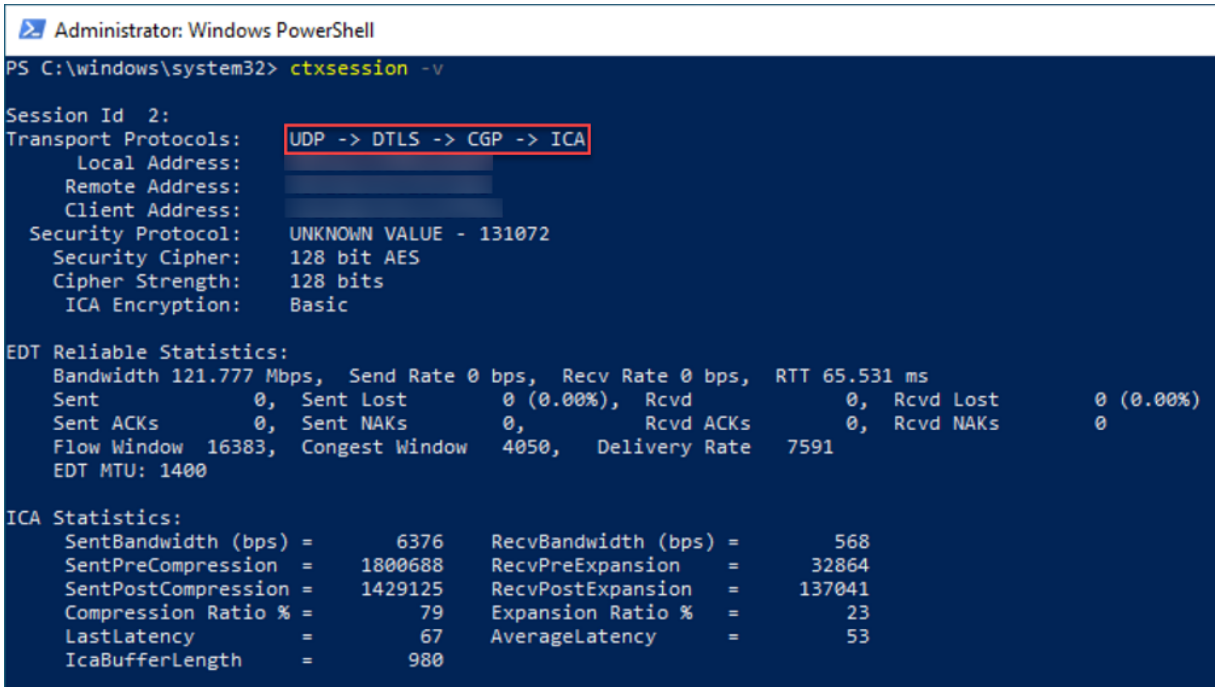
Dans Director, recherchez la session et sélectionnez **Détails**. Si le **Type de connexion** est HDX et que le **Protocole** est UDP, EDT est utilisé comme protocole de transport pour la session.




Pour utiliser l'utilitaire CtxSession.exe, lancez une invite de commandes ou PowerShell au sein de la session et exécutez `ctxsession.exe`. Pour voir des statistiques détaillées, exécutez `ctxsession.exe -v`. Si EDT est en cours d'utilisation, le protocole de transport affiche l'une des caractéristiques suivantes :

- **UDP > ICA** (fiabilité de session désactivée)
- **UDP > CGP > ICA** (fiabilité de session activée)
- **UDP > DTLS > CGP > ICA** (ICA est chiffré de bout en bout par DTLS)




### Lorsque les sessions ne parviennent pas à se connecter via EDT

Pour résoudre les problèmes liés au **transport adaptatif** et à **EDT**, nous vous suggérons ce qui suit :

1. Passez en revue les sections Configuration système requise, Configuration réseau requise, Problèmes connuset Choses à savoir, et assurez-vous que tout est correct.
2. Vérifiez s'il existe des stratégies Citrix dans Studio ou si l'objet de stratégie de groupe écrase le paramètre **HDX Adaptive Transport** souhaité.
3. Vérifiez s'il existe des paramètres sur le client qui écrasent le paramètre HDX Adaptive Transport souhaité. Il peut s'agir d'une préférence de stratégie de groupe, d'un paramètre configuré à l'aide du modèle d'administration de l'application Workspace en option ou d'une configuration manuelle du paramètre **HDXoverUDP** dans le registre ou le fichier de configuration du client.
4. Sur les machines VDA multi-session, assurez-vous que les écouteurs UDP sont actifs. Ouvrez une invite de commandes sur la machine VDA et exécutez `netstat -a -p udp`. Pour plus d'informations, consultez Comment confirmer le protocole HDX Enlightened Data Transport.
5. Vérifiez si les règles de pare-feu appropriées ont été configurées dans les pare-feu réseau et les pare-feu exécutés sur les machines VDA.

6. Lancez une session directe en interne, en contournant NetScaler Gateway ou Citrix Gateway Service, puis vérifiez le protocole utilisé. Si la session utilise EDT, le VDA est prêt à utiliser EDT pour les connexions externes via NetScaler Gateway ou Citrix Gateway Service.
7. Si EDT fonctionne pour les connexions internes directes et non pour les sessions passant par NetScaler Gateway ou Citrix Gateway Service :
   - Assurez-vous que la **Fiabilité de session** est activée.
   - Si vous utilisez NetScaler Gateway, assurez-vous que votre configuration est conforme à la configuration requise décrite dans la section Configurer NetScaler Gateway pour prendre en charge Enlightened Data Transport et HDX Insight.
8. Si vous utilisez Citrix Gateway Service, assurez-vous que Rendezvous est activé et qu'il fonctionne.
9. Vérifiez si les connexions de vos utilisateurs nécessitent une MTU non standard. Les connexions avec une MTU effective en dessous de 1500 octets entraînent la fragmentation des paquets EDT, ce qui peut à son tour affecter les performances ou même entraîner des échecs de lancement de session. Ce problème est fréquent lors de l'utilisation d'un VPN, de certains points d'accès Wi-Fi et de réseaux mobiles, tels que les réseaux 4G et 5G. Assurez-vous que la découverte MTU est activé ou que vous avez défini une MTU personnalisée, comme indiqué dans l'article How to configure MSS when using EDT on networks with non-standing MTU.

### Problèmes connus

- Les chemins réseau asymétriques peuvent entraîner l'échec de la découverte MTU pour les connexions qui ne passent pas par NetScaler Gateway ou Citrix Gateway Service. Pour résoudre ce problème, effectuez une mise à niveau vers VDA version 2103 ou ultérieure. [CVADHELP-16654]
- Lorsque vous utilisez NetScaler Gateway, les chemins réseau asymétriques peuvent entraîner l'échec de la découverte MTU. Cela est dû à un problème sur Gateway qui empêche la propagation du bit Ne pas fragmenter (DF) dans l'en-tête des paquets EDT. Un correctif pour ce problème est disponible à partir de la version 13.1 build 17.42 du microprogramme. Pour plus d'informations sur la procédure d'activation du correctif, consultez la documentation de NetScaler Gateway. [CGOP-18438]
- La découverte MTU peut échouer pour les utilisateurs qui se connectent via un réseau DS-Lite. Certains modems ne respectent pas le bit DF lorsque le traitement des paquets est activé, ce qui empêche la découverte MTU de détecter la fragmentation. Dans ce cas, les options disponibles sont les suivantes :
  - Désactivez le traitement des paquets sur le modem de l'utilisateur.
  - Désactivez la **découverte MTU** et utilisez une MTU codé en dur, comme décrit dans l'article How to configure MSS when using EDT on networks with non-standing MTU.

- Désactivez le **Transport adaptatif** pour forcer les sessions à utiliser TCP. Si seul un sous-ensemble d'utilisateurs est affecté, envisagez de le désactiver côté client afin que les autres utilisateurs puissent continuer à utiliser EDT.

## HDX Direct (Technical Preview)

June 27, 2024

Lors de l'accès aux ressources fournies par Citrix, HDX Direct permet aux périphériques clients internes et externes d'établir une connexion directe sécurisée avec l'hôte de la session si une communication directe est possible.

> **Important :**
>
> HDX Direct est actuellement disponible en version Technical Preview. Cette fonctionnalité est fournie sans support et n'est pas encore recommandée pour une utilisation dans les environnements de production. Pour envoyer des commentaires ou signaler des problèmes, utilisez ce formulaire.

### Configuration système requise

Configuration système requise pour utiliser HDX Direct :

- Plan de contrôle
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 ou ultérieure
- Virtual Delivery Agent (VDA)
  - Windows : version 2402 ou ultérieure
- Application Workspace
  - Windows : version 2402 ou ultérieure
- Niveau d'accès
  - Citrix Workspace avec Citrix Gateway Service
  - Citrix Workspace avec NetScaler Gateway
- Autre
  - Le transport adaptatif doit être activé pour les connexions directes externes

## Configuration réseau requise

La configuration réseau requise pour utiliser HDX Direct est la suivante :

### Hôtes de sessions

Si vos hôtes de session disposent d'un pare-feu tel que le pare-feu Windows Defender, vous devez autoriser le trafic entrant suivant pour les connexions internes.

| Description | Source | Protocole | Port |
|---|---|---|---|
| Connexion interne directe | Client | TCP | 443 |
| Connexion interne directe | Client | UDP | 443 |

> Remarque :
>
> Le programme d'installation du VDA ajoute les règles entrantes appropriées au pare-feu Windows Defender. Si vous utilisez un autre pare-feu, vous devez ajouter les règles ci-dessus.

### Réseau client

Le tableau suivant décrit le réseau client pour les utilisateurs internes et externes.

### Utilisateurs internes

| Description | Protocole | Source | Port source | Destination | Port de destination |
|---|---|---|---|---|---|
| Connexion interne directe | TCP | Réseau client | 1024–65535 | Réseau VDA | 443 |
| Connexion interne directe | UDP | Réseau client | 1024–65535 | Réseau VDA | 443 |

### Utilisateurs externes

| Description | Protocole | Source | Port source | Destination | Port de destination |
|---|---|---|---|---|---|
| STUN (utilisateurs externes uniquement) | UDP | Réseau client | 1024–65535 | Internet (voir remarque ci-dessous) | 3478, 19302 |
| Connexion utilisateur externe | UDP | Réseau client | 1024–65535 | Adresse IP publique du centre de données | 1024–65535 |

**Réseau de centres de données**

Le tableau suivant décrit le réseau du centre de données pour les utilisateurs internes et externes.

**Utilisateurs internes**

| Description | Protocole | Source | Port source | Destination | Port de destination |
|---|---|---|---|---|---|
| Connexion interne directe | TCP | Réseau client | 1024–65535 | Réseau VDA | 443 |
| Connexion interne directe | UDP | Réseau client | 1024–65535 | Réseau VDA | 443 |

**Utilisateurs externes**

| Description | Protocole | Source | Port source | Destination | Port de destination |
|---|---|---|---|---|---|
| STUN (utilisateurs externes uniquement) | UDP | Réseau VDA | 1024–65535 | Internet (voir remarque ci-dessous) | 3478, 19302 |
| Connexion utilisateur externe | UDP | DMZ/Réseau interne | 1024–65535 | Réseau VDA | 55000–55250 |

| Description | Protocole | Source | Port source | Destination | Port de destination |
|---|---|---|---|---|---|
| Connexion utilisateur externe | UDP | Réseau VDA | 55000–55250 | IP publique du client | 1024–65535 |

> **Remarque :**
>
> Le VDA et l'application Workspace tentent d'envoyer des requêtes STUN aux serveurs suivants dans le même ordre :
>
> - stunserver.stunprotocol.org:3478
> - employees.org:3478
> - stun.l.google.com:19302
>
> Si vous modifiez la plage de ports par défaut pour les connexions utilisateur externes à l'aide du paramètre de stratégie **Plage de ports HDX Direct**, les règles de pare-feu correspondantes doivent correspondre à votre plage de ports personnalisée.

### Configuration

HDX Direct est désactivé par défaut. Vous pouvez configurer cette fonctionnalité à l'aide du paramètre **HDX Direct** dans la stratégie Citrix.

- **HDX Direct** : permet d'activer ou de désactiver une fonctionnalité.
- **Mode HDX Direct** : détermine si **HDX Direct** est disponible pour les clients internes uniquement ou pour les clients internes et externes.
- **Plage de ports HDX Direct** : définit la plage de ports que le VDA utilise pour les connexions provenant de clients externes.

### Considérations

Les points suivants sont à prendre en compte lors de l'utilisation de HDX Direct :

- HDX Direct pour les utilisateurs externes est uniquement disponible avec EDT (UDP) comme protocole de transport. Le **transport adaptatif** doit donc être activé.
- Si vous utilisez **HDX Insight**, notez que l'utilisation de **HDX Direct** empêche la collecte de données HDX Insight, car la session ne serait plus transmise par proxy via NetScaler Gateway.
- Lorsque vous utilisez des machines non persistantes pour vos applications et bureaux virtuels, Citrix recommande d'activer **HDX Direct** sur les hôtes de session plutôt que dans l'image maître/modèle afin que chaque machine génère ses propres certificats.

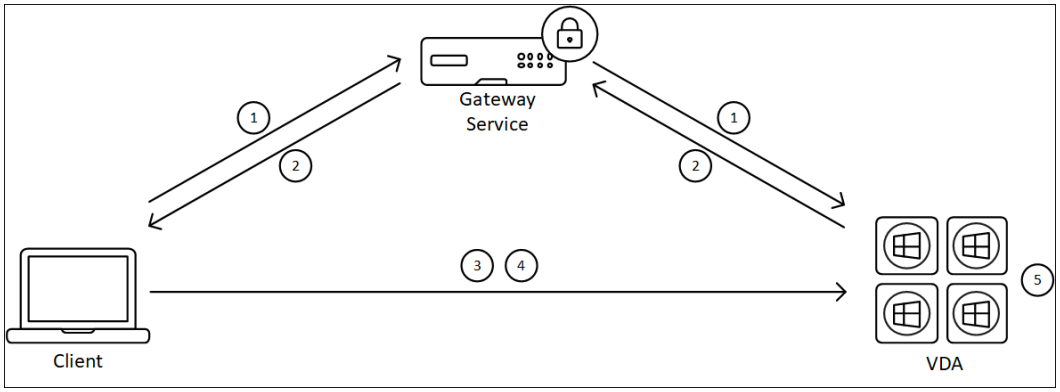
- L'utilisation de vos propres certificats avec HDX Direct n'est actuellement pas prise en charge.

## Fonctionnement

HDX Direct permet aux clients d'établir une connexion directe avec l'hôte de session lorsqu'une communication directe est disponible. Lorsque des connexions directes sont établies à l'aide de HDX Direct, des certificats auto-signés sont utilisés pour sécuriser la connexion directe à l'aide du cryptage au niveau du réseau (TLS/DTLS).

### Utilisateurs internes

Le schéma suivant présente une vue d'ensemble du processus de connexion HDX Direct des utilisateurs internes.



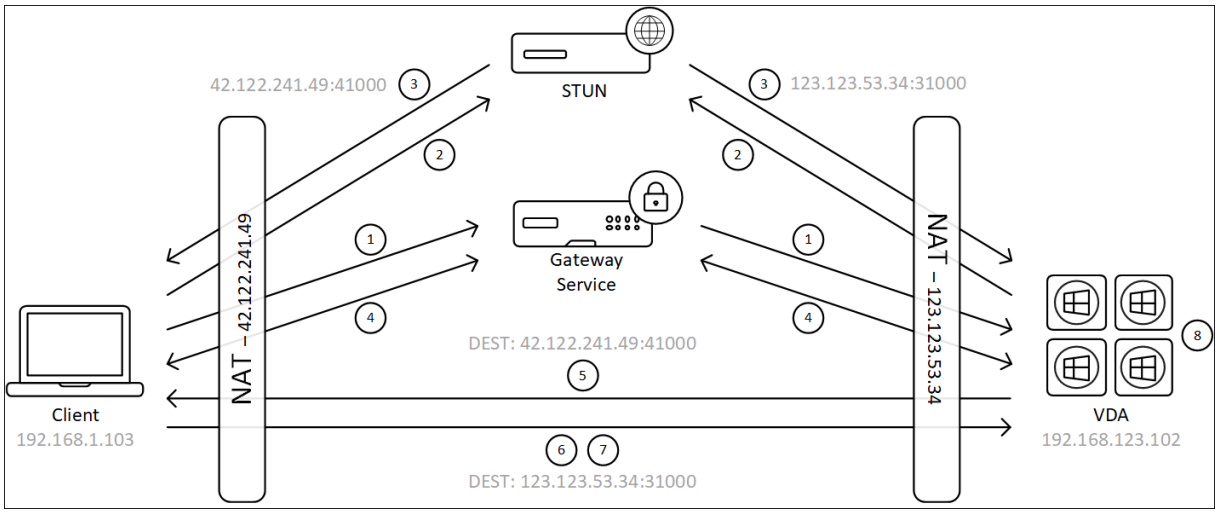

1. Le client établit une session HDX via Gateway Service.
2. Une fois la connexion établie, le VDA envoie au client le nom de domaine complet de la machine VDA, une liste de ses adresses IP et le certificat de la machine VDA via la connexion HDX.
3. Le client analyse les adresses IP pour voir s'il peut accéder directement au VDA.
4. Si le client peut accéder directement au VDA avec l'une des adresses IP partagées, il établit une connexion directe avec le VDA, sécurisée par (D)TLS à l'aide d'un certificat correspondant à celui échangé à l'étape (2).
5. Une fois la connexion directe établie, la session est transférée vers la nouvelle connexion, mettant fin à la connexion à Gateway Service.

> **Remarque :**
>
> Après avoir établi la connexion à l'étape 2 ci-dessus, la session est active. Les étapes suivantes ne retardent ni n'entravent pas la capacité de l'utilisateur à utiliser l'application ou le bureau virtuel. Si l'une des étapes suivantes échoue, la connexion via Gateway est maintenue sans interrompre la session de l'utilisateur.

### Utilisateurs externes

Le schéma suivant présente une vue d'ensemble du processus de connexion HDX Direct pour les utilisateurs externes :




1. Le client établit une session HDX via Gateway Service.
2. Une fois la connexion établie, le client et le VDA envoient une requête STUN pour découvrir leurs adresses IP et ports publics.
3. Le serveur STUN répond au client et au VDA avec leurs adresses IP et ports publics correspondants.
4. Par le biais de la connexion HDX, le client et le VDA échangent leurs adresses IP publiques et leurs ports UDP, et le VDA envoie son certificat au client.
5. Le VDA envoie des paquets UDP à l'adresse IP publique et au port UDP du client. Le client envoie des paquets UDP à l'adresse IP publique et au port UDP du VDA.
6. À la réception d'un message du VDA, le client répond par une demande de connexion sécurisée.
7. Lors de la prise de contact DTLS, le client vérifie que le certificat correspond au certificat échangé à l'étape (4). Après validation, le client envoie son jeton d'autorisation. Une connexion directe sécurisée est désormais établie.
8. Une fois la connexion directe établie, la session est transférée vers la nouvelle connexion, mettant fin à la connexion à Gateway Service.

> **Remarque :**
>
> Après avoir établi la connexion à l'étape 2 ci-dessus, la session est active. Les étapes suivantes ne retardent ni n'entravent pas la capacité de l'utilisateur à utiliser l'application ou le bureau virtuel. Si l'une des étapes suivantes échoue, la connexion via Gateway est maintenue sans interrompre la session de l'utilisateur.

## Gestion des certificats

### Hôte de la session

Les deux services suivants de la machine VDA gèrent la création et la gestion des certificats, tous deux configurés pour s'exécuter automatiquement au démarrage de la machine :

- Service Citrix ClxMtp : responsable de la génération et de la rotation des clés de certificats CA.
- Service Citrix Certificate Manager : responsable de la génération et de la gestion du certificat CA racine autosigné et des certificats de machine.

Les étapes suivantes décrivent le processus de gestion des certificats :

1. Les services sont lancés au démarrage de la machine.
2. `Citrix ClxMtp Service` crée des clés si aucune n'a encore été créée.
3. Le service Citrix Certificate Manager vérifie si **HDX Direct** est activé. Dans le cas contraire, le service s'arrête de lui-même.
4. Si **HDX Direct** est activé, le service Citrix Certificate Manager vérifie si un certificat CA racine autosigné existe. Dans le cas contraire, un certificat racine autosigné est créé.
5. Une fois qu'un certificat d'autorité de certification racine est disponible, le service Citrix Certificate Manager vérifie s'il existe un certificat de machine autosigné. Dans le cas contraire, le service génère des clés et crée un nouveau certificat à l'aide du nom de domaine complet de la machine.
6. Si un certificat de machine existant a été créé par le service Citrix Certificate Manager et que le nom du sujet ne correspond pas au nom de domaine complet de la machine, un nouveau certificat est généré.

> **Remarque :**
>
> Le service Citrix Certificate Manager génère des certificats RSA qui exploitent des clés de 2 048 bits.

### Machine cliente

Pour établir une connexion **HDX Direct** sécurisée, le client doit faire confiance aux certificats utilisés pour sécuriser la session. Pour faciliter cela, le client reçoit le certificat CA pour la session via le fichier ICA (fourni par Workspace). Il n'est donc pas nécessaire de distribuer des certificats CA aux magasins de certificats des appareils clients.

# Compatibilité NAT

June 27, 2024

Pour établir une connexion directe entre un périphérique utilisateur externe et l'hôte de session, HDX Direct utilise la perforation pour la traversée NAT et le STUN pour faciliter l'échange de l'adresse IP publique et des cartographies de ports pour la machine cliente et l'hôte de session. Ceci est similaire au fonctionnement des solutions VoIP, de communications unifiées et de P2P.

Tant que les pare-feux et autres composants réseau sont configurés pour autoriser le trafic UDP pour les requêtes STUN et les sessions HDX, HDX Direct pour les utilisateurs externes devrait fonctionner. Cependant, dans certains scénarios, les types NAT des réseaux utilisateur et hôte de session entraînent une combinaison incompatible, entraînant ainsi l'échec de HDX Direct.

## Validations

Vous pouvez valider le type NAT sur le client et l'hôte de session à l'aide de l'utilitaire client STUN de STUNTMAN :

1. Téléchargez le package approprié pour la plate-forme cible sur stunprotocol.org et extrayez le contenu.
2. Ouvrez une invite de terminal et accédez au répertoire dans lequel le contenu a été extrait.
3. Exécutez la commande suivante :
   ```
   .\stunclient.exe stunserver.stunprotocol.org --mode behavior
   ```
4. Prenez note de la sortie.

Si les tests de liaison et de comportement sont réussis, le **test de liaison** et le **test de comportement** l'indiquent et un comportement NAT est spécifié :


Si les tests échouent, le **test de liaison** et le **test de comportement** l'indiquent.

Consultez le tableau suivant pour déterminer si HDX Direct pour utilisateurs externes est censé fonctionner sur la base des résultats des tests du client et de l'hôte de session :

| Machine cliente | Hôte de la session | Il devrait fonctionner ? |
|---|---|---|
| Cartographie indépendante des terminaux | Cartographie indépendante des terminaux | Oui |
| Cartographie indépendante des terminaux | Cartographie dépendante des terminaux | Oui |
| Cartographie dépendante des terminaux | Cartographie indépendante des terminaux | Oui |
| Cartographie dépendante des terminaux | Cartographie dépendante des terminaux | Non |
| Mappage dépendant de l'adresse et du port | Tout type de NAT | Non |
| Tout type de NAT | Mappage dépendant de l'adresse et du port | Non |
| échec | Tout type de NAT | Non |
| Tout type de NAT | échec | Non |
| échec | échec | Non |

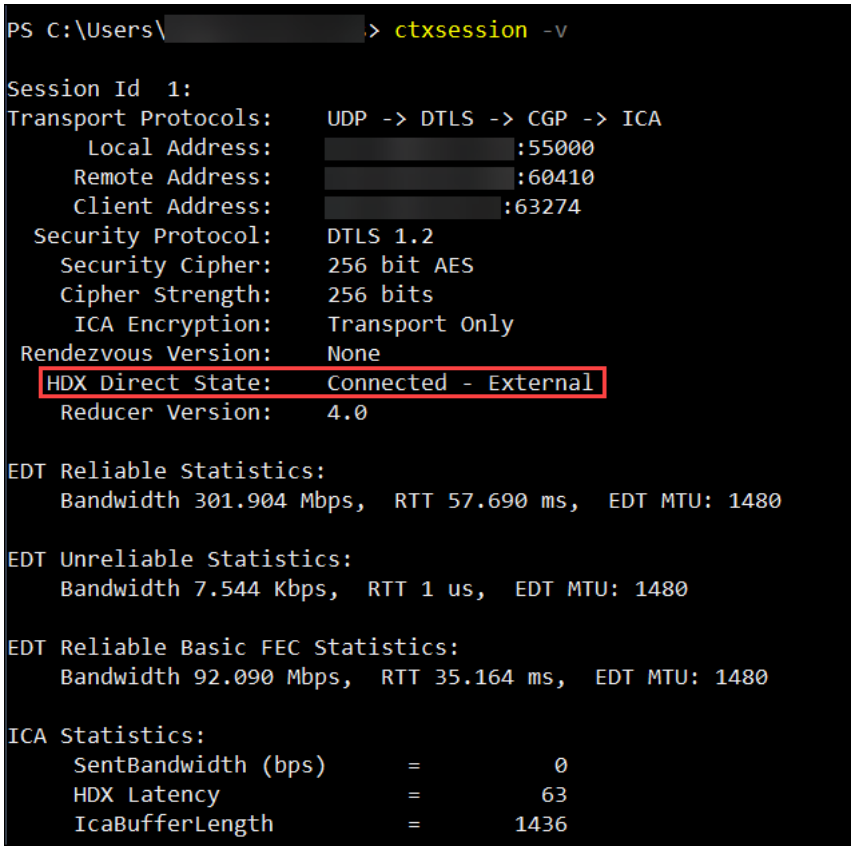
## Dépannage

June 27, 2024

Pour vérifier que **HDX Direct** a réussi à établir une connexion directe, exécutez l'utilitaire `CtxSession.exe` sur la machine VDA.

Pour exécuter l'utilitaire `CtxSession.exe`, lancez une invite de commandes ou PowerShell durant la session et exécutez `ctxsession.exe -v`. Si la connexion **HDX Direct** est établie, le **statut de HDX Direct** est `Connected`.




Vous pouvez également consulter les journaux d'événements de l'hôte de la session pour savoir si la connexion HDX Direct a été établie ou a échoué. Pour plus de détails, consultez la section **Journaux d'événements**.

> Remarque :
>
> Selon l'environnement et le nombre d'adresses IP disponibles pour les hôtes de session, l'établissement de la connexion HDX Direct peut prendre jusqu'à 5 minutes.

### Si HDX Direct ne parvient pas à établir une connexion directe

Si HDX Direct ne parvient pas à établir une connexion directe, suivez les étapes suivantes :

1. Assurez-vous que la version du VDA et la version de l'application Workspace utilisées prennent en charge la fonctionnalité conformément à la configuration système requise.
2. Vérifiez qu'une stratégie est appliquée au VDA qui active HDX Direct et qu'aucune autre stratégie n'a une priorité plus élevée pour désactiver cette fonctionnalité.
3. Vérifiez que vous avez appliqué au VDA une stratégie qui définit le mode HDX Direct souhaité et qu'aucune autre stratégie ayant une priorité plus élevée ne remplace la configuration.
4. Assurez-vous que le service Citrix CLxMTP est en cours d'exécution sur l'hôte de la session.

5. Assurez-vous que le service Citrix Certificate Manager est en cours d'exécution sur l'hôte de la session. S'il ne fonctionne pas, essayez de le démarrer manuellement. Le service s'arrête automatiquement si HDX Direct est désactivé.
6. Vérifiez si l'hôte de la session possède son certificat Root CA auto-signé :
    a) Délivré à : CA-<hostname> (Par exemple, CA-FTLW11-001)
    b) Délivré par : CA-<hostname> (Par exemple, CA-FTLW11-001)
    c) Informations sur l'émetteur : l'entreprise est Citrix Systems, Inc.
7. Vérifiez si l'hôte de la session possède son certificat de serveur auto-signé :
    a) Délivré à : <host FQDN> (Par exemple, FTLW11-001.ctxlab.net)
    b) Délivré par : CA-<hostname> (Par exemple, CA-FTLW11-001)
    c) Informations sur l'émetteur : l'entreprise est Citrix Systems, Inc.
8. Si des certificats manquent, contactez le support technique de Citrix.
9. Si les certificats sont présents :
    a) Arrêtez le service Citrix Certificate Manager sur l'hôte de la session.
    b) Supprimez à la fois le certificat Root CA auto-signé et le certificat de serveur auto-signé.
    c) Démarrez le service Citrix Certificate Manager sur l'hôte de la session. Le service crée de nouveaux certificats une fois qu'il démarre.
10. Pour les utilisateurs internes :
    a) Assurez-vous que le pare-feu de l'hôte de session ne bloque pas le trafic entrant sur UDP 443 ou TCP 443, respectivement pour HDX sur EDT et HDX sur TCP.
    b) Assurez-vous que votre pare-feu réseau ne bloque pas le trafic sur UDP 443 et TCP 443 entre le réseau de vos clients et le réseau des hôtes de session.
11. Pour les utilisateurs externes :
    a) Vérifiez le type de NAT du client et de l'hôte de session et assurez-vous que la combinaison est censée fonctionner. Consultez la section Compatibilité NAT pour plus de détails.
    b) Si le test NAT échoue sur le client ou sur l'hôte de session :
        i. Si un pare-feu est en cours d'exécution sur le système, assurez-vous qu'il ne bloque pas le trafic sortant sur UDP 3478.
        ii. Assurez-vous que les pare-feux de votre réseau ne bloquent pas le trafic sortant sur UDP 3478.
        iii. Assurez-vous que les pare-feux ne bloquent pas la réponse du serveur STUN.
    c) Assurez-vous que les règles appropriées sont configurées pour autoriser tout le trafic nécessaire à vos pare-feux réseau. Consultez la section Configuration réseau requise pour plus de détails.

d) Si vous modifiez la plage de ports par défaut à l'aide du paramètre de stratégie de plage de ports HDX Direct, assurez-vous que vos règles de pare-feu sont définies pour la plage de ports personnalisée.

### Journaux d'événements

Les événements suivants sont consignés dans le journal des événements de la machine VDA :

| Journal | ID | Source | Niveau | Description |
|---|---|---|---|---|
| Journaux des applications et des services > Citrix-HostCore-HDX Direct/Operational | 1 | HDX Direct | Information | Connexion HDX Direct établie pour l'utilisateur <username> interne. |
| Journaux des applications et des services > Citrix-HostCore-HDX Direct/Operational | 2 | HDX Direct | Information | Connexion HDX Direct établie pour l'utilisateur <username> externe. |
| Journaux des applications et des services > Citrix-HostCore-HDX Direct/Operational | 3 | HDX Direct | Information | Échec de la connexion HDX Direct pour l'utilisateur <username>. |

### Problèmes connus

HDX Direct peut cesser de fonctionner après avoir effectué une mise à niveau sur place du VDA sur une machine sur laquelle **HDX Direct** est déjà activé.
Pour résoudre le problème, procédez comme suit :

1. Arrêtez le service Citrix Certificate Manager sur l'hôte de la session.
2. Supprimez le certificat Root CA auto-signé et le certificat de serveur auto-signé.

3. Ouvrez le registre.
4. Supprimez la clé `HKLM\Software\Citrix\HDX-Direct`.
5. Accédez à `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`.
6. Définissez la valeur **SSLEnabled** sur `0`.
7. Supprimez le contenu de la valeur **SSLThumbprint**.
8. Démarrez le **Citrix Certificate Manager Service**.

## Secure HDX (Technical Preview)

June 27, 2024

Secure HDX est une solution de cryptage au niveau de l'application (ALE) qui empêche tout élément de réseau sur le chemin du trafic de pouvoir inspecter le trafic HDX. Pour ce faire, il fournit un véritable cryptage de bout en bout (E2EE) au niveau de l'application entre l'application Citrix Workspace (client) et le VDA (hôte de session) à l'aide du cryptage AES-256-GCM.

> **Important :**
>
> Secure HDX est actuellement disponible en version Technical Preview. Cette fonctionnalité est fournie sans support et n'est pas encore recommandée pour une utilisation dans les environnements de production. Pour envoyer des commentaires ou signaler des problèmes, utilisez ce formulaire.

### Configuration système requise

La liste suivante décrit la configuration requise pour utiliser Secure HDX.

- Plan de contrôle
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 ou ultérieure
- Virtual Delivery Agent (VDA)
  - Windows : version 2402 ou ultérieure
- Application Workspace
  - Windows : version 2402 ou ultérieure
- Niveau d'accès
  - Citrix Workspace
  - Citrix StoreFront 2402 ou version ultérieure

### Configuration

Secure HDX est désactivé par défaut. Vous pouvez configurer cette fonctionnalité à l'aide du paramètre HDX Secure dans la stratégie Citrix :

**Secure HDX**: définit s'il faut activer la fonctionnalité pour toutes les sessions, uniquement pour les connexions directes, ou la désactiver.

### Considérations

Les points suivants sont à prendre en compte lors de l'utilisation de Secure HDX :

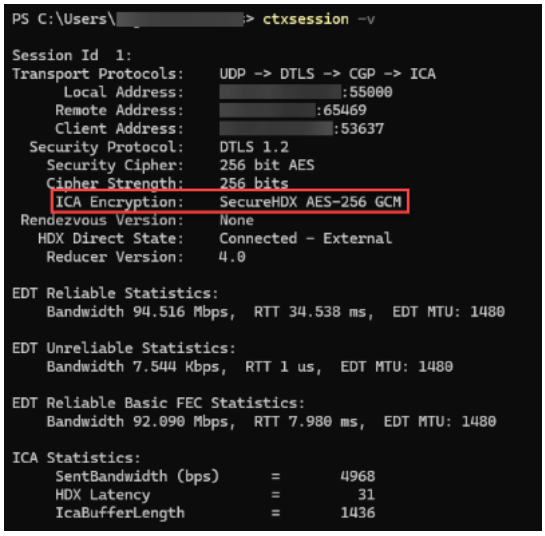
- Si des utilisateurs essaient de se connecter à un hôte de session sur lequel Secure HDX est activé à l'aide d'un client qui ne prend pas en charge cette fonctionnalité, la connexion sera refusée.
- Actuellement, Secure HDX ne prend pas en charge la continuité de service. Si vous activez la continuité de service dans votre environnement Citrix Cloud, il se peut que vous ne puissiez pas vous connecter à des hôtes de session sur lesquels Secure HDX est activé en cas de panne du service Cloud.
- Si vous utilisez HDX Insight, notez que l'utilisation de Secure HDX empêche la collecte de données HDX Insight, car NetScaler n'est pas en mesure d'inspecter le trafic HDX crypté. Si vous devez utiliser HDX Insight, vous pouvez configurer Secure HDX pour l'activer uniquement lors des connexions directes.
- Si vous utilisez SmartControl, notez que l'utilisation de Secure HDX empêche SmartControl de fonctionner, car NetScaler n'est pas en mesure d'inspecter le trafic HDX crypté. Si vous devez utiliser SmartControl, vous pouvez configurer Secure HDX pour l'activer uniquement lors de connexions directes.
- L'ICA multi-stream n'est pas prise en charge lorsque Secure HDX est activé.
- Si vous utilisez des solutions tierces qui reposent sur l'inspection du trafic HDX, elles ne fonctionneront plus si vous activez Secure HDX, car le trafic HDX est crypté.

### Dépannage

Pour vérifier si Secure HDX est activé, vous pouvez exécuter l'utilitaire `ctxsession.exe` sur la machine VDA.

Pour exécuter l'utilitaire `CtxSession.exe`, lancez une invite de commandes ou PowerShell durant la session et exécutez `ctxsession.exe -v`. Si Secure HDX est activé, le cryptage ICA Encryption affiche `SecureHDX AES-256 GCM`.




**Lorsque Secure HDX ne s'active pas durant la session**

- Assurez-vous que la version du VDA utilisée prend en charge la fonctionnalité conformément à la configuration système requise.
- Vérifiez qu'une stratégie est appliquée au VDA qui active HDX Direct et qu'aucune autre stratégie de priorité supérieure ne peut désactiver cette fonctionnalité.
- Si la machine client se connecte via NetScaler Gateway ou Gateway Service, assurez-vous que Secure HDX n'est pas défini sur « Connexions directes uniquement ».
- Si l'hôte de session était déjà en cours d'exécution lorsque vous avez configuré Secure HDX, redémarrez l'ordinateur pour garantir la prise d'effet des modifications.

## Liste verte des canaux virtuels

June 27, 2024

La liste verte des canaux virtuels est une fonctionnalité qui vous permet de contrôler les canaux virtuels non-Citrix autorisés dans votre environnement. Par défaut, la fonctionnalité de liste verte des canaux virtuels est activée. Par conséquent, seuls les canaux virtuels Citrix sont autorisés à s'ouvrir dans les sessions Citrix Virtual Apps and Desktops. S'il est nécessaire d'utiliser des canaux virtuels personnalisés, qu'ils soient locaux ou provenant d'un tiers, ils doivent être explicitement ajoutés à la liste d'autorisation.

### Configuration

La liste verte des canaux virtuels est activée par défaut. Vous pouvez configurer cette fonctionnalité à l'aide des paramètres suivants de la stratégie Citrix :

- **Liste verte des canaux virtuels** : pour activer ou désactiver la fonctionnalité et ajouter des canaux virtuels à la liste.
- **Limitation de journalisation de la liste verte des canaux virtuels** : définit la période de limitation pour la journalisation des événements de la liste verte des canaux virtuels.
- **Journalisation de la liste verte des canaux virtuels** : définit le niveau de journalisation de la liste verte des canaux virtuels.

### Ajout de canaux virtuels à la liste d'autorisation

Pour ajouter une chaîne virtuelle à la liste verte, vous avez besoin des informations suivantes :

1. Le nom du canal virtuel tel que défini dans le code, qui peut contenir jusqu'à sept caractères. Par exemple, `CTXCVC1`.
2. Les chemins d'accès aux processus qui ouvrent le canal virtuel sur la machine VDA. Par exemple, `C:\Program Files\Application\run.exe`.

Une fois que vous avez les informations requises, vous devez ajouter le canal virtuel à la liste d'autorisation à l'aide du paramètre de stratégie Liste d'autorisation des canaux virtuels. Pour ajouter un canal virtuel à la liste, entrez le nom du canal virtuel suivi d'une virgule, puis le chemin d'accès au processus qui accède au canal virtuel. S'il existe plusieurs processus, vous pouvez les ajouter en séparant chaque processus par des virgules.

#### Dans le cas de processus uniques

En utilisant les exemples précédents, ajoutez les éléments suivants à la liste :

```
CTXCVC1,C:\Program Files\Application\run.exe
```

#### Dans le cas de plusieurs processus

S'il y a plusieurs processus, ajoutez l'entrée suivante à la liste :

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

### Caractères génériques

L'utilisation de caractères génériques (*) est prise en charge. Vous pouvez utiliser des caractères génériques lorsque les noms des répertoires ou des exécutables changent en fonction de la version de l'application ou si le composant tiers est installé dans les profils des utilisateurs.

Vous pouvez utiliser des caractères génériques dans les scénarios suivants :

- Pour remplacer le nom complet du répertoire.
  Par exemple : `C:\Program Files\Application\*\run1.exe`
- Pour remplacer une partie du nom du répertoire.
  Par exemple : `C:\Program Files\Application\v*\run1.exe`
- Pour remplacer le nom de l'exécutable.
  Par exemple : `C:\Program Files\Application\v1.2\*.exe`
- Pour remplacer une partie du nom de l'exécutable.
  Par exemple : `C:\Program Files\Application\v1.2\run*.exe`

Les restrictions suivantes s'appliquent :

- Le caractère générique ne peut être utilisé que pour remplacer un seul répertoire. Par exemple, si l'exécutable se trouve dans `C:\Program Files\Application\v1.2\run1.exe`
  - Autorisé : `C:\Program Files\Application\*\run1.exe`
  - Non autorisée : `C:\Program Files\*\run1.exe`
- Les entrées doivent contenir l'extension de fichier.
  - Autorisé : `C:\Program Files\Application\v1.2\*.exe`
  - Non autorisée : `C:\Program Files\Application\v1.2\*`
- Tous les chemins doivent être locaux.

> **Remarque :**
>
> - Les chemins réseau ne sont pas autorisés.
> - La prise en charge des caractères génériques est disponible à partir de Citrix Virtual Apps and Desktops 2206.
> - La prise en charge des caractères génériques est disponible dans Citrix Virtual Apps and Desktops 2203 LTSR à partir de la version CU2.

### Utilisation des variables d'environnement système

Vous pouvez utiliser des variables d'environnement système pour simplifier la définition des processus approuvés dans la liste verte. Vous pouvez utiliser toutes les variables prêtes à l'emploi, telles que %`programfiles`%, %`programfiles(x86)`%, %`systemdrive`% et %`systemroot`%.

Vous pouvez également utiliser des variables d'environnement personnalisées tant qu'elles sont définies au niveau du système.

Les exemples suivants présentent les variables d'environnement prêtes à l'emploi :

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application\*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

L'exemple suivant décrit une variable d'environnement système personnalisée :

- Nom de variable personnalisé : `app`
- Valeur de variable personnalisée : `%programfiles%\Application\`
- Entrée dans la liste d'autorisation : `CTXCVC1,%app%\run.exe`

> **Remarque :**
>
> Les variables d'environnement utilisateur ne sont pas prises en charge.
>
> La prise en charge des variables d'environnement est disponible à partir de la version 2209 de Citrix Virtual Apps and Desktops.

### Obtenir des noms et des processus de canaux virtuels

Le moyen le plus simple d'obtenir le nom du canal virtuel et le processus qui l'ouvre sur la machine VDA est de demander ces informations au développeur ou au fournisseur tiers qui a fourni le canal virtuel.

Vous pouvez également obtenir ces informations en appliquant les journaux de la fonctionnalité et en procédant comme suit :

1. Une fois que les composants client et serveur du canal virtuel personnalisé sont en place, lancez une application virtuelle ou un bureau virtuel.
2. Dans le journal des événements système de la machine VDA, recherchez le nom du canal virtuel personnalisé et le processus qui a essayé de l'ouvrir. Pour plus d'informations sur les événements disponibles, consultez la section Journaux d'événements.
3. Déconnectez-vous de la session.
4. Ajoutez une entrée dans les paramètres de la stratégie de liste verte des canaux virtuels pour le canal virtuel et le processus identifiés.
5. Redémarrez la machine.
6. Une fois le VDA enregistré, exécutez l'application virtuelle ou le bureau virtuel pour vérifier que les canaux virtuels personnalisés s'ouvrent correctement.

### Considérations relatives aux canaux virtuels Citrix

Tous les canaux virtuels Citrix intégrés sont approuvés et peuvent s'ouvrir sans autre configuration. Toutefois, les deux fonctionnalités suivantes nécessitent des entrées explicites dans la liste verte en raison de dépendances externes :

- Redirection multimédia
- Pack d'optimisation HDX RealTime pour Skype Entreprise

#### Redirection multimédia

Si vous utilisez un lecteur multimédia autre que Windows Media Player comme lecteur multimédia de votre système, vous devez l'ajouter à la liste verte en tant que processus approuvé. Les informations suivantes sont requises pour l'entrée dans la liste verte :

- Nom du canal virtuel : `CTXMM`
- Processus : chemin d'accès au lecteur multimédia utilisé sur votre machine VDA. Par exemple, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Entrée dans la liste d'autorisation : `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

#### Pack d'optimisation HDX RealTime pour Skype Entreprise

Les informations suivantes sont requises pour l'entrée dans la liste verte :

- Nom du canal virtuel : `CTXRMEP`
- Processus : chemin d'accès à l'exécutable Skype Entreprise sur votre machine VDA, qui peut varier en fonction de la version de Skype Entreprise ou si vous avez utilisé un chemin d'installation personnalisé. Par exemple, `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.
- Entrée dans la liste d'autorisation : `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

## Dépannage

June 27, 2024

Si votre canal virtuel personnalisé ne s'ouvre pas, procédez comme suit :

1. Assurez-vous que vous utilisez la version de VDA appropriée.

2. Vérifiez que vous avez appliqué au VDA une stratégie avec le canal virtuel personnalisé figurant dans la liste verte des canaux virtuels et qu'aucune autre stratégie ayant une priorité plus élevée ne remplace la configuration.
3. Consultez le journal des événements dans le VDA et vérifiez que le nom du canal virtuel indiqué correspond à celui défini dans la liste verte.

    a) Si vous avez plusieurs processus, assurez-vous qu'ils sont correctement définis, comme décrit dans la section Ajouter de canaux virtuels à la liste d'autorisation.
    b) Si vous utilisez des caractères génériques dans le chemin de processus défini, assurez-vous de respecter les directives relatives à l'utilisation de caractères génériques.
    c) Si vous utilisez des variables d'environnement dans le chemin de processus défini, assurez-vous de respecter les directives de la section Utilisation de variables d'environnement système.

## Journaux d'événements

Les événements suivants sont consignés dans le journal des événements de la machine VDA.

### VDA mono-session

Les événements suivants sont consignés dans le journal des événements de la machine VDA mono-session :

| Nom du journal | ID | Source | Niveau | Description |
|---|---|---|---|---|
| Système | 2001 | `Picadd` | Information | Le canal virtuel personnalisé <`vcName`> a été ouvert par le processus < `processName`> |
| Système | 2002 | `Picadd` | Avertissement | Le canal virtuel personnalisé <`vcName`> ne peut pas être ouvert par le processus < `processName`> |

| Nom du journal | ID | Source | Niveau | Description |
|---|---|---|---|---|
| Système | 2003 | Picadd | Information | <username> a ouvert le canal virtuel personnalisé <vcName> |
| Système | 2004 | Picadd | Avertissement | <username> a essayé d'ouvrir le canal virtuel personnalisé <vcName> |
| Système | 2005 | Picadd | Erreur | Le chemin indiqué dans la stratégie < pathInPolicy > ne peut pas être résolu en chemin de processus. |
| Système | 2007 | Picadd | Information | Le chemin de processus chargé est <processPath >. |
| Système | 2008 | Picadd | Erreur | La variable d'environnement <varName> dans le chemin de stratégie VC est introuvable. |

**VDA multi-session**

Les événements suivants sont consignés dans le journal des événements de la machine VDA multisession :

| Nom du journal | ID | Source | Niveau | Description |
|---|---|---|---|---|
| Système | 13 | Rpm | Information | Le canal virtuel personnalisé <vcName> a été ouvert par le processus <processName> |
| Système | 14 | Rpm | Avertissement | Le canal virtuel personnalisé <vcName> ne peut pas être ouvert par le processus <processName> |
| Système | 15 | Rpm | Information | <username> a ouvert le canal virtuel personnalisé <vcName> |
| Système | 16 | Rpm | Avertissement | <username> a essayé d'ouvrir le canal virtuel personnalisé <vcName> |
| Système | 17 | Rpm | Erreur | Le chemin indiqué dans la stratégie <pathInPolicy> ne peut pas être résolu en chemin de processus. |
| Système | 18 | Rpm | Information | Le chemin de processus chargé est <processPath>. |

| Nom du journal | ID | Source | Niveau | Description |
|---|---|---|---|---|
| Système | 19 | Rpm | Erreur | La variable d'environnement <varName> dans le chemin de stratégie VC est introuvable. |

## Canaux virtuels tiers connus

June 27, 2024

Vous trouverez ci-dessous des solutions tierces connues qui utilisent des canaux virtuels Citrix personnalisés. Cette liste n'inclut pas toutes les solutions qui utilisent un canal virtuel Citrix personnalisé.

- Cerner
- ControlUp
- Cisco WebEx Teams
- Logiciel de bureau virtuel Cisco WebEx Meetings
- deviceTrust
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- Midmark IQPath Client Extensions
- Nuance PowerMic Client Extensions
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings pour VDI
- Ultimate IA-Connect

Pour obtenir des détails sur l'ajout des canaux virtuels associés à la liste d'autorisation, contactez les fournisseurs des solutions. Vous pouvez également suivre les étapes décrites dans la section Obtention de noms et de processus de canaux virtuels.

## Appareils

June 27, 2024

HDX offre une expérience utilisateur haute définition sur n'importe quel périphérique, n'importe où. Les articles de la section Périphériques décrivent ces périphériques :

- Analyse
- Périphérique USB générique
- Mappage des lecteurs clients
- Appareils mobiles et à écran tactile
- Périphériques en série
- Claviers spécialisés
- Webcams

### Périphérique USB optimisé ou générique

Un périphérique USB optimisé est un périphérique pour lequel l'application Citrix Workspace prend en charge des fonctions spécifiques. Par exemple, la possibilité de rediriger les webcams en utilisant le canal virtuel HDX Multimedia. Un périphérique générique est un périphérique USB pour lequel il n'existe aucune fonction spécifique dans l'application Citrix Workspace.

Par défaut, la redirection USB générique ne peut pas rediriger les périphériques USB avec canal virtuel optimisé à moins d'être mis en mode Générique.

En général, vous obtenez de meilleures performances pour les périphériques USB en mode Optimisé qu'en mode Générique. Cependant, il existe des cas où un périphérique USB n'est pas complètement fonctionnel en mode Optimisé. Il peut être nécessaire de passer en mode Générique pour avoir un accès complet à ses fonctionnalités.

Avec les périphériques de stockage de masse USB, vous pouvez utiliser le mappage de lecteurs clients ou la redirection USB générique, ou les deux ; il vous suffit de les configurer dans les stratégies Citrix. Les principales différences sont les suivantes :

Si la redirection USB générique et les stratégies de mappage de lecteurs clients sont activées, alors lorsqu'un périphérique de stockage de masse est inséré avant ou après le démarrage d'une session, il est redirigé à l'aide du mappage de lecteur client.

Lorsque ces conditions sont remplies, le périphérique de stockage de masse est redirigé à l'aide de la redirection USB générique :

- La redirection USB générique et les stratégies de mappage du lecteur client sont activées.
- Un périphérique est configuré pour la redirection automatique.
- Un périphérique de stockage de masse est inséré avant ou après le démarrage d'une session.

Pour plus d'informations, consultez http://support.citrix.com/article/CTX123015.

| Fonctionnalité | Mappage des lecteurs clients | Redirection USB générique |
|---|---|---|
| Activée par défaut | Oui | Non |
| Accès en lecture seule configurable | Oui | Non |
| Accès chiffré au périphérique | Oui, si le cryptage est déverrouillé avant l'accès au périphérique sur la session virtuelle. | Citrix Virtual Desktops uniquement |

## Analyse

June 27, 2024

Le scanner est un périphérique qui numérise optiquement des images, du texte imprimé, de l'écriture manuscrite ou un objet, et le convertit en image numérique.

Si vous utilisez un scanner et que vous disposez d'un ordinateur Windows, il y a de fortes chances que vous utilisiez le pilote du scanner WIA. Ce pilote est responsable de la communication entre votre ordinateur et le scanner.

- **Windows Image Acquisition** (WIA) est le modèle de pilote et l'API de Microsoft qui permettent aux logiciels de communiquer avec du matériel d'imagerie tel que des scanners.
- **TWAIN** (Windows et Mac) est un autre protocole de numérisation qui connecte les scanners et les applications en fournissant une interface standard. TWAIN permet aux applications d'acquérir des images à partir de périphériques compatibles TWAIN (scanners, appareils photo numériques, etc.).

## Redirection TWAIN

June 27, 2024

### Introduction

TWAIN est un protocole de numérisation utilisé pour lier un logiciel d'imagerie à des scanners ou à des périphériques photo numériques.

#### Fonctionnement de TWAIN

- Numérisez vos documents à l'aide de l'une des applications 32 bits de votre session Citrix.

  > **Remarque :**
  >
  > Utilisez un scanner compatible TWAIN connecté localement pour numériser les documents.

- Le module d'analyse Citrix redirige la requête TWAIN vers le scanner du client.
- Une fois l'analyse terminée, l'hôte de la session en est informé.

### Exigences

#### Plan de contrôle Citrix

- Citrix Virtual Apps and Desktops 1912 ou versions ultérieures
- Citrix DaaS

#### Hôte de la session

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Windows 11
  - Windows Server 2022 ou version ultérieure
- VDA
  - Version 1912 ou ultérieure
- Application
  - Application 32 bits

#### Machine cliente

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Windows 11
- Application Workspace
  - Windows : version 1912 ou ultérieure

- Scanneur
  - Scanner conforme à la norme TWAIN

## Configuration

- Installez les pilotes TWAIN sur le point de terminaison client.
- Configurez les périphériques ou les applications pour sélectionner le protocole de numérisation requis s'ils prennent en charge à la fois TWAIN et WIA.
- Liez le scanner au point de terminaison client localement (via USB).
- Redirigez les périphériques TWAIN vers la session via une redirection USB si nécessaire.

> **Remarque :**
>
> Les périphériques TWAIN ne fonctionnent pas correctement avec la redirection USB, ce qui entraîne une mauvaise qualité de numérisation.

### Paramètres de stratégie

Paramètres de stratégie pour configurer la redirection TWAIN et améliorer la numérisation.

- **Redirection de périphérique TWAIN client :** pour activer ou désactiver la redirection TWAIN.

> **Remarque :**
>
> Par défaut, la redirection TWAIN est activée.

- **Niveau de compression TWAIN :** pour définir les niveaux de compression des images du client vers l'hôte.

Pour plus d'informations, consultez la section Paramètres de stratégie Périphériques TWAIN.

## Dépannage

Essayez TWAIN avec l'application de test publique Twacker, qui peut être téléchargée à partir de cette URL.

Suivez les étapes pour valider TWAIN dans le cadre d'une session de bureau publiée :

1. Installez **Twacker** sur le VDA.
2. Lancez **Twacker** (version 32 bits).
3. Cliquez sur **File > Select Source**, puis sélectionnez votre scanner dans la liste.
4. Cliquez sur **File > Acquire**.

5. Cliquez sur le **bouton Scan** pour tester votre scanner.

Si la numérisation **Twacker** est réussie, cela confirme que la configuration de **Citrix Virtual Apps and Desktops** :

- Est configurée pour la redirection USB
- Utilise les périphériques TWAIN
- Répond à toutes les exigences en matière de machines clientes locales

Si vous rencontrez toujours des problèmes de numérisation dans une application particulière, il s'agit probablement d'un problème logiciel.

## Appareils WIA

June 27, 2024

### Exigences

- Le scanner doit être compatible WIA.
- Installez les pilotes WIA sur le périphérique local. Ils ne sont pas requis sur le serveur.
- Connectez le scanner localement (par exemple, via USB).
- Assurez-vous que le scanner utilise le service Acquisition d'image Windows local et non le pilote TWAIN.
- Assurez-vous qu'aucune stratégie n'est appliquée au compte d'utilisateur utilisé pour le test, limitant la bande passante dans la session ICA. Par exemple, la limite de bande passante de redirection du périphérique USB client.

#### Liste verte des applications d'acquisition d'image Windows

Une liste d'autorisation vous permet de contrôler quelles applications du VDA peuvent accéder à la redirection du scanner Acquisition d'image Windows. L'Éditeur du Registre utilise les entrées du paramètre de liste d'autorisation sur chaque VDA contenant Acquisition d'image Windows. Par défaut, aucune application n'a accès à l'acquisition d'image Windows.

Pour ajuster Acquisition d'image Windows pour les applications du VDA, reportez-vous au paramètre Liste d'autorisation d'applications Acquisition d'image Windows de la liste des fonctionnalités gérées via le Registre.

Pour plus d'informations sur les paramètres de stratégie, voir Paramètres de stratégie des périphériques WIA.

# Périphériques USB génériques

June 27, 2024

## Introduction

La fonctionnalité de redirection USB générique permet de rediriger des périphériques USB depuis des machines clientes vers des sessions HDX, ce qui permet aux utilisateurs finaux d'interagir avec une large sélection de périphériques USB génériques au cours de leur session HDX. Cela est utile dans les scénarios où les utilisateurs doivent utiliser des périphériques spécialisés qui ne disposent pas d'un support optimisé ou qui ne sont pas adaptés.

> **Remarque :** les périphériques USB non optimisés pour la prise en charge des canaux virtuels reviendront au canal virtuel USB générique à l'aide de la redirection USB brute.

## Comment fonctionne ce service ?

La redirection USB générique fonctionne à petite échelle, en redirigeant les requêtes USB et les messages de réponse entre les machines clientes et les bureaux virtuels XenDesktop.

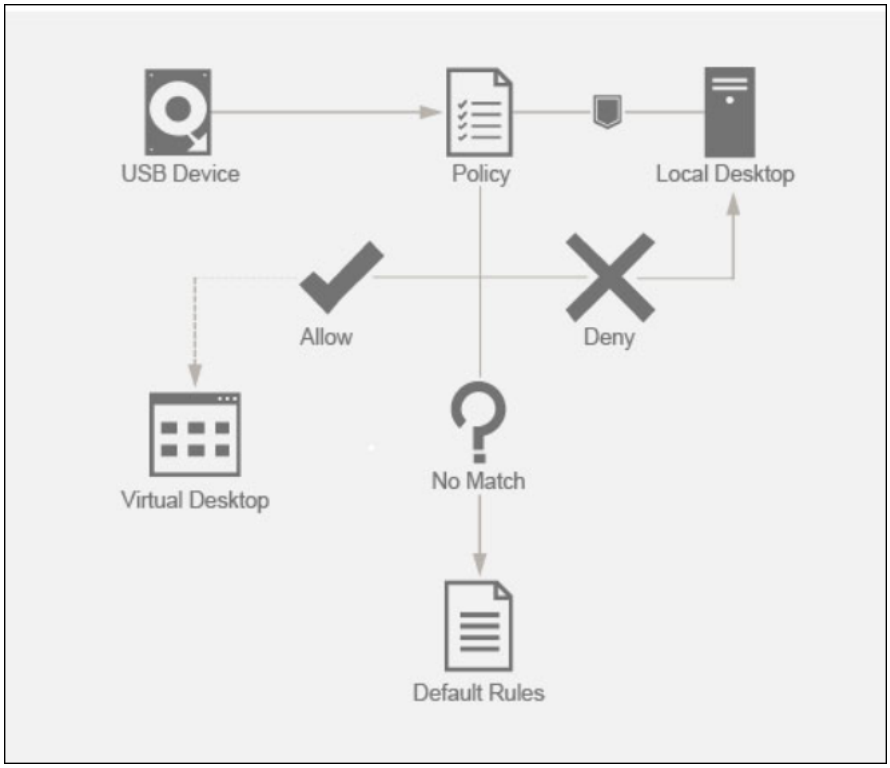
Cela permet d'éviter l'utilisation de pilotes de périphériques compatibles sur la machine cliente ; le pilote doit uniquement être pris en charge sur le bureau virtuel. Les règles de stratégie de redirection USB suivent un certain ordre de priorité qui permet de respecter les stratégies côté client et les règles par défaut une fois que les règles de stratégie Desktop Delivery Controller ont été évaluées et appliquées. Cela permet aux administrateurs Citrix d'empêcher la redirection de tout périphérique non autorisé/usurpé au cours d'une session.

En outre, la journalisation des événements des périphériques non autorisés qui tentent d'accéder à la session à distance peut être auditée et signalée, et les administrateurs peuvent prendre des mesures supplémentaires pour empêcher l'exfiltration de données.

Lorsqu'un utilisateur branche un périphérique USB, l'hôte de session vérifie celui-ci par rapport à chaque règle de stratégie de manière consécutive jusqu'à ce qu'une correspondance soit trouvée. La première correspondance trouvée pour un périphérique est considérée comme définitive.

- Si la première correspondance est une règle Allow, le périphérique est envoyé vers le bureau virtuel.
- Si la première correspondance est une règle Deny, le périphérique n'est pas redirigé vers la session et ne peut être utilisé que sur le périphérique d'utilisateur local. Si aucune correspondance n'est trouvée, les règles par défaut sont utilisées.




## Configuration

June 27, 2024

La redirection USB est désactivée par défaut. Vous pouvez configurer la redirection USB générique à l'aide des paramètres suivants de la stratégie Citrix :

- **Redirection de périphérique USB client** : pour activer ou désactiver la redirection USB
- **Règles de redirection de périphérique USB client** : pour spécifier une action spécifique sur le périphérique, c'est-à-dire autoriser ou refuser l'accès à un périphérique particulier
- **Règles de redirection de périphérique USB client (version 2)** : pour spécifier les règles de filtrage, de division et de connexion automatique des périphériques USB
- **Règles d'optimisation de périphérique USB client** : pour désactiver l'optimisation ou pour modifier le mode d'optimisation
- **Autoriser la connexion automatique des périphériques USB existants** : pour autoriser ou empêcher la connexion automatique des périphériques USB existants connectés à un point de terminaison client au début d'une session HDX
- **Autoriser la connexion automatique des nouveaux périphériques USB** : pour autoriser ou empêcher la connexion automatique des périphériques USB connectés à un point de terminaison client pendant une session HDX

Pour plus d'informations, reportez-vous à la section Paramètres de stratégie Périphériques USB.

## Procédure de configuration de la redirection USB

Par défaut, la configuration de redirection USB est désactivée. Pour l'utiliser, la stratégie de redirection USB et les règles de redirection spécifiques doivent être activées et configurées sur le Desktop Delivery Controller.

> **Remarque :**
>
> Si vous utilisez des composants antérieurs à la version 2212 ou si vous utilisez l'application Workspace pour Linux/Mac, consultez la section Configuration de la redirection USB héritée pour plus de détails sur la configuration de la redirection USB.

### Activation de la redirection USB générique

1. Ouvrez les **stratégies Citrix Web Studio** et cliquez sur l'onglet **Stratégies**.
2. Cliquez sur **Créer une stratégie**, puis développez **ICA > Stratégies de périphériques USB**.
3. Modifiez la **Stratégie de redirection de périphérique USB client**.
4. Sélectionnez **Autorisé**, puis cliquez sur **Enregistrer**.

### Création de règles de stratégie de redirection USB

Lorsque l'utilisateur tente de rediriger un périphérique USB vers Virtual Desktop, il est vérifié par rapport à chaque règle de stratégie USB jusqu'à ce qu'une correspondance soit trouvée. La première correspondance trouvée pour un périphérique est considérée comme définitive. Si la première correspondance est une règle **Allow**, le périphérique correspondant peut être redirigé vers le bureau virtuel. Si la première correspondance est une règle **Deny**, le périphérique correspondant n'est disponible que dans le bureau local. Si aucune correspondance n'est trouvée, les règles par défaut sont utilisées.

**Règles de périphériques** Comme pour les périphériques USB standard, les règles de périphériques définies dans la stratégie ou la configuration de l'application Citrix Workspace client sur le point de terminaison sélectionnent les périphériques à transférer. L'application Citrix Workspace utilise ces règles pour décider sur quels périphériques USB la redirection vers la session à distance doit être autorisée ou bloquée.

Chaque règle se compose d'un mot clé d'action (**Allow, Connect ou Deny**), de deux-points (:) et d'un zéro ou de plusieurs paramètres de filtre correspondant aux périphériques réels du sous-système USB

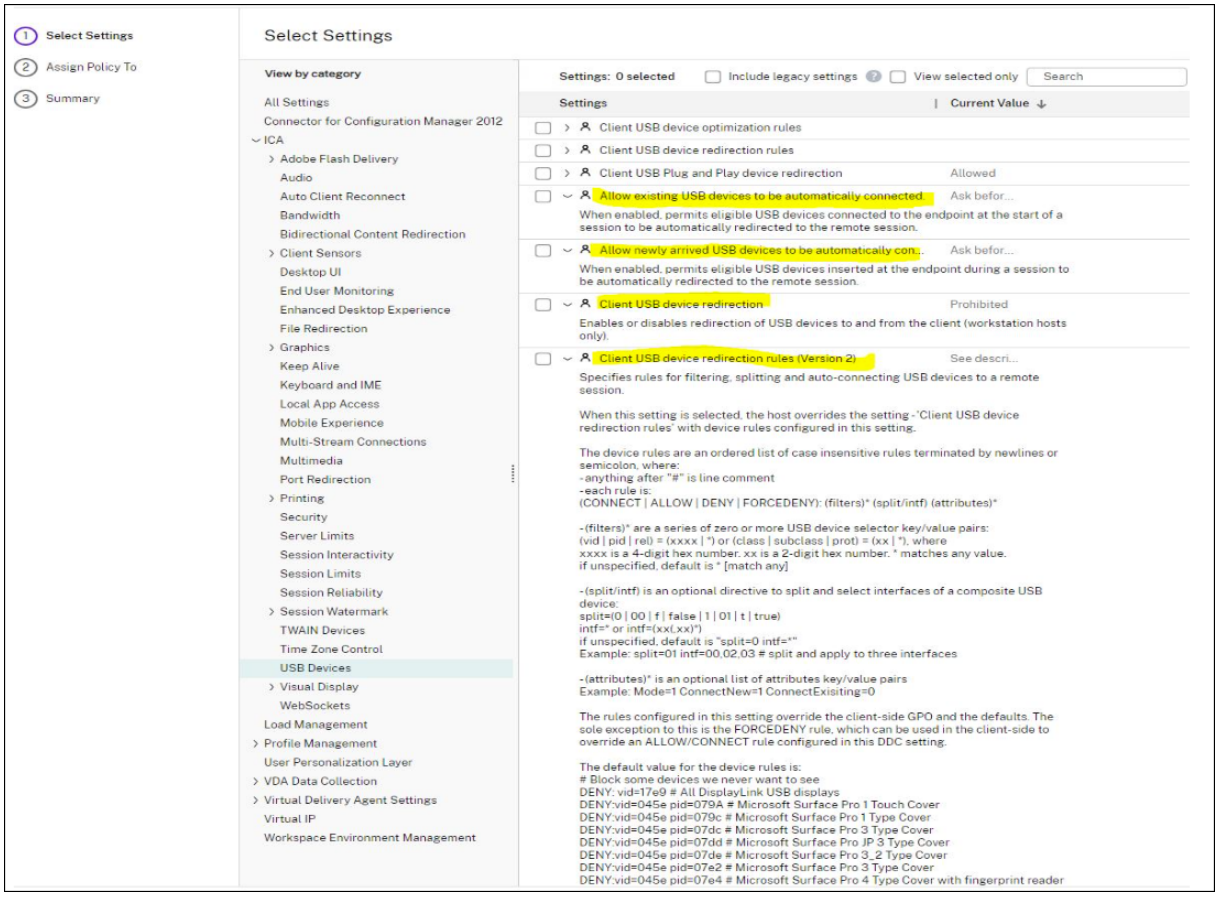
des points de terminaison. Ces paramètres de filtre correspondent aux métadonnées du descripteur de périphérique USB utilisées par chaque périphérique USB pour s'identifier.

Chaque règle de périphériques est constituée d'un texte en clair qui s'affiche sur une seule ligne et d'un commentaire facultatif après le caractère #. Les règles sont mises en correspondance de haut en bas (ordre de priorité décroissant). La première règle qui correspond au périphérique ou à l'interface enfant est appliquée. Les règles suivantes qui sélectionnent le même périphérique ou la même interface sont ignorées.

**Exemple :** ALLOW VID=1050 PID=0421 #Device1
**Exemple :** CONNECT VID=xxxx PID=yyyy Class=03 #Device2

| Mot clé | Description |
| --- | --- |
| CONNECT | Utilisez ce mot clé pour autoriser la redirection des périphériques via le canal virtuel USB et pour leur permettre d'être redirigés automatiquement lors du lancement de la session et lors de l'insertion. |
| ALLOW | Utilisez ce mot clé pour autoriser la redirection des périphériques via le canal virtuel USB. |
| DENY | Utilisez ce mot clé pour empêcher la redirection des périphériques via le canal virtuel USB. |




**Définition de la stratégie sur le Desktop Delivery Controller** :

1. Ouvrez les **stratégies Citrix Web Studio** et cliquez sur l'onglet **Stratégies**.
2. Cliquez sur **Créer une stratégie**, puis développez **ICA > Stratégies de périphériques USB**.
3. Modifiez les **Règles de redirection de périphérique USB** client (**version 2**).
4. Définissez la valeur en fonction des exemples fournis dans la description pour chaque périphérique USB qui doit être redirigé, puis cliquez sur Enregistrer.

   Par exemple : Allow: VID=056A PID=00A4 #STU-430
   Deny: Class=08 subclass=05 # Stockage de masse

   > **Remarque :**
   >
   > Si un administrateur Citrix coche la case **Utiliser valeur par défaut**, puis clique sur **Enregistrer**, les règles par défaut se trouvent dans le registre suivant du VDA.
   >
   > **Attention :**
   >
   > Reportez-vous à la clause d'exclusion de responsabilité à la fin de cet article avant d'utiliser l'Éditeur du Registre.

`HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

> **Remarque :**
>
> Les stratégies peuvent toujours être définies sur la machine cliente à l'aide des règles de périphérique de stratégie de groupe, mais cela n'est plus nécessaire sur les nouvelles versions de CVAD et CWA.
>
> Pour la configuration héritée des périphériques USB, reportez-vous à la section Configuration de la redirection USB héritée.

**Configurer la redirection automatique des périphériques USB (facultatif)**

Les périphériques USB sont automatiquement redirigés lorsque la prise en charge USB est activée. Les paramètres de préférences de l'utilisateur USB sont également définis pour la connexion automatique aux périphériques USB. Il n'est pas toujours recommandé de rediriger tous les périphériques USB. Les utilisateurs peuvent rediriger explicitement les périphériques de la liste de périphériques USB qui ne sont pas automatiquement redirigés. Pour empêcher l'ajout à la liste ou la redirection des périphériques USB, utilisez DeviceRules sur le point de terminaison du client ou sur la stratégie DDC. Cette stratégie peut être définie sur le Desktop Delivery Controller, sur le client à l'aide d'un objet de stratégie de groupe, à l'aide des préférences de Citrix Workspace ou de l'onglet Connections sous CDViewer. Toutes ces méthodes sont décrites ci-dessous :

**Définition de la stratégie sur le Desktop Delivery Controller** :

Deux stratégies peuvent être définies sur le Desktop Delivery Controller pour autoriser la redirection automatique des périphériques USB :

- Autoriser la connexion automatique des périphériques USB existants
- Autoriser la connexion automatique des nouveaux périphériques USB

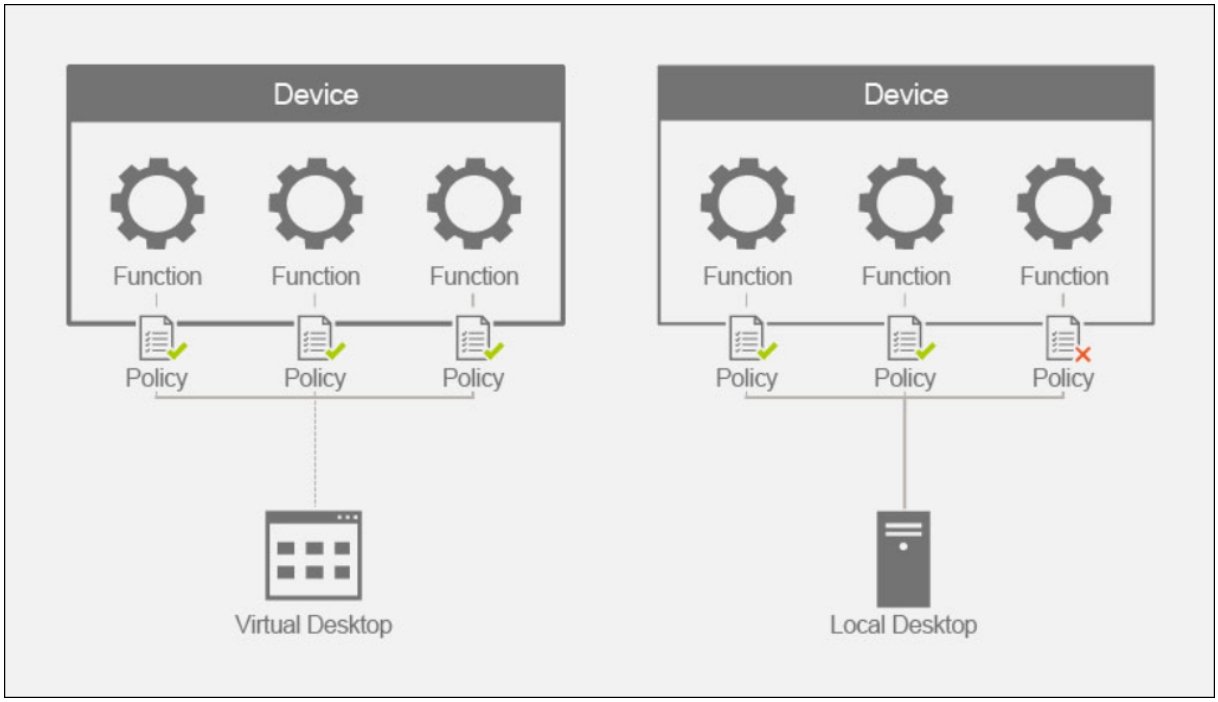
1. Ouvrez les **stratégies Citrix Web Studio** et cliquez sur l'onglet **Stratégies**.
2. Cliquez sur **Créer une stratégie**, puis développez **ICA > Stratégies de périphériques USB**.
3. Modifiez le paramètre **Autoriser la connexion automatique des périphériques USB existants**.
4. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.
5. Modifiez le paramètre **Autoriser la connexion automatique des nouveaux périphériques USB**.
6. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.

# Périphériques composites et division de périphériques

June 27, 2024

Un périphérique USB composite est un périphérique unique qui agit comme plusieurs périphériques USB indépendants connectés à un ordinateur. Il possède un seul connecteur USB, mais il peut exposer plusieurs interfaces à l'ordinateur, chacune ayant son propre ensemble de fonctionnalités. Lorsqu'un utilisateur branche un périphérique USB composite, le périphérique hôte vérifie toutes les fonctions (interfaces) par rapport à chaque règle de stratégie. Si la première correspondance pour une fonction (interface) est une règle Deny, la règle est considérée comme définitive pour le périphérique composite et le périphérique est refusé. Si la première correspondance pour une fonction (interface) est une règle Allow, le périphérique hôte continue de faire correspondre les règles à la fonction suivante (interface). Le périphérique composite est autorisé si aucune fonction (interface) n'est refusée par une règle de stratégie. Si la correspondance définitive pour le périphérique composite est une règle Deny, le périphérique n'est disponible que sur le bureau local, sinon le périphérique est redirigé à distance vers le bureau virtuel. Si aucune correspondance n'est trouvée, les règles par défaut sont utilisées.




Nous pouvons diviser le périphérique composite en utilisant les règles appropriées de la stratégie Règles de redirection de périphérique (version 2) afin d'autoriser uniquement les fonctionnalités spécifiques d'un périphérique composite. Par exemple, vous souhaitez utiliser uniquement les fonctions HID d'une clé FIDO2, mais pas la fonctionnalité de la carte à puce. Dans ce cas, vous définissez les règles comme dans l'exemple suivant :

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Fonctions HID FIDO2 autorisées sur Yubikey 5.
2. Deny: VID=1050 PID=0407 split=01 intf=02 #Fonction de carte à puce bloquée sur Yubikey 5.

> **Conseil :**
>
> Lorsque vous créez des règles de stratégie, reportez-vous aux codes de catégories USB, disponibles sur le site Web USB.

### Configuration d'un pavé de signature

1. Installez le pilote de périphérique approprié sur l'hôte VDA.
2. Activez la **stratégie Redirection de périphérique USB client** dans **Citrix Web Studio**.
3. Modifiez la stratégie **Règles de redirection de périphérique USB client** (**version 2**).
    a) Définissez les informations **VID** et **PID** pour le pavé de signature qui doit être redirigé, puis cliquez sur **Enregistrer**. Par exemple : **Connect**: VID=056A PID=00A4 #STU-430
4. Modifiez la stratégie **Règles d'optimisation de périphérique USB client**.
    a) Définissez le mode ainsi que d'autres informations sur le périphérique. Par exemple : Mode=00000004 VID=056A PID=00A4 class=03 #Périphérique fonctionnant en mode capture
5. Modifiez la stratégie **Autoriser la connexion automatique des périphériques USB existants**.
6. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.
7. Modifiez la stratégie **Autoriser la connexion automatique des nouveaux périphériques USB**.
8. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.

Une fois ces stratégies définies dans la console Studio, les lancements de sessions suivants entraîneront la redirection automatique du périphérique et aucune action supplémentaire de l'utilisateur final ne sera requise.

> **Remarque :**
>
> Remplacez le VID et le PID par les VID et PID réels du périphérique à rediriger.

### Configuration du clavier Bloomberg à l'aide de la redirection USB

1. Activez la **stratégie Redirection de périphérique USB client** dans **Citrix Web Studio**.
2. Les claviers Bloomberg 5 sont définis par défaut dans les règles de redirection de périphérique USB client (version 2) et aucune action administrative supplémentaire n'est requise.
3. Modifiez la stratégie **Autoriser la connexion automatique des périphériques USB existants**.
4. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.
5. Modifiez la stratégie **Autoriser la connexion automatique des nouveaux périphériques USB**.
6. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.

Une fois ces stratégies définies dans la console Studio, les clés Bloomberg seront automatiquement présentées lors des sessions HDX suivantes et ne nécessiteront aucune action supplémentaire de l'utilisateur final.

### Configuration d'une clé FIDO2 à l'aide de la redirection USB

Citrix recommande d'utiliser la redirection FIDO2 pour utiliser les clés FIDO2 dans vos sessions HDX. Cependant, il peut arriver que vous deviez rediriger les clés FIDO2 à l'aide de la redirection USB. Il s'agit notamment de scénarios dans lesquels la redirection FIDO2 n'est pas disponible, car la fonctionnalité n'est pas prise en charge par le client, le VDA ou le système d'exploitation (par exemple, Windows Server 2016).

Il peut également arriver que plusieurs modes soient activés sur la clé, mais que vous ne souhaitiez autoriser qu'un sous-ensemble de ceux-ci dans vos sessions HDX. Par exemple, vous souhaitez autoriser FIDO2 et OTP, mais bloquer les cartes à puce.

Les étapes suivantes montrent comment configurer une clé FIDO2 à l'aide de la redirection USB (Yubikey vid=1050, pid=0407).

1. Activez la **stratégie Redirection de périphérique USB client** dans **Citrix Web Studio**.
2. Modifiez la stratégie **Règles de redirection de périphérique USB client** (version 2).
    a) Définissez le **VID** et le **PID** ainsi que la configuration du périphérique divisé pour la clé FIDO2 à rediriger dans la session, puis cliquez sur **Enregistrer**.
    b) **Connect**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Fonctions HID FIDO2 autorisées sur Yubikey 5.

c) **Deny**: VID=1050 PID=0407 split=01 intf=02 #Fonction de carte à puce bloquée sur Yubikey 5.

3. Modifiez la stratégie **Autoriser la connexion automatique des périphériques USB existants**.
4. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.
5. Modifiez la stratégie **Autoriser la connexion automatique des nouveaux périphériques USB**.
6. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.

Une fois ces stratégies définies dans la console Studio, les claviers FIDO2 seront automatiquement présentés lors des sessions HDX suivantes et ne nécessiteront aucune action supplémentaire de l'utilisateur final.

### Configuration d'une souris 3D à l'aide de la redirection USB

Actuellement, les pilotes SpaceMouse 3dConnexion ne sont pris en charge que sur les systèmes d'exploitation des postes de travail (Win 10 et Win 11). Ils ne fonctionnent pas sur le système d'exploitation du serveur. Voici les étapes à suivre pour configurer une SpaceMouse Enterprise sur le système d'exploitation d'un poste de travail (VID=046D, PID=C016).

1. Installez le dernier pilote Windows sur l'hôte VDA.
2. Activez la **stratégie Redirection de périphérique USB client** dans **Citrix Web Studio**.
3. Modifiez la stratégie **Règles de redirection de périphérique USB client** (**version 2**).

   a) Définissez les informations **VID** et **PID** pour le pavé de signature qui doit être redirigé, puis cliquez sur **Enregistrer**. Par exemple : **Connect**: VID=046D PID=C016 #SpaceMouse Enterprise

4. Modifiez la stratégie **Règles d'optimisation de périphérique USB client**.

   a) Définissez le mode ainsi que d'autres informations sur le périphérique. Par exemple : Mode=00000004 VID=046D PID=C016 class=03 #Périphérique fonctionnant en mode capture

5. Modifiez la stratégie **Autoriser la connexion automatique des périphériques USB existants**.
6. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.

7. Modifiez la stratégie **Autoriser la connexion automatique des nouveaux périphériques USB**.
8. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.

## Dépannage

June 27, 2024

Les étapes suivantes doivent être suivies pour résoudre les problèmes liés à la redirection USB :

1. Vérifiez que la configuration système requise est respectée pour la redirection USB. Notamment les versions de CVAD et CWA, les périphériques et les pilotes de périphériques pris en charge sur la plate-forme du système d'exploitation considérée.
2. Assurez-vous que la configuration est appropriée en fonction des versions des composants et des plates-formes utilisées dans votre environnement. Consultez la note dans la section Configuration de la redirection USB héritée pour plus de détails sur les composants qui nécessitent des paramètres de configuration hérités.
3. Vérifiez que le périphérique figure dans la liste des périphériques que le client a énumérés.

    a) Barre d'outils Préférences de Workspace : examinez les périphériques énumérés dans l'onglet Périphériques de la barre d'outils Préférences de Workspace (cliquez avec le bouton droit sur **l'icône CWA > Centre de connexion > Préférences**, puis cliquez sur l'onglet **Périphériques**).

    b) `CtxUsbDiagnostics.exe` (Recommandé) : exécutez cet outil dans une fenêtre d'invite de commandes. La sortie vous fournit des informations spécifiques au périphérique pour une session spécifique. Elle indique si un périphérique est redirigé ou non. Elle indique également si un ensemble de règles empêche la redirection du périphérique. Pour plus d'informations, reportez-vous à la section Outil de diagnostic.

    c) USBView ou autres outils tiers : exécutez un outil tiers tel que USBView sur le point de terminaison ou la machine cliente pour vous assurer que le périphérique est détecté sur le point de terminaison.

4. Si vous voyez le périphérique en cours d'énumération :

    a) Si vous voyez une règle Deny dans la sortie de l'outil CtxUsbDiagnostics pour un périphérique particulier, vérifiez les stratégies configurées dans Studio et assurez-vous qu'elles sont correctement définies dans la stratégie de la version 2. Si la règle Deny n'

apparaît pas dans la stratégie Studio, sélectionnez la stratégie côté client, puis les valeurs par défaut côté client pour trouver la règle Deny correspondante.

b) S'il n'y a pas de règle Deny dans la sortie de CtxUsbDiagnostics, l'application Citrix Workspace autorise la redirection du périphérique en cochant/cliquant sur le bouton approprié dans l'onglet Périphériques de la fenêtre Préférences (Périphériques > Gérer les périphériques). Une fois redirigés, les périphériques sont disponibles dans la session. Pour vous en assurer, vous pouvez vérifier Device Manager, USBView ou une application similaire dans la session HDX.

5. Si vous ne voyez pas le périphérique présenté pendant la session :

   a) Il est possible que le pilote de périphérique approprié ne soit pas installé correctement sur l'hôte VDA. Assurez-vous que les dernières versions des pilotes de périphériques sont correctement installées sur l'hôte VDA. Certains pilotes de périphériques ne sont pas pris en charge sur les machines Terminal Server. Assurez-vous que ce n'est pas le cas avec le périphérique que vous essayez de rediriger.

   b) Assurez-vous que le périphérique n'est pas utilisé sur le point de terminaison client. Certains périphériques nécessitent également l'installation de pilotes sur le point de terminaison client, ce qui peut empêcher leur redirection au cours de la session.

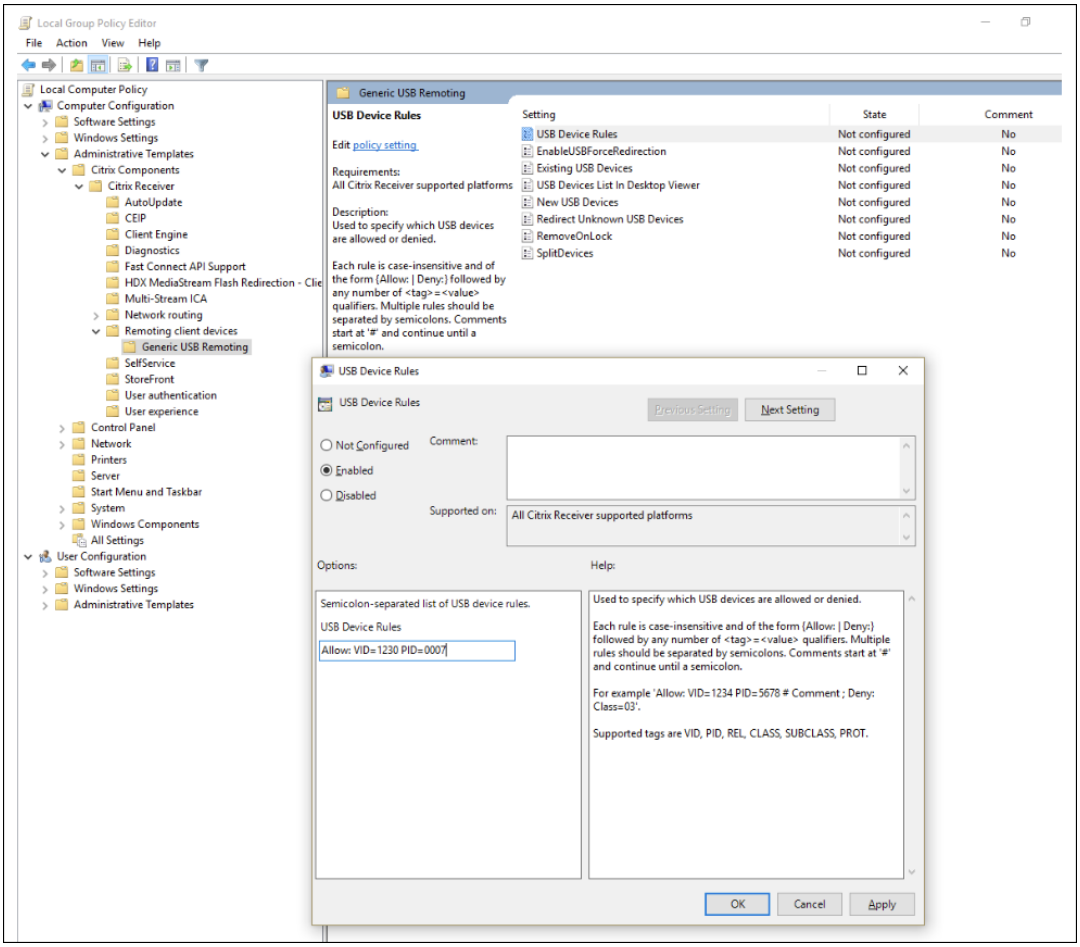
6. Vérifiez que les règles relatives à l'USB sont correctement définies sur le point de terminaison client :

   a) **Application Citrix Workspace pour Windows** :

      i. Vérifiez que la stratégie de groupe sur le client (ajoutez plus de détails et utilisez SS pour cela) est correctement définie et n'entre pas en conflit avec les règles définies dans Studio.

      ii. Validez ces règles par défaut dans le registre du client.




(`HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`)are appropriately set and not in conflict with the rules set in Studio and client group policy.

b) Application Citrix Workspace pour Linux : pour trier les problèmes liés à l'application Citrix Workspace pour Linux, consulter la documentation relative aux périphériques USB pour l'application Citrix Workspace pour Linux

c) Application Citrix Workspace pour Mac : pour trier les problèmes liés à l'application Citrix Workspace pour Mac, consultez Application Citrix Workspace pour Mac

> **Remarque :**
>
> - Sur TSVDA, les périphériques audio ne peuvent pas utiliser la redirection USB par défaut. La méthode recommandée pour utiliser ces périphériques consiste à utiliser le VC audio optimisé.
> - Parfois, les périphériques USB composites peuvent ne pas être automatiquement fractionnés même si une règle de redirection de périphérique correcte est définie pour les fraction-

ner. Ce problème se produit, car le périphérique est en mode faible consommation. Dans pareils cas, le périphérique enfant qui passe en mode faible consommation peut ne pas figurer dans la liste des périphériques. Pour résoudre ce problème, vous pouvez utiliser les solutions suivantes :

- Déconnectez la session, insérez le périphérique USB, puis reconnectez la session.

- Débranchez le périphérique USB, puis rebranchez-le. Cette action fait sortir le périphérique du mode faible consommation.

- Parfois, les paramètres de l'économiseur de batterie USB peuvent être activés pour optimiser l'autonomie de la batterie. Si le point de terminaison client se met en veille, le périphérique USB peut être déconnecté. Dans un tel scénario, vous devrez peut-être déconnecter, puis reconnecter le périphérique afin de le présenter à nouveau lors de la session.

### Journaux d'événements

Les administrateurs peuvent désormais surveiller les périphériques non autorisés que les utilisateurs pourraient tenter de rediriger et prendre les mesures appropriées. Voici certains des messages d'événement qui sont enregistrés dans l'observateur d'événements sur l'hôte VDA pour les périphériques autorisés à être redirigés et pour les périphériques qui ne le sont pas.

| | |
|---|---|
| **Id** | 1000 |
| **Name** | UsbEventAcceptDevice |
| **Severity** | Informational |
| **Facility** | System |
| **Text** | The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted. |
| **Comment** | This message logs the device info of a device redirected in an HDX session |

| | |
|---|---|
| **Id** | 1001 |
| **Name** | UsbEventPolicyRejectsDeviceV1 |
| **Severity** | Warning |
| **Facility** | System |
| **Text** | The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio. |
| **Comment** | This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule. |
| **Arguments** | |

| | |
|---|---|
| **Id** | 1002 |
| **Name** | UsbEventPolicyRejectsDeviceV2 |
| **Severity** | Warning |
| **Facility** | System |
| **Text** | The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio. |
| **Comment** | This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt. |
| **Arguments** | |

## Outil de diagnostic USB

June 27, 2024

`CtxUsbDiagnostics.exe` est un outil de ligne de commande sur le VDA permettant aux administrateurs Citrix de diagnostiquer et de résoudre rapidement les problèmes de redirection des périphériques USB rencontrés sur le client. Cet utilitaire collecte les informations essentielles pour évaluer et prioriser les problèmes de configuration associés aux périphériques USB connectés au client, dont la redirection échoue lors d'une session HDX.

## Exigences

### Hôte de la session

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Windows 11 21H2 ou version ultérieure
  - Windows Server 2016 ou version ultérieure
- VDA
  - Windows : Citrix Virtual Apps and Desktop version 2311 ou ultérieure

### Machine cliente

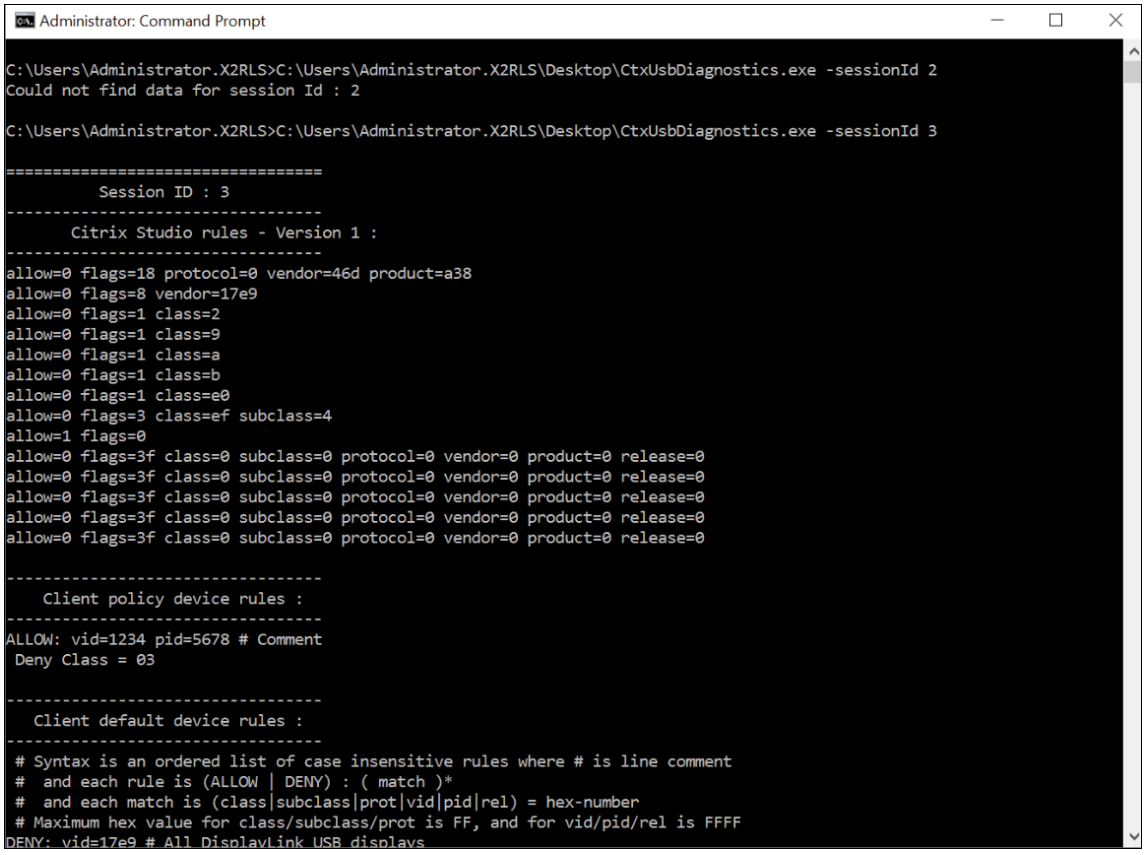
- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
- Application Workspace
  - Windows : version 2311 ou ultérieure

## À quoi sert cet outil ?

L'outil fournit actuellement :

- SessionID
- Les stratégies relatives aux périphériques VDA (règles relatives aux périphériques définies dans Studio)
- Les périphériques clients et stratégies relatives aux périphériques clients (règles relatives aux périphériques)
- Une liste des périphériques, leur état de redirection et les raisons pour lesquelles ils ont été autorisés ou refusés




> **Remarque :**
>
> L'administrateur peut consulter les informations relatives à le périphérique pour toutes les sessions actives.

### Informations affichées

- **Règles de Citrix Studio - Version 1/2**
  - Les règles DDC indiquent l'utilisation de l'ancienne stratégie « **Règles de redirection du périphérique USB client** » ou « **Règles de redirection du périphérique USB client (version 2)** » dans Studio. Les informations figurant dans cette section répertorient toutes les règles configurées par l'administrateur Citrix.

```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

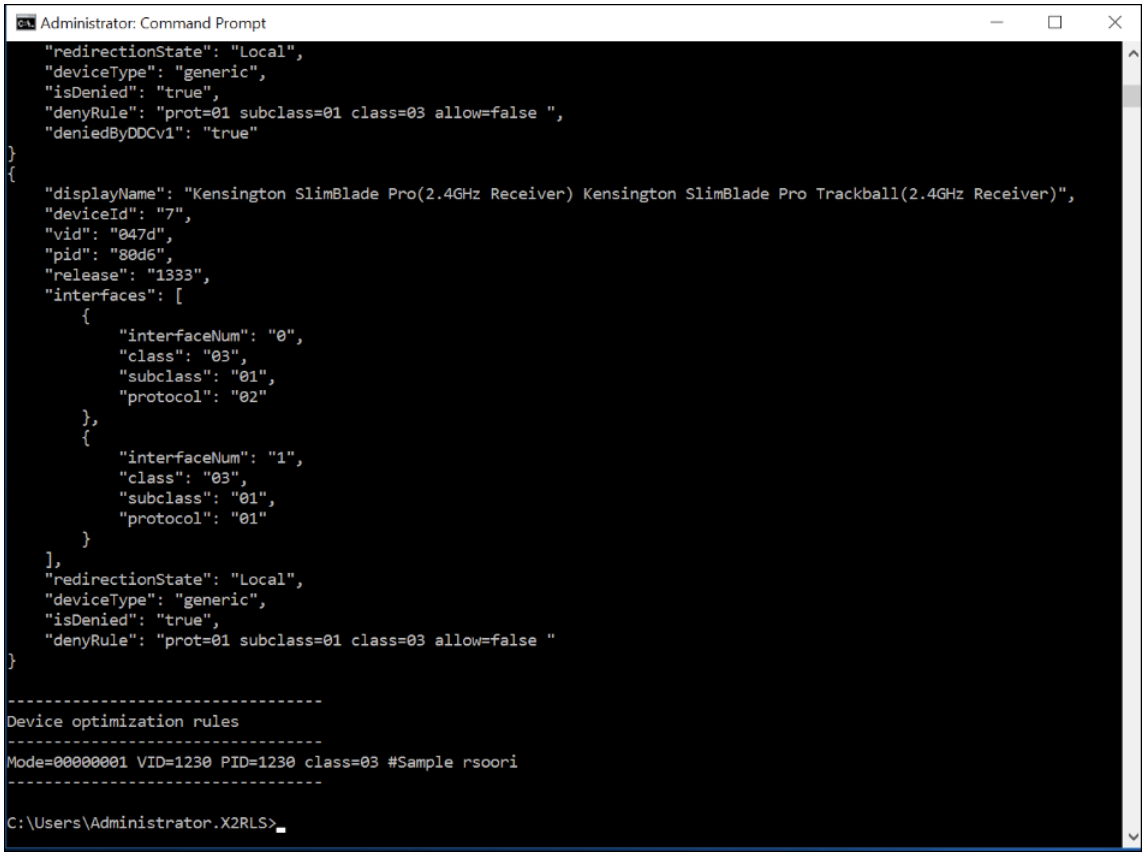
---------------------------------
          Session ID : 1
---------------------------------
       Citrix Studio rules - Version 2 :
---------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- **Règles relatives aux périphériques par défaut du client**
  - Cette section répertorie les règles définies dans le registre du client.

```
---------------------------------
  Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #  and each rule is (ALLOW | DENY) : ( match )*
 #  and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- **Règles d'optimisation de périphérique**
  - La section répertorie les règles d'optimisation de périphérique définies dans « Règles d'optimisation de périphérique USB client ».




## Liste des périphériques

Cette section répertorie des informations utiles sur chaque périphérique connecté au point de terminaison client, les informations matérielles, s'il est redirigé ou non, si la règle de redirection de périphérique correcte est définie ou non, etc.

| Nom de balise | Description |
|---|---|
| displayName | Répertorie le nom courant de le périphérique. |
| vid | ID du fournisseur |
| pid | ID du produit |
| Interfaces | Cette sous-section répertorie toutes les interfaces au cas où le périphérique composite aurait été scindé en plusieurs périphériques enfants. |
| InterfaceNum | Index du descripteur d'interface |
| class | Code de classe |

| Nom de balise | Description |
| --- | --- |
| subclass | Code de sous-classe |
| protocole | Protocole |
| redirectionState | **Local** indique que le périphérique n'est pas redirigé dans la session ICA. **Thissession** indique que le périphérique est redirigé dans la session ICA. **OtherSession** indique que le périphérique est redirigé vers une autre session ICA. |
| optiEnabled | La valeur **true** indique que le périphérique est optimisé. La valeur **false** indique que le périphérique n'est pas optimisé et que le transfert de données s'effectue via le canal virtuel USB. |
| deviceType | **generic** indique que le périphérique ne dispose pas d'un canal virtuel optimisé et que le trafic passe par le canal virtuel USB. **optimisé** signifie que le transfert de données associé au périphérique s'effectue via un canal virtuel dédié. |
| isDenied | **true** indique que le périphérique n'est pas redirigé en raison d'une règle de stratégie définie par l'administrateur. **false** indique que le périphérique est redirigé en raison de la stratégie appliquée. |
| denyRule | Ce champ est utile si isDenied est défini sur **true**. Il indique à l'administrateur la règle spécifique définie dans la stratégie qui empêche la redirection du périphérique. |

## Configuration de la redirection USB héritée

June 27, 2024

Si vous utilisez des composants antérieurs à la version 2212 ou si vous utilisez l'application Citrix Workspace pour Linux, suivez ce guide pour configurer la redirection USB dans votre environnement.

### Activation de la redirection USB générique

1. Ouvrez les **stratégies Citrix Web Studio** et cliquez sur l'onglet **Stratégies**.
2. Cliquez sur **Créer une stratégie**, puis développez **ICA > Stratégies de périphériques USB**.
3. Modifiez la **Stratégie de redirection de périphérique USB client**.
4. Sélectionnez **Autorisé**, puis cliquez sur **Enregistrer**.

### Création de règles de stratégie de redirection USB

Lorsque l'utilisateur tente de rediriger un périphérique USB vers Virtual Desktop, il est vérifié par rapport à chaque règle de stratégie USB jusqu'à ce qu'une correspondance soit trouvée. La première correspondance trouvée pour un périphérique est considérée comme définitive. Si la première correspondance est une règle Allow, le périphérique correspondant peut être redirigé vers le bureau virtuel. Si la première correspondance est une règle Deny, le périphérique correspondant n'est disponible que dans le bureau local. Si aucune correspondance n'est trouvée, les règles par défaut sont utilisées.

**Définition de la stratégie sur le Desktop Delivery Controller** :

1. Ouvrez les **stratégies Citrix Web Studio** et cliquez sur l'onglet **Stratégies**.
2. Cliquez sur **Créer une stratégie**, puis développez **ICA > Stratégies de périphériques USB**.
3. Modifiez les **Règles de redirection de périphérique USB client**.
4. Définissez la valeur en fonction des exemples fournis dans la description pour chaque périphérique USB qui doit être redirigé, puis cliquez sur Enregistrer.
   Par exemple :
   Allow: VID=056A PID=00A4 #STU-430
   Deny: Class=08 subclass=05 # Stockage de masse

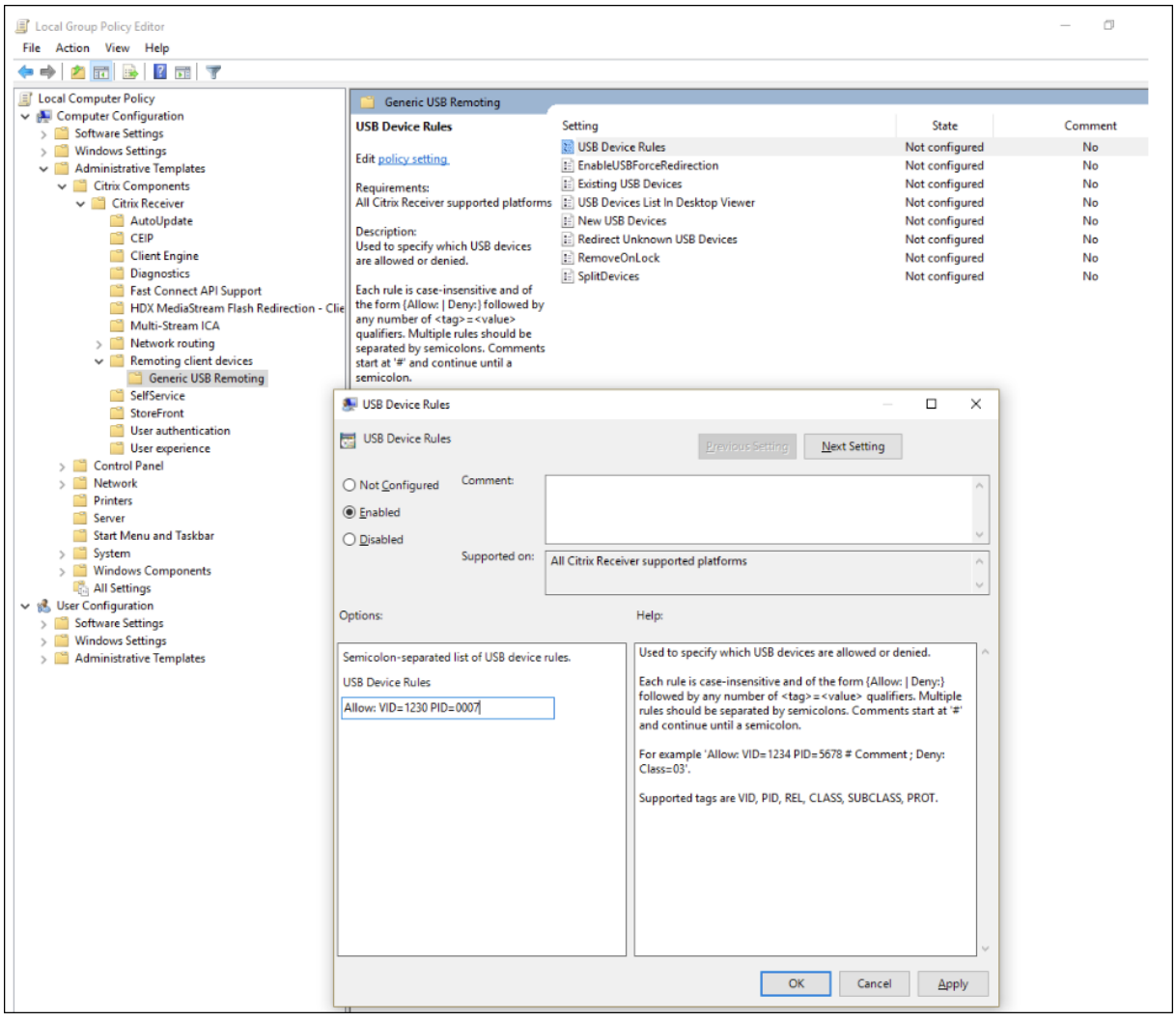
   > **Remarque :**
   >
   > Si un administrateur Citrix coche la case Utiliser valeur par défaut, puis clique sur Enregistrer, les règles par défaut se trouvent dans le registre suivant du VDA.
   >
   > **Attention :**
   >
   > Reportez-vous à la clause d'exclusion de responsabilité à la fin de cet article avant d'utiliser l'Éditeur du Registre.
   > `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

**Utilisation des objets de stratégie de groupe sur le client :**

1. Ouvrez l'**Éditeur de stratégie de groupe locale**, puis accédez à **Modèles d'administration > Composants Citrix > Citrix Receiver > Accès à distance des périphériques clients > Utilisation à distance de dispositifs USB génériques**.
2. Ouvrez le **paramètre Règles de périphériques USB** et activez-le. Ajoutez la règle de périphérique USB comme dans cet exemple.
   La règle Allow: VID=1230 PID=0007 autorise le périphérique avec l'ID de fournisseur 1230 et l'ID de produit 0007.

> **Remarque :**
>
> Utilisez la règle Allow: VID=xxxx PID=xxxx lorsqu'un périphérique spécifique doit figurer en haut de la liste des règles de périphériques.




> **Remarque :**
>
> Un outil comme USBView ou la barre d'outils de connexion peut être utilisé pour déterminer les

> détails du périphérique tels que le VID et le PID (inclure le SS ici).

### Configurer la redirection automatique des périphériques USB

Les périphériques USB sont automatiquement redirigés lorsque la prise en charge USB est activée. Les paramètres de préférences de l'utilisateur USB sont également définis pour la connexion automatique aux périphériques USB. Il n'est pas toujours recommandé de rediriger tous les périphériques USB. Les utilisateurs peuvent rediriger explicitement les périphériques de la liste de périphériques USB qui ne sont pas automatiquement redirigés. Pour empêcher l'ajout à la liste ou la redirection des périphériques USB, utilisez DeviceRules sur le point de terminaison du client ou sur la stratégie DDC.

Cette stratégie peut être définie sur le Desktop Delivery Controller, sur le client à l'aide d'un objet de stratégie de groupe, à l'aide des préférences de Citrix Workspace ou de l'onglet Connections sous CDViewer. Toutes ces méthodes sont décrites ci-dessous :

**Définition de la stratégie sur le Desktop Delivery Controller** :

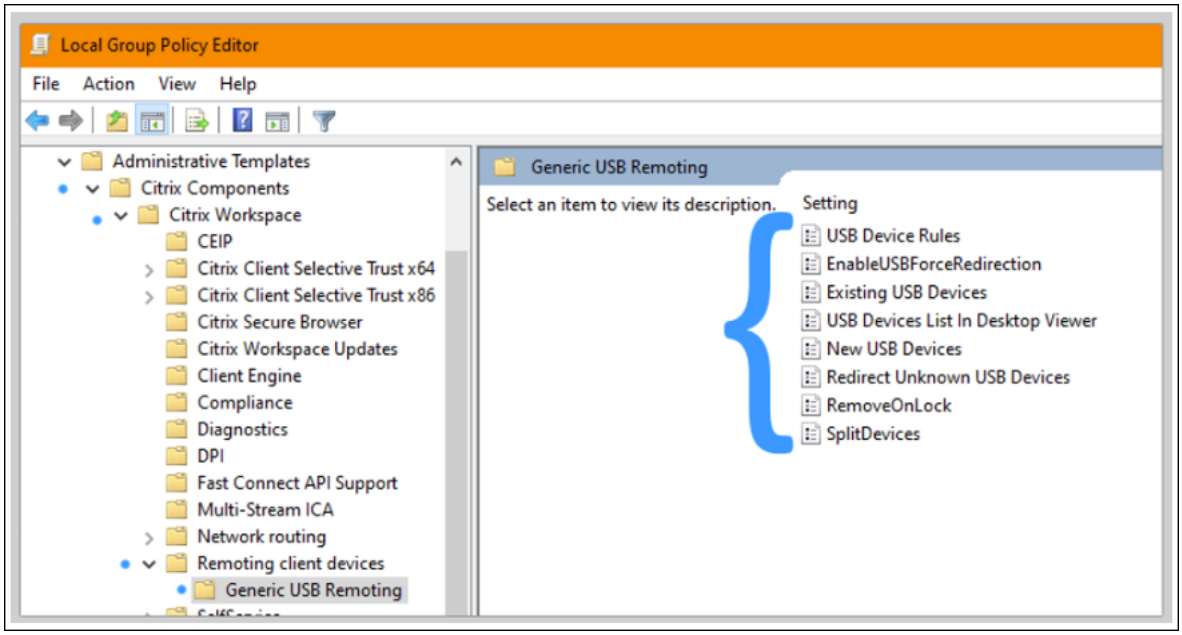
Le Desktop Delivery Controller peut définir deux stratégies pour autoriser la redirection automatique des périphériques USB : « Autoriser la connexion automatique des périphériques USB existants et Autoriser la connexion automatique des nouveaux périphériques USB »

1. Ouvrez les **stratégies Citrix Web Studio** et cliquez sur l'onglet **Stratégies**.
2. Cliquez sur **Créer une stratégie**, puis développez **ICA > Stratégies de périphériques USB**.
3. Modifiez le paramètre **Autoriser la connexion automatique des périphériques USB existants**.
4. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.
5. Modifiez le paramètre **Autoriser la connexion automatique des nouveaux périphériques USB**.
6. Désélectionnez la case **Utiliser valeur par défaut** et sélectionnez **Rediriger automatiquement les périphériques USB disponibles** dans le menu déroulant, puis cliquez sur **Enregistrer**.

**Utilisation des objets de stratégie de groupe sur le client :**

1. Ouvrez **Éditeur de stratégie de groupe local** et accédez à **Modèles d'administration > Composants Citrix > Citrix Receiver > Accès à distance des périphériques clients > Utilisation à distance de dispositifs USB génériques**.
2. Ouvrez **Nouveaux périphériques USB**, sélectionnez **Activé** et cliquez sur **OK**.
3. Ouvrez **Périphériques USB existants**, sélectionnez **Activé** et cliquez sur **OK**.




**À l'aide du Centre de connexion Citrix :**

1. Accédez à **Préférences de Citrix Workspace > Connexions**.
2. Assurez-vous que les options suivantes sont sélectionnées :

    a) Au démarrage d'une session, connecter les périphériques automatiquement
    b) Lorsqu'un nouveau périphérique est connecté alors qu'une session est en cours, connecter le périphérique automatiquement

3. Cliquez sur **OK**.

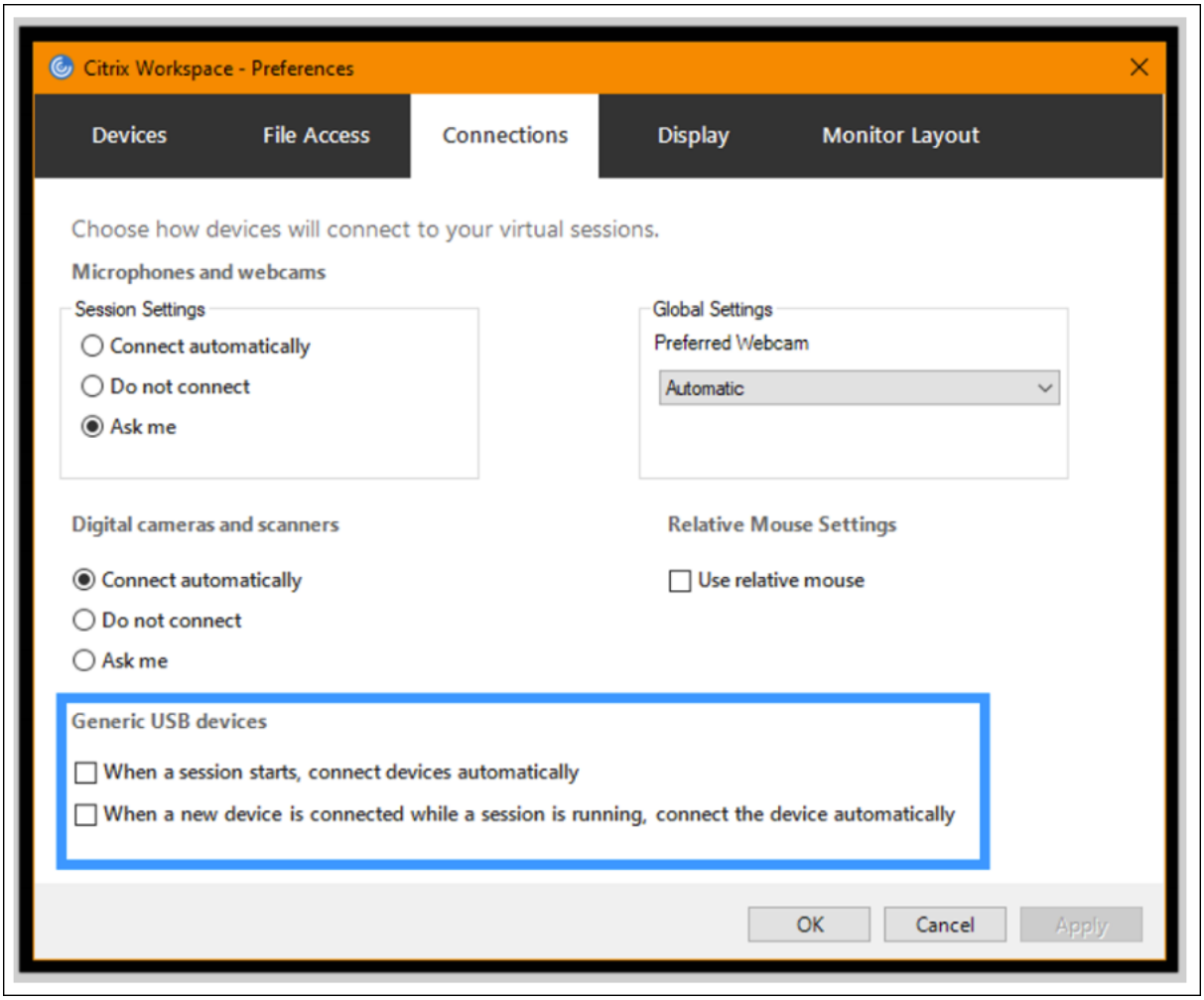
**À l'aide de la barre d'outils de connexion de CDViewer :**

1. Après le démarrage d'une session, cliquez sur le menu déroulant **CDViewer**, puis sélectionnez l'onglet **Préférences de Citrix Workspace > Connexions**.
2. Assurez-vous que les options suivantes sont sélectionnées :

    a) Au démarrage d'une session, connecter les périphériques automatiquement
    b) Lorsqu'un nouveau périphérique est connecté alors qu'une session est en cours, connecter le périphérique automatiquement

3. Cliquez sur **Appliquer** et **OK** pour enregistrer la stratégie.




Pour les configurations basées sur un client, les clés de registre sont définies sur la machine cliente à l'emplacement suivant :

> **Attention :**
>
> Reportez-vous à la clause d'exclusion de responsabilité à la fin de cet article avant d'utiliser l'Éditeur du Registre.
>
> `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

## Mappage des lecteurs clients (CDM)

June 27, 2024

Le mappage des lecteurs clients rend les lecteurs de stockage situés sur le point de terminaison client disponibles dans le cadre d'une session Citrix HDX afin de permettre le transfert de fichiers et de

dossiers du client vers l'hôte de la session, et vice versa. Cette fonctionnalité est activée par défaut avec des privilèges de lecture et d'écriture. Pour empêcher les utilisateurs d'ajouter ou de modifier des fichiers et dossiers sur les lecteurs clients mappés, activez le paramètre de stratégie **Accès en lecture unique sur le lecteur client**. Lorsque vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre **Redirection de lecteur client** est défini sur **Autorisé** et ajouté à la stratégie.

Par mesure de sécurité, les lecteurs de point de terminaison sont mappés par défaut sans autorisation d'exécution. Pour permettre aux utilisateurs d'exécuter des fichiers exécutables directement à partir des lecteurs clients mappés, modifiez la valeur de registre **ExecuteFromMappedDrive** dans l'hôte de la session. Pour plus de détails, consultez la section Disques clients mappés dans la section **Fonctionnalités HDX gérées via le registre** .

## Exigences

Les conditions requises pour utiliser le CDM sont les suivantes :

### Plan de contrôle Citrix

- Citrix Virtual Apps and Desktops 1912 ou versions ultérieures
- Citrix DaaS

### Hôte de la session

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Windows Server 2016 ou version ultérieure
  - Linux : veuillez vous référer à la configuration système requise pour Linux VDA
- VDA
  - Windows : Citrix Virtual Apps and Desktops 1912 ou versions ultérieures
  - Linux : veuillez vous référer à la documentation Linux VDA

### Machine cliente

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Linux : veuillez vous référer à l'application Workspace pour connaître la configuration système requisepour Linux.

### Stratégies associées

Reportez-vous à la section relatives aux références des paramètres de stratégie pour en savoir plus sur les paramètres du CDM.

### Scénarios double-hop (double tronçon)

Le CDM est pris en charge dans les scénarios double-hop. Par défaut, le lecteur du point de terminaison client est mappé à la session du second tronçon et les lecteurs du premier tronçon ne sont pas disponibles. Toutefois, cette fonctionnalité peut être définie de telle sorte que les lecteurs du premier tronçon sont mappés lors de la session du second tronçon au lieu des lecteurs du point de terminaison client.

Pour configurer cette fonctionnalité, modifiez la valeur de registre suivante :

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\
- Nom de la valeur : NativeDriveMapping
- Type de valeur : REG_SZ
- Données de valeur :
  - True : mappe les lecteurs de la session du premier tronçon lors de la session du second tronçon
  - False : mappe les lecteurs du point de terminaison du client lors de la deuxième session

> **Remarque :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

## Prise en charge des périphériques clients mobiles et à écran tactile

June 27, 2024

Citrix Virtual Apps and Desktops permet aux utilisateurs d'accéder à leurs applications et bureaux publiés à partir de périphériques clients mobiles et à écran tactile.

### Exigences

#### Plan de contrôle Citrix

- Citrix Virtual Apps and Desktops 1912 ou versions ultérieures
- Citrix DaaS

#### Hôte de la session

- Système d'exploitation
  - Windows 10 1903 ou version ultérieure
  - Windows 11 21H2 ou version ultérieure
  - Windows Server 2016 ou version ultérieure
- VDA
  - Windows : Citrix Virtual Apps and Desktops version 7.15 ou ultérieure

#### Machine cliente

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Windows 11 21H2 ou version ultérieure
- Application Citrix Workspace pour Windows version 1808 ou ultérieure

### Mode tablette pour périphériques à écran tactile avec Windows Continuum

Continuum est une fonctionnalité de Windows 10 qui s'adapte à la manière dont la machine cliente est utilisée. Lorsque le VDA détecte la présence d'un clavier ou d'une souris sur un client tactile, il place le client en mode bureau. Si un clavier ou une souris n'est pas détecté(e), le VDA place le client en mode tablette/mobile. Cette détection se produit lors de la connexion et de la reconnexion à une session, ainsi que pendant la session lorsque le clavier ou la souris est attaché ou détaché.

Par défaut, cette fonction est activée. Pour désactiver cette fonctionnalité, configurez les paramètres de stratégie Basculer en mode tablette.

Outre les exigences relatives aux périphériques à écran tactile mentionnées ci-dessus, les éléments suivants sont requis pour Windows Continuum :

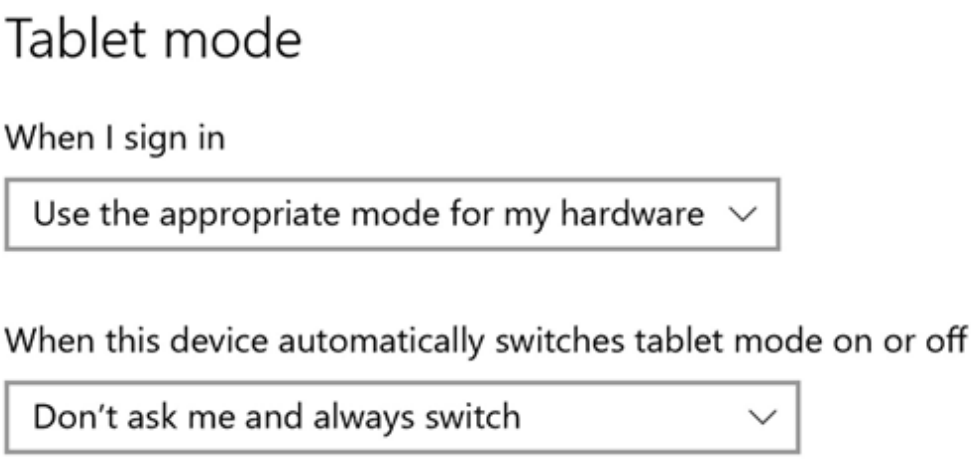
**XenServer (anciennement Citrix Hypervisor)**

- Citrix Hypervisor 8.2 ou version ultérieure
- Exécutez la commande CLI XenServer pour permettre le basculement ordinateur portable/tablette :
  **xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1**

> **Important :**
>
> La mise à jour de l'image de base pour un catalogue de machines existant après la modification du paramètre de métadonnées n'affecte pas les machines virtuelles précédemment provisionnées. Après avoir modifié l'image de base de la machine virtuelle XenServer, créez un catalogue, choisissez l'image de base et provisionnez une nouvelle machine MCS (Machine Creation Services).

**Hôte de la session**

- Système d'exploitation
  - Windows 10 1903 ou version ultérieure
  - Windows 11 21H2 ou version ultérieure
- VDA
  - Windows : version 7.16 ou ultérieure
  - **En raison des limites actuelles des configurations du système d'exploitation, l'utilisateur devra définir les options suivantes dans les menus déroulants après avoir démarré la première session ICA et redémarré le VDA :**
    - **Paramètres > Système > Mode tablette**
      - Utiliser le mode approprié à mon matériel
      - Ne pas me demander et toujours changer de mode



Le **mode tablette** offre une interface utilisateur qui est mieux adaptée aux écrans tactiles :

- Boutons légèrement plus grands.
- L'écran de démarrage et les applications que vous démarrez s'ouvrent en mode plein écran.
- La barre des tâches contient un bouton Précédent.
- Les icônes sont supprimées de la barre des tâches.

Vous avez accès à l'Explorateur de fichiers.

Windows 10 charge le pilote GPIO sur la machine virtuelle cible en fonction de ce BIOS mis à jour. Il est utilisé pour basculer entre les modes de tablette et de bureau dans la machine virtuelle.

L'application Citrix Workspace pour HTML5 ne prend pas en charge les fonctionnalités de Windows Continuum.

Le **mode bureau** offre l'interface utilisateur traditionnelle où vous interagissez de la même manière que sur un PC avec un clavier et une souris.

### Stylets Microsoft Surface Pro et Surface Book

Nous prenons en charge la fonctionnalité de stylet standard avec les applications Windows Ink. La prise en charge comprend le pointage, l'effacement, la pression du stylet, les signaux Bluetooth et d'autres fonctionnalités en fonction du microprogramme du système d'exploitation et du modèle de stylet. Par exemple, la pression du stylet peut atteindre 4096 niveaux. Cette fonctionnalité est activée par défaut.

Les exigences relatives à la prise en charge de la fonctionnalité de stylet sont les suivantes :

**Plan de contrôle Citrix**

- Citrix Virtual Apps and Desktops 1903 ou version ultérieure
- Citrix DaaS

**Hôte de la session**

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Windows 11 21H2 ou version ultérieure
  - Windows Server 2016 ou version ultérieure
- VDA
  - Windows : Citrix Virtual Apps and Desktops 1903 ou version ultérieure

**Machine cliente**

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Windows 11 21H2 ou version ultérieure
- Application Citrix Workspace pour Windows version 1902 ou ultérieure

Pour une démonstration de Windows Ink et de la fonctionnalité de stylet, cliquez sur ce graphique :


Pour désactiver ou activer cette fonctionnalité, consultez Stylets Microsoft Surface Pro et Surface Book dans la liste des fonctionnalités gérées via le Registre.

### Problèmes connus

Les problèmes connus liés à la prise en charge du stylet sont les suivants :

- En raison des limites du système d'exploitation de Windows Server 2k22, les utilisateurs ne pourront pas définir de raccourcis ni modifier les paramètres du stylet et de l'encre dans le Panneau de configuration lorsqu'ils se connectent à des applications ou à des bureaux du serveur 2k22.
- Les raccourcis de stylet ne sont pas respectés dans un client Windows 11 compatible avec le stylet en raison d'une limitation du système d'exploitation.

## Ports série

June 27, 2024

La plupart des nouveaux PC n'ont pas de ports série (COM) intégrés. Les ports sont faciles à ajouter en utilisant des convertisseurs USB. Les applications adaptées aux ports série impliquent souvent des capteurs, des contrôleurs, d'anciens lecteurs de chèques, etc. Certains périphériques USB avec port COM virtuel utilisent des pilotes spécifiques au fournisseur à la place des pilotes fournis par Windows (usbser.sys). Ces pilotes vous permettent de forcer le port COM virtuel du périphérique USB pour qu'il ne change pas même s'il est connecté à différentes prises USB. Cela peut être effectué à partir de **Gestionnaire de périphériques > Ports (COM & LPT) > Propriétés** ou de l'application qui contrôle le périphérique.

Le mappage des ports COM clients permet d'utiliser, au cours de sessions virtuelles, les périphériques connectés aux ports COM sur le point de terminaison de l'utilisateur. Vous pouvez utiliser ces mappages de la même façon que n'importe quel mappage réseau.

Pour chaque port COM, un pilote du système d'exploitation attribue un nom de lien symbolique tel que COM1 et COM2. Les applications utilisent ensuite le lien pour accéder au port.

> **Important :**
>
> Si un périphérique peut se connecter au point de terminaison en utilisant directement USB, cela ne signifie pas qu'il peut être redirigé à l'aide de la redirection USB générique. Certains périphériques USB fonctionnent comme des ports COM virtuels, auxquels les applications peuvent accéder de la même manière qu'un port série physique. Le système d'exploitation peut extraire les ports COM et les traiter comme des partages de fichiers. Deux protocoles courants pour COM virtuel sont CDC ACM ou MCT. Lorsqu'elles sont connectées via un port RS-485, les applications peuvent ne pas fonctionner du tout. Procurez-vous un convertisseur RS-485 vers RS232 pour utiliser RS-485 en tant que port COM.

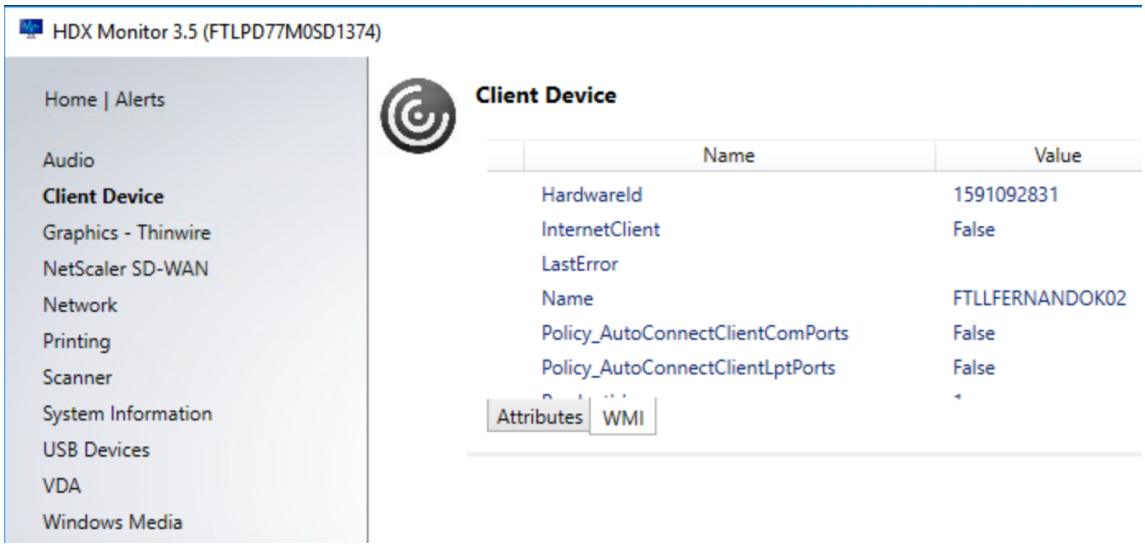
> **Important :**
>
> Certaines applications reconnaissent le périphérique (par exemple, un dispositif de signature numérique) de manière cohérente uniquement s'il est connecté à COM1 ou COM2 sur le poste de travail client.

### Mapper un port COM client à un port COM serveur

Vous pouvez mapper les ports COM clients à une session Citrix de trois manières :

- Stratégies Studio. Pour de plus amples informations sur les stratégies, consultez la section Paramètres de stratégie de redirection des ports.
- Invite de commande VDA.
- Outil de configuration Remote Desktop (Terminal Services).

1. Activez les stratégies **Studio Redirection du port COM client** et **Connecter automatiquement les ports COM du client**. Une fois qu'elles sont appliquées, certaines informations sont disponibles dans HDX Monitor.




2. Si la stratégie **Connecter automatiquement les ports COM du client** n'a pas réussi à mapper le port, vous pouvez mapper le port manuellement ou utiliser des scripts d'ouverture de session. Connectez-vous au VDA et, dans une fenêtre d'invite de commande, tapez :

   NET USE COMX: \\CLIENT\COMZ:

   Ou

   NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

   **X** est le numéro du port COM sur le VDA (les ports 1 à 9 sont disponibles pour le mappage). **Z** est le numéro du port COM client que vous voulez mapper.

Pour vérifier si l'opération a réussi, tapez **NET USE** dans une invite de commande VDA. La liste qui apparaît affiche les lecteurs, ports LPT et ports COM mappés.

```
C:\Windows\system32>net use
New connections will be remembered.


Status       Local     Remote                    Network

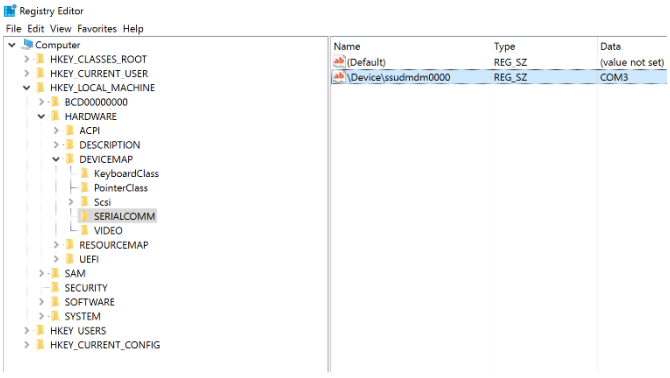
-------------------------------------------------------------------------------
             COM3      \\Client\COM3:            Citrix Client Network
```

3. Pour utiliser ce port COM dans une application ou un bureau virtuel, installez l'application de votre périphérique utilisateur et pointez-la vers le nom du port COM mappé. Par exemple, si le port COM1 du client est mappé sur le port COM3 du serveur, installez votre application de périphérique de port COM dans le VDA et pointez-la vers le port COM3 dans la session. Utilisez ce port COM comme vous utiliseriez n'importe quel autre port COM de la machine utilisateur.

> **Important :**
>
> Le mappage des ports COM n'est pas compatible avec l'interface TAPI. Vous ne pouvez pas mapper les périphériques TAPI (Windows Telephony Application Programming Interface) aux ports COM du client. TAPI définit un moyen standard pour les applications de contrôler les fonctions téléphoniques pour les données, les télécopies et les appels. TAPI gère la signalisation, y compris la numérotation, la réponse et la fin des appels, ainsi que des services supplémentaires tels que la mise en attente, le transfert et les conférences téléphoniques.

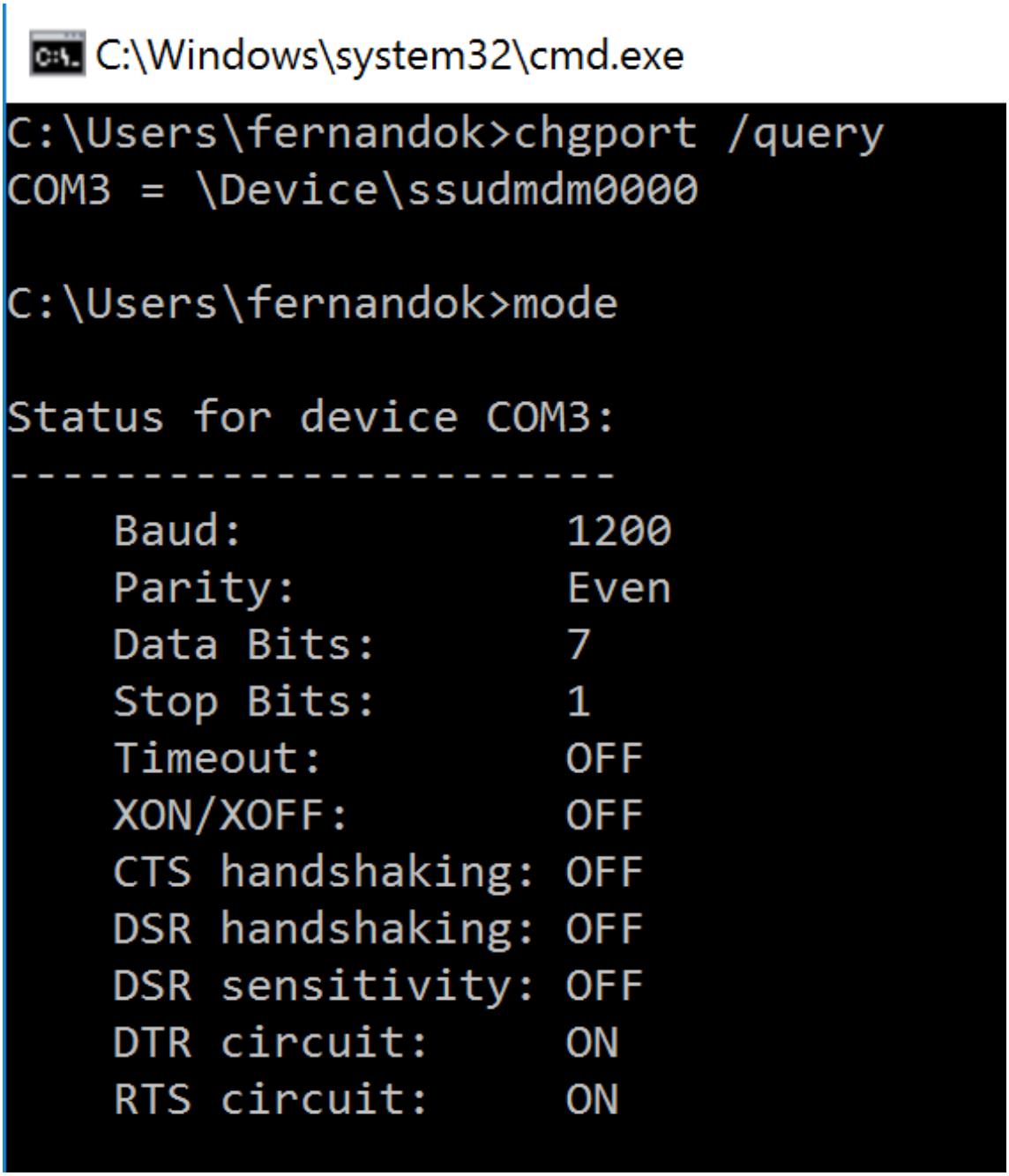
## Dépannage

1. Assurez-vous que vous pouvez accéder au périphérique directement depuis le point de terminaison, sans passer par Citrix. Tant que le port n'est pas mappé au VDA, vous n'êtes pas connecté à une session Citrix. Suivez les instructions de dépannage fournies avec le périphérique et vérifiez d'abord qu'il fonctionne localement.
   Lorsqu'un périphérique est connecté à un port COM série, une clé de registre est créée sur la ruche affichée ici :



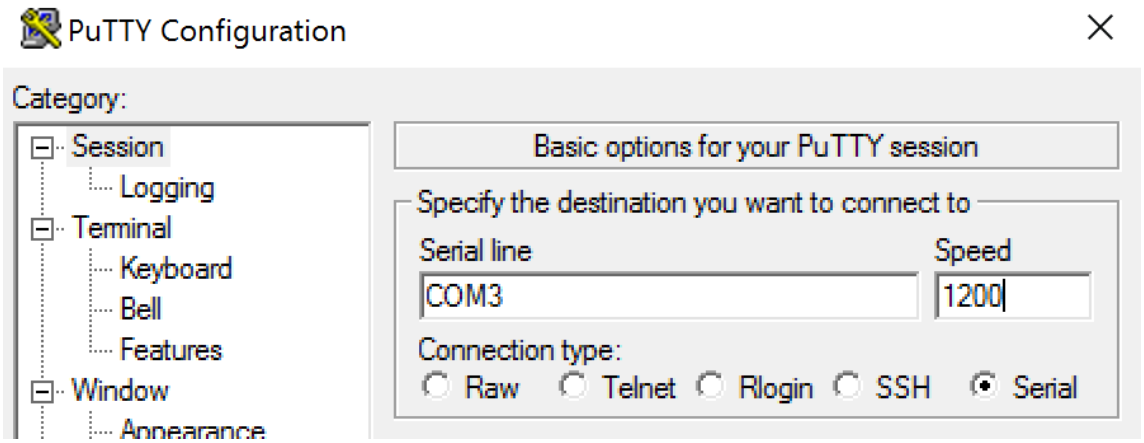

 

Vous pouvez également trouver ces informations à partir de l'invite de commande en exécutant **chgport /query**.




Si les instructions de dépannage du périphérique ne sont pas disponibles, essayez d'ouvrir une session PuTTY. Choisissez **Session** et dans **Serial line**, spécifiez votre port COM.




Vous pouvez exécuter **MODE** dans une fenêtre de commande locale. La sortie peut afficher le port COM utilisé et les données Baud/Parity/Data Bits/Stop Bits, dont vous avez besoin dans votre session PuTTY. Si la connexion PuTTY est réussie, appuyez sur **Entrée** pour voir le retour du périphérique. Quels que soient les caractères que vous tapez, ils peuvent être répétés à l'écran ou obtenir une réponse. Si cette étape échoue, vous ne pouvez pas accéder au périphérique à partir d'une session virtuelle.

2. Mappez le port COM local sur le VDA (en utilisant des stratégies ou **NET USE COMX: \\CLIENT\COMZ:**) et répétez les mêmes procédures PuTTY qu'à l'étape précédente, mais cette fois à partir du PuTTY du VDA. Si PuTTY échoue, affichant l'erreur **Unable to open connection to COM1. Unable to open serial port**, il est possible qu'un autre périphérique utilise COM1.

3. Exécutez **chgport /query**. Si le pilote série Windows intégré sur le VDA attribue automatiquement \Device\Serial0 à un port COM1 de votre VDA, procédez comme suit :
   A. Ouvrez CMD sur le VDA et tapez **NET USE**.

   B. Supprimez tout mappage existant (par exemple, COM1) sur le VDA.

   **NET USE COM1 /DELETE**

   C. Mappez le périphérique sur le VDA.

   **NET USE COM1: \\CLIENT\COM3:**

   D. Pointez votre application sur le VDA vers COM3.

   Enfin, essayez de mapper votre port COM local (par exemple, COM3) à un autre port COM sur le VDA (autre que COM1, par exemple COM3). Assurez-vous que votre application pointe vers celui-ci :
   **NET USE COM3: \\CLIENT\COM3**

4. Si maintenant vous voyez le port mappé, que PuTTY fonctionne mais qu'aucune donnée ne passe, il peut s'agir d'une condition de concurrence. L'application peut connecter et ouvrir le

port avant qu'il ne soit mappé, ce qui l'empêche d'être mappé. Essayez l'une des solutions suivantes :

- Ouvrez une deuxième application publiée sur le même serveur. Attendez quelques secondes que le port soit mappé, puis ouvrez l'application réelle qui essaie d'utiliser le port.
- Activez les stratégies de redirection de port COM à partir de l'Éditeur de stratégie de groupe dans Active Directory au lieu de Studio. Ces stratégies sont **Redirection du port COM client** et **Connecter automatiquement les ports COM du client**. Les stratégies appliquées de cette manière peuvent être traitées avant les stratégies Studio, garantissant que le port COM est mappé. Les stratégies Citrix sont transmises au VDA et stockées dans : `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- Utilisez ce script d'ouverture de session pour l'utilisateur ou au lieu de publier l'application, publiez un script .bat qui supprime d'abord tout mappage sur le VDA, remappe le port COM virtuel, puis lance l'application :

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200 (ou toute valeur requise)
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (ou toute valeur requise)
START C:\Program Files\<chemin de votre logiciel>\
```

5. Process Monitor de Sysinternals est l'outil de dernier recours. Lors de l'exécution de l'outil sur le VDA, trouvez et filtrez les objets comme COM3, picaser.sys, CdmRedirector, mais surtout <your_app>.exe. Toutes les erreurs peuvent apparaître comme Accès refusé ou similaire.

## Claviers spécialisés

June 27, 2024

### Claviers Bloomberg

> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous as-

> sumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Citrix Virtual Apps and Desktops prend en charge le clavier Starboard modèles 4 et 5 de Bloomberg (et le modèle 3 précédent). Ce clavier permet aux clients du secteur financier d'utiliser les fonctions spéciales du clavier pour accéder aux données du marché financier et effectuer des transactions rapidement.

> **Important :**
>
> Nous vous recommandons d'utiliser le clavier Bloomberg avec une seule session. Nous ne recommandons pas d'utiliser le clavier avec plusieurs sessions simultanées (un client pour plusieurs sessions).

Le clavier Bloomberg est un périphérique composite USB comprenant plusieurs périphériques USB dans une même coque physique :

- Clavier.
- Lecteur d'empreintes digitales.
- Périphérique audio avec touches pour augmenter et diminuer le volume et couper le haut-parleur et le microphone. Ce périphérique comprend un haut-parleur intégré, un microphone et une prise pour le microphone et le casque.
- Hub USB pour connecter tous ces périphériques au système.

**Exigences :**

- La session à laquelle l'application Citrix Workspace pour Windows se connecte doit prendre en charge les périphériques USB.
- Application Citrix Workspace 2207 pour Linux pour prendre en charge les modèles de clavier Bloomberg 5.
- Application Citrix Workspace 2109 pour Windows pour prendre en charge les modèles de clavier Bloomberg 5.
- Application Citrix Workspace 1808 pour Windows ou Citrix Receiver pour Windows 4.8 minimum pour prendre en charge les modèles de clavier Bloomberg 3 et 4.
- Application Citrix Workspace 1808 pour Windows ou Citrix Receiver pour Windows 4.12 minimum pour utiliser le mode KVM (deux câbles USB avec un câble routé via KVM) pour le modèle 4.

Pour plus d'informations sur la configuration des claviers Bloomberg sur l'application Citrix Workspace pour Windows, consultez la section Configuration des claviers Bloomberg.

Pour activer la prise en charge du clavier Bloomberg, reportez-vous à Claviers Bloomberg dans la liste des fonctionnalités gérées via le Registre.

**Vérifier la prise en charge :**

Pour déterminer si la prise en charge du clavier Bloomberg est activée dans l'application Citrix Workspace, vérifiez si Desktop Viewer signale correctement les périphériques du clavier Bloomberg.

Scénario de bureau :

Ouvrez Desktop Viewer. Si la prise en charge du clavier Bloomberg est activée, l'application Desktop Viewer affiche trois périphériques sous l'icône USB :

Pour le clavier Bloomberg 5 :

- Bloomberg LP Bloomberg Biometric Module
- Bloomberg LP Keyboard (Composite device with two interfaces)
- Bloomberg LP Keyboard Audio (Composite device with three interfaces)

Pour les claviers Bloomberg 3 et 4 :

- Bloomberg Fingerprint Scanner
- Bloomberg Keyboard Features
- Bloomberg LP Keyboard 2013

Scénario d'application transparente uniquement :

Ouvrez le menu **Centre de connexion** à partir de l'icône de la zone de notification Application Citrix Workspace. Si la prise en charge du clavier Bloomberg est activée, les trois périphériques apparaissent dans le menu **Périphériques**.

Une coche en regard de chacun de ces périphériques indique qu'ils sont connectés à la session.

## Webcams

June 27, 2024

### Streaming de webcam haute définition

Les webcams peuvent être utilisées par les applications de visioconférence s'exécutant au sein de la session virtuelle. L'application sur le serveur sélectionne le format et la résolution de la webcam en fonction des types de format pris en charge. Lors du démarrage d'une session, le client envoie les informations de la webcam au serveur. Choisissez une webcam dans l'application de visioconférence. Lorsque la webcam et l'application prennent toutes les deux en charge le rendu haute définition, l'application utilise une résolution haute définition. Nous prenons en charge les résolutions de webcam jusqu'à 1920x1080.

Cette fonctionnalité requiert Citrix Receiver pour Windows, version minimale 4.10. Pour obtenir la liste des plates-formes d'application Citrix Workspace qui prennent en charge la redirection de webcam HDX, consultez le tableau des fonctionnalités de l'application Citrix Workspace.

Pour plus d'informations sur le streaming de webcam haute définition, voir Conférences vidéo et compression vidéo de webcam HDX.

Vous pouvez utiliser une clé de Registre pour désactiver et activer la fonctionnalité, puis configurer une résolution spécifique. Pour de plus amples informations, consultez Diffusion de webcam haute définition et résolution de webcam haute définition dans la liste des fonctionnalités gérées via le registre.

## Graphiques

June 27, 2024

Les graphiques Citrix HDX comprennent un ensemble complet de technologies de codage et d'accélération graphique qui optimise la mise à disposition des applications riches en graphiques à partir de Citrix Virtual Apps and Desktops. Les technologies graphiques fournissent la même expérience qu'avec un bureau physique lors de l'utilisation à distance d'applications virtuelles qui sont riches en graphiques.

Vous pouvez utiliser une solution logicielle ou matérielle pour la restitution des graphiques. La restitution logicielle requiert une bibliothèque tierce appelée logiciel de rastérisation. Par exemple, Windows inclut le module de rastérisation WARP pour les graphiques DirectX. Vous pouvez souhaiter utiliser un autre outil de restitution logicielle. Le rendu matériel (accélération matérielle) nécessite un processeur graphique (GPU).

Les graphiques HDX proposent une configuration de codage par défaut qui est optimisée pour les cas d'utilisation les plus courants. Les administrateurs informatiques peuvent également utiliser des stratégies Citrix pour configurer divers paramètres liés aux graphiques afin de répondre aux différents besoins et proposer l'expérience utilisateur recherchée.

### Thinwire

Thinwire est la technologie de communication à distance d'écran par défaut de Citrix utilisée dans Citrix Virtual Apps and Desktops.

La technologie de communication à distance d'écran permet aux graphiques générés sur une machine d'être transmis, généralement via un réseau, vers une autre machine. Les graphiques sont créés par l'utilisateur, à l'aide de frappes clavier ou d'actions de souris par exemple.

### HDX 3D Pro

Les fonctions HDX 3D Pro dans Citrix Virtual Apps and Desktops vous permettent de mettre à disposition des bureaux et applications qui fonctionnent mieux avec un processeur graphique pour l'accélération matérielle. Ces applications incluent les applications graphiques 3D professionnelles basées sur OpenGL et DirectX. Le VDA standard prend uniquement en charge l'accélération GPU de DirectX.

### Accélération GPU pour OS mono-session Windows

En utilisant HDX 3D Pro, vous pouvez mettre à disposition des applications au graphisme intensif dans le cadre des applications ou bureaux hébergés sur des machines avec OS mono-session. HDX 3D Pro prend en charge les ordinateurs hôtes physiques, (y compris les bureaux, les lames et les stations de travail en rack) et les technologies de virtualisation GPU Passthrough et GPU offertes par les hyperviseurs XenServer, vSphere et Hyper-V (Passthrough uniquement).

À l'aide de la fonctionnalité GPU Passthrough, vous pouvez créer des machine virtuelle bénéficiant d'un accès exclusif à du matériel de traitement graphique dédié. Vous pouvez installer plusieurs processeurs graphiques sur l'hyperviseur et affecter individuellement des machine virtuelle à chacun de ces processeurs graphiques.

À l'aide de la virtualisation GPU, plusieurs machines virtuelles peuvent accéder directement à la puissance de traitement graphique d'un processeur graphique physique unique.

### Accélération GPU pour OS multi-session Windows

HDX 3D Pro permet aux applications exigeantes en ressources graphiques exécutées dans de sessions d'OS multi-session Windows d'être restituées sur le processeur graphique du serveur (GPU). En déplaçant la restitution OpenGL, DirectX, Direct3D et Windows Presentation Foundation (WPF) sur le processeur graphique du serveur, l'unité centrale du serveur n'est pas ralentie par la restitution des graphiques. Par ailleurs, le serveur est capable de traiter davantage de graphiques car la charge est partagée entre le processeur graphique et l'unité centrale.

### Framehawk

> **Important :**
>
> À partir de Citrix Virtual Apps and Desktops 7 1903, Framehawk n'est plus pris en charge. Utilisez Thinwire avec le transport adaptatif activé.

Framehawk est une technologie de communication à distance d'écran pour les travailleurs mobiles via des connexions sans fil haut débit (réseaux cellulaires Wi-Fi et 4G/LTE). Framehawk aide à résoudre les problèmes d'interférence spectrale et de propagation à trajets multiples et propose une expérience fluide et interactive aux utilisateurs d'applications et de bureaux virtuels.

### Filigrane de session textuel

Filigranes de session textuels pour dissuader et suivre le vol de données. Ces informations traçables apparaissent sur le bureau de la session comme un moyen de dissuasion pour ceux qui utilisent des

photographies et des captures d'écran pour voler des données. Vous pouvez spécifier un filigrane, qui est une couche de texte. Le filigrane peut s'afficher sur l'intégralité de l'écran de session sans modifier le contenu du document d'origine. Les filigranes de session textuels nécessitent un support VDA.

#### Taux de rafraîchissement adaptatif

Grâce aux nouvelles améliorations d'évolutivité, HDX adapte le taux de rafraîchissement des moniteurs virtuels à la stratégie FPS cible définie. Le taux de rafraîchissement adaptatif (ARR) est disponible pour les VDA mono-session et multi-sessions, et fonctionne à la fois pour les scénarios accélérés par unité de traitement graphique et sans unité de traitement graphique.

#### mode tolérance de pertes

Le mode de tolérance aux pertes est complètement retravaillé pour garantir que la session reste interactive lorsqu'une perte de paquets est détectée.

### Informations connexes

- HDX 3D Pro
- Accélération GPU pour OS mono-session Windows
- Accélération GPU pour OS multi-session Windows
- Framehawk
- Thinwire
- Filigrane de session textuel

## Plage dynamique élevée (HDR) 10 bits

June 27, 2024

Avec les sessions de bureau virtuel HDR (High Dynamic Range) 10 bits, vous pouvez utiliser des fonctionnalités d'encodage et de décodage améliorées pour générer des images et des vidéos de haute qualité avec une gamme étendue de couleurs, ainsi qu'un contraste et une luminosité accrus. Vous pouvez également personnaliser le niveau de luminance blanche, les données EDID (Extended Display Identification Data) et la qualité visuelle pour améliorer l'expérience utilisateur.

### Configuration système requise

Point de terminaison :

- Application Citrix Workspace pour Windows 2209 ou version ultérieure pour les unités de traitement graphique NVIDIA

- Les unités de traitement graphique NVIDIA avec prise en charge du décodage HEVC 10 bits (H.265) 444 sur le point de terminaison
- Moniteurs compatibles HDR 10 bits, le HDR 10 bits doit être activé sur tous les moniteurs à l'aide des paramètres d'affichage.

Serveur :

- Système d'exploitation mono-session Windows VDA 2209 ou version ultérieure pour les unités de traitement graphique NVIDIA, et VDA 2308 ou version ultérieure pour les unités de traitement graphique Intel
- GPU NVIDIA avec prise en charge du codage HEVC 444 10 bits sur le VDA

## Stratégies requises

Point de terminaison :

- Activer le décodage H.265 pour les graphiques

Serveur :

- Optimiser pour la charge des graphiques 3D
- Indicateur d'état graphique (facultatif)

## Configurations serveur

Le lancement d'une session Citrix sur un moniteur de point de terminaison 10 bits compatible HDR active la session HDR par défaut. Dans les sessions HDR multi-écrans, le HDR 10 bits doit être activé sur tous les moniteurs de points de terminaison. Les sessions HDR sont prises en charge en mode fenêtré et en mode plein écran.

### Niveau de blanc de référence

Ce paramètre définit le niveau de luminosité blanche par valeur nit. Il contrôle la luminosité relative de l'écran HDR dans la session. La valeur par défaut est de 80 nits. Définissez la clé de registre suivante pour définir une valeur nit différente :

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Type : REG_DWORD
- Nom : RefWhiteLevel

Pour activer ce paramètre, vous devez soit redimensionner votre session, soit la déconnecter, puis la relancer.

#### Remplacement EDID

Vous pouvez configurer le VDA pour utiliser la norme EDID du moniteur de point de terminaison pour vos sessions HDR. Cela vous permet d'utiliser pleinement les capacités d'affichage du moniteur en faisant correspondre la gamme de couleurs et la plage de luminosité. Par défaut, les sessions HDR adoptent un affichage compatible HDR1000.
Vous pouvez exporter l'EDID du moniteur de point de terminaison à l'aide de NVIDIA ou d'autres outils. Appliquez-le au VDA à l'aide de la clé de registre suivante :

- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Type : REG_BINARY
- Nom : EDIDOverride

Lorsque vous enregistrez l'EDID dans le registre, il ne doit pas contenir de virgules, d'espaces ou de caractères spéciaux. Pour activer l'EDID de remplacement, déconnectez-vous et lancez une nouvelle session.

#### Expérience visuelle sans perte

Activez les stratégies suivantes pour une expérience visuelle sans perte :

- Autoriser la compression visuelle sans perte
- Qualité visuelle : Toujours sans perte ou Sans perte si possible

Une fois les règles définies, vous pouvez contrôler la qualité de la session HDR à l'aide de l'indicateur d'état graphique en utilisant le curseur de qualité d'image ou en passant en mode pixel parfait.

#### Autoriser le verrouillage de l'écran de Windows

Vous pouvez utiliser cette stratégie pour autoriser tous les délais d'expiration de l'affichage Windows, y compris le verrouillage de l'écran, à appliquer à une session Citrix Virtual Desktop sur le système d'exploitation du poste de travail. Ce paramètre peut être défini à l'aide d'un objet de stratégie de groupe Citrix dans Citrix Studio.

Par défaut, lorsque ce paramètre n'est pas activé, un bureau Citrix Virtual Desktop ne répond pas aux délais d'expiration liés au verrouillage de session, à l'économiseur d'écran ou à la désactivation de l'affichage pendant une session active.

Lorsqu'un économiseur d'écran protégé par mot de passe est configuré sur un VDA de poste de travail, ce paramètre doit être activé pour permettre le verrouillage automatique de la session Citrix Virtual Desktop lorsque le délai d'expiration de l'économiseur d'écran est atteint.

L'activation de ce paramètre lorsqu'un délai d'expiration d'affichage est configuré sur le VDA entraîne l'expiration de ce délai, ce qui entraîne une session qui ne se met pas à jour tant que l'utilisateur ne reprend pas l'interaction avec la session. Par exemple, l'heure affichée n'est pas mise à jour et les nouvelles notifications ne sont pas affichées.

#### Autres considérations

- Vous pouvez lancer des sessions HDR 10 bits sur un maximum de quatre moniteurs sur les GPU virtuels.
- La session Citrix revient en mode 8 bits, non HDR, dans les cas suivants :
  - Si HDR 10 bits n'est pas activé sur l'un des moniteurs de point de terminaison
  - Activation du partage d'écran.
  - Configuration d'une disposition d'affichage virtuel sur le VDA.
  - Passer en mode pixel parfait sans définir la stratégie **Autoriser la compression visuelle sans perte**.

## HDX 3D Pro

June 28, 2024

Les fonctions HDX 3D Pro de Citrix Virtual Apps and Desktops vous permettent de mettre à disposition des bureaux et applications qui fonctionnent mieux avec un processeur graphique pour l'accélération matérielle. Ces applications incluent les applications graphiques 3D professionnelles basées sur OpenGL et DirectX. Le VDA standard prend uniquement en charge l'accélération GPU de DirectX.

Pour les paramètres de stratégie HDX 3D Pro, voir Optimiser pour la charge des graphiques 3D.

Toutes les applications Citrix Workspace prises en charge peuvent être utilisés avec des graphiques 3D. Pour de meilleures performances avec les charges de travail 3D complexes, les moniteurs haute résolution, les configurations multi-moniteurs et les applications haute fréquence d'images, nous recommandons d'utiliser la dernière version de l'application Citrix Workspace pour Windows et de l'application Citrix Workspace pour Linux. Pour obtenir des informations sur les versions prises en charge de l'application Citrix Workspace, consultez la section Étapes clés du cycle de vie de l'application Citrix Workspace.

Les applications professionnelles 3D exemples comprennent :

- les applications de conception, de fabrication et d'ingénierie assistées par ordinateur (CAD/-CAM/CAE) ;
- les logiciels GIS (Geographical Information System) ;

- PACS (Picture Archiving Communication System) pour l'imagerie médicale ;
- les applications utilisant les dernières versions OpenGL, DirectX, NVIDIA CUDA, OpenCL et WebGL ;
- les applications non graphiques consommant énormément de ressources informatiques qui utilisent des GPU NVIDIA CUDA (Compute Unified Device Architecture) pour le traitement en parallèle.

HDX 3D Pro offre la meilleure expérience utilisateur possible sur toute bande passante :

- Sur les connexions WAN : mettez à disposition une expérience utilisateur interactive sur des connexions WAN avec des bandes passantes de 1,5 Mbps seulement.
- Sur les connexions LAN : mettez à disposition une expérience utilisateur équivalente à celle d'un bureau local sur des connexions LAN.

  Vous pouvez remplacer les stations de travail complexes et coûteuses par des machines utilisateur beaucoup plus simples et transférer le traitement graphique vers le centre de données pour une gestion centralisée.

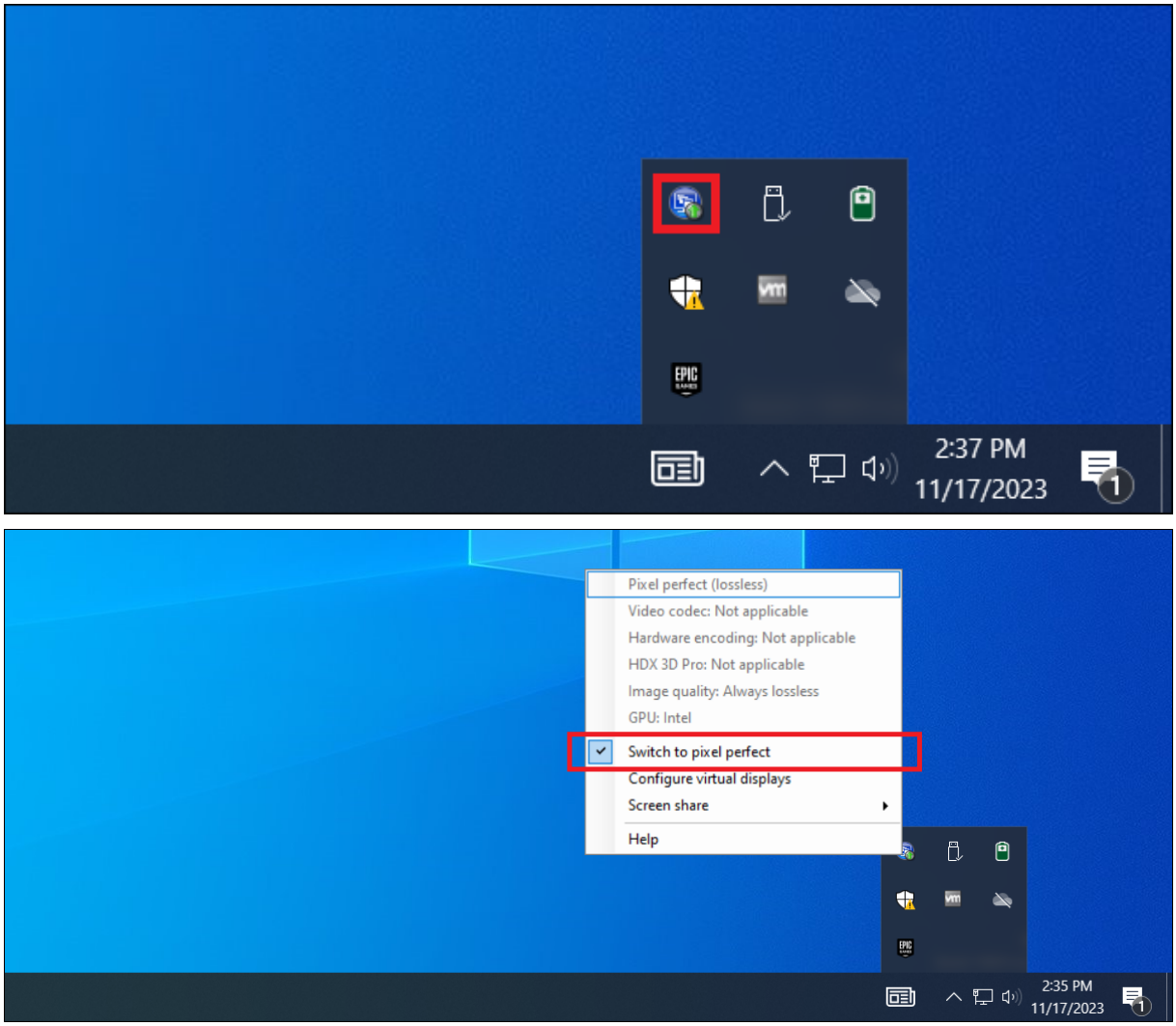
### Option de compression sans perte pour les cas d'utilisation spécialisés

HDX 3D Pro offre également un codec UC sans perte pour prendre en charge les applications pour lesquelles les graphiques gourmands en pixels sont nécessaires, comme l'imagerie médicale. La véritable compression sans perte est recommandée uniquement pour les scénarios d'utilisation spécifiques car elle consomme davantage de ressources réseau et de traitement.

Lors de l'utilisation de la compression sans perte :

- L'indicateur sans perte de l'indicateur d'état de graphique, une icône dans la zone de notification, avertit l'utilisateur si l'écran affiché est une trame avec ou sans perte. Cette icône est utile lorsque le paramètre de stratégie **Qualité visuelle** spécifie **Sans perte si possible**. L'indicateur sans perte devient vert lorsque les images envoyées sont sans perte.




- Le commutateur sans perte permet à l'utilisateur de passer en mode **Toujours sans perte** à tout moment dans la session. Pour sélectionner ou désélectionner le **Mode sans perte** à tout moment au cours d'une session, cliquez avec le bouton droit sur l'icône et cliquez sur **Basculer vers au pixel près** ou utilisez le raccourci ALT + MAJ + 1.
  - Pour la compression sans perte : HDX 3D Pro utilise le codec sans perte pour la compression quel que soit le codec sélectionné au travers de la stratégie.
  - Pour la compression avec perte : HDX 3D Pro utilise le codec original, soit celui par défaut, soit celui sélectionné via la stratégie.

    les paramètres du commutateur Sans perte ne sont pas conservés pour les sessions ultérieures. Pour utiliser le codec sans perte pour chaque connexion, sélectionnez **Toujours sans perte** dans le paramètre de **Stratégie de qualité visuelle**.

Vous pouvez remplacer le raccourci par défaut, ALT+MAJ+1, pour sélectionner ou désélectionner Sans perte dans une session. Configurez un nouveau paramètre de registre à l'adresse `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`.

- Nom : HKEY_LOCAL_MACHINE_HotKey, Type : chaîne

| | | | | |
|---|---|---|---|---|
| Le format pour configurer une combinaison de raccourcis est C=0 | 1, A=0 | 1, S=0 | 1, W=0 | 1, K = Val. Les clés doivent être séparées par une virgule (,). L'ordre des touches n'est pas important. |

-
- A, C, S, W et K représentent des touches, où C=Contrôle, A=ALT, S=MAJ, W=Win et K=une touche valide. Les valeurs autorisées pour K sont 0-9, a-z, et tout code clavier virtuel.
- Par exemple :
  pour F10, définissez K=0x79
  Pour Ctrl + F10, définissez C=1, K=0x79
  Pour Alt + A, définissez A=1, K=a ou A=1, K=A ou K=A, A=1
  pour Ctrl + Alt + 5, définissez C=1, A=1, K=5 ou A=1, K=5, C=1
  pour Ctrl + Shift F5, définissez A=1, S=1, K=0x74

### Optimiser l'expérience utilisateur de HDX 3D Pro

Lorsque plusieurs utilisateurs partagent une connexion disposant d'une bande passante limitée (par exemple dans une succursale), nous vous recommandons d'utiliser le paramètre de stratégie Limite de bande passante de session générale pour limiter la bande passante disponible pour chaque utilisateur. L'utilisation de ce paramètre évite les trop fortes fluctuations de la bande passante au fur et à mesure que les utilisateurs ouvrent une session ou se déconnectent. Comme HDX 3D Pro s'adapte automatiquement pour utiliser toute la bande passante disponible, de fortes variations de celle-ci pendant les sessions des utilisateurs peuvent avoir un impact négatif sur les performances.
Ainsi, si 20 utilisateurs partagent une connexion de 60 Mbps, la bande passante disponible pour chaque utilisateur peut varier entre 3 Mbps et 60 Mbps en fonction du nombre d'utilisateurs simultanés. Pour optimiser l'expérience utilisateur dans ce scénario, déterminez la bande passante requise par utilisateur aux heures de pointe et limitez en permanence les utilisateurs à cette valeur.
Pour les utilisateurs de souris 3D, nous vous recommandons d'augmenter la priorité du canal virtuel Generic USB Redirection à 0. Pour plus d'informations sur la modification de la priorité du canal virtuel, consultez l'article CTX128190 du centre de connaissances.
Utilisez l'outil HDX Monitor pour valider l'opération et la configuration des technologies de visualisation HDX et pour diagnostiquer et résoudre les problèmes HDX. L'outil est disponible dans le dossier **Support** du support d'installation de Citrix Virtual Apps and Desktops.

# Accélération GPU pour OS multi-session Windows

June 27, 2024

Citrix Virtual Apps and Desktops prend en charge les applications gourmandes en ressources graphiques exécutées dans des sessions de système d'exploitation multi-sessions Windows pour être affichées sur l'unité de traitement graphique (GPU) du serveur. En déplaçant la génération OpenGL, DirectX, Direct3D et Windows Presentation Foundation (WPF) vers le GPU du serveur, celui-ci peut être utilisé plus efficacement.

Windows Server étant un système d'exploitation multi-utilisateurs, un processeur graphique auquel accède Citrix Virtual Apps peut être partagé par de multiples utilisateurs sans qu'une virtualisation du GPU (vGPU) ne soit nécessaire.

Soyez prudent avec les procédures qui impliquent la modification du registre : une modification incorrecte du registre peut entraîner des problèmes graves pouvant nécessiter une réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

## Partage GPU

Le partage GPU permet le rendu matériel GPU des applications OpenGL et DirectX dans les sessions de bureau à distance. Il a les caractéristiques suivantes :

- Peut être utilisée sur des machines bare metal ou virtuelles pour améliorer la scalabilité et les performances des applications.
- Permet plusieurs sessions simultanées pour partager les ressources GPU (la plupart des utilisateurs ne requièrent pas les performances de restitution d'un processeur graphique dédié).
- Ne requiert aucun paramètre spécial.

Un GPU peut être affecté à la machine virtuelle Windows Server en mode pass-through complet ou GPU virtuel (vGPU) suivant les exigences de l'hyperviseur et du fournisseur de GPU. Les déploiements bare metal sur les machines physiques Windows Server sont également pris en charge.

Le partage GPU ne dépend pas d'une carte graphique spécifique.

- Pour les machines virtuelles, sélectionnez une carte graphique compatible avec l'hyperviseur utilisé. Pour obtenir une liste des composants matériels compatibles avec XenServer, consultez la page Liste de compatibilité matérielle de l'hyperviseur.

- Lors de l'exécution sur des machines bare metal, il est recommandé de n'activer qu'une seule carte vidéo par système d'exploitation. Si plusieurs processeurs graphiques sont installés sur le matériel, désactivez-les tous sauf un à l'aide de Device Manager.

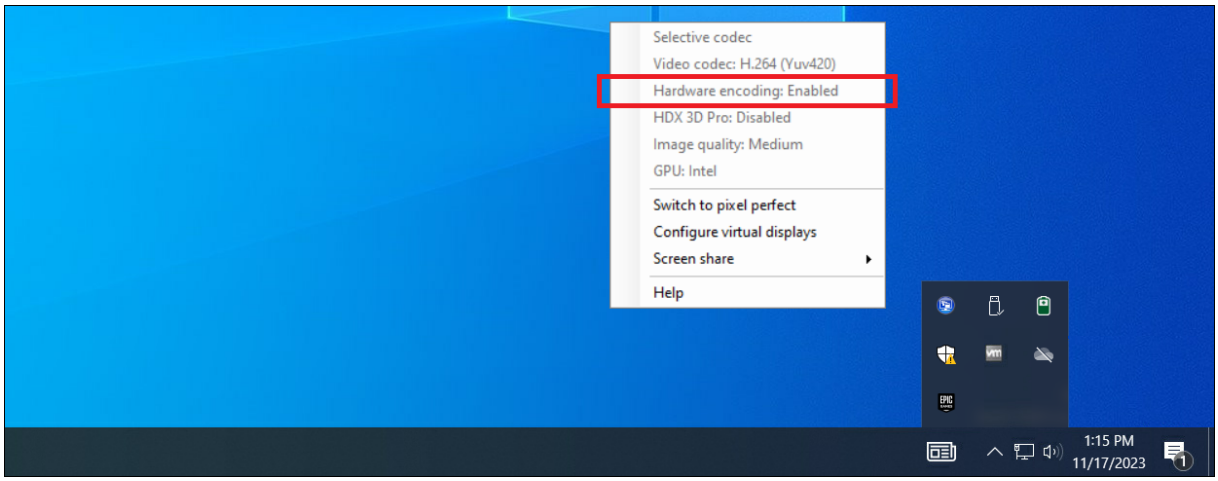
La scalabilité utilisant le partage GPU dépend de plusieurs facteurs :

- les applications étant exécutées ;
- la quantité de mémoire vive vidéo qu'elles consomment ;
- la puissance de traitement de la carte graphique.

certaines applications gèrent les insuffisances de RAM vidéo mieux que d'autres. Si le matériel devient surchargé, cela peut provoquer une instabilité ou un vidage du pilote de la carte graphique. Limitez le nombre d'utilisateurs simultanés pour éviter de tels problèmes.

- Accès à un encodeur vidéo haute performance pour les GPU NVIDIA et les processeurs graphiques Intel Iris Pro. Cette fonctionnalité est contrôlée par un paramètre de stratégie (activé par défaut) et autorise l'utilisation du codage matériel pour l'encodage H.264 (le cas échéant). Si ce matériel n'est pas disponible, le VDA utilise le codage basé sur l'UC avec le codec vidéo logiciel. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie des graphiques.

L'indicateur d'état graphique peut être utilisé pour confirmer que l'accélération du GPU se produit :




### Restitution DirectX, Direct3D et WPF

La restitution DirectX, Direct3D et WPF sont uniquement disponibles sur les serveurs dotés d'un processeur graphique prenant en charge les versions DDI 9ex, 10 ou 11.

- Sur Windows Server 2016 et versions ultérieures, les sessions de Services Bureau à distance (RDS) des sessions sur le serveur hôte de session Bureau à distance utilisent le pilote de rendu de base Microsoft en tant qu'adaptateur par défaut. Pour utiliser le processeur graphique dans

les sessions de services Bureau à distance dans Windows Server 2016 et versions ultérieures, activez le paramètre **Utiliser la carte graphique matérielle par défaut pour toutes les sessions des services Bureau à distance** dans la stratégie de groupe **Stratégie ordinateur local** > **Configuration ordinateur** > **Modèles d'administration** > **Composants Windows** > **Services Bureau à distance** > **Hôte de la session Bureau à distance** > **Environnement de session à distance**.

- Pour activer les applications WPF pour effectuer la restitution à l'aide du GPU du serveur, créez les paramètres dans le registre du serveur exécutant les sessions OS multi-session Windows. Pour plus d'informations sur le paramètre de Registre, reportez-vous à Rendu Windows Presentation Foundation (WPF) dans la liste des fonctionnalités gérées via le Registre.

### Accélération de processeur graphique pour les applications CUDA ou OpenCL

L'accélération GPU d'applications CUDA et OpenCL exécutées dans une session utilisateur est désactivée par défaut.

Pour utiliser les fonctionnalités d'évaluation d'accélération CUDA, activez les paramètres de registre. Pour plus d'informations, reportez-vous à Accélération de processeur graphique pour les applications CUDA ou OpenCL dans la liste des fonctionnalités gérées via le Registre.

## Accélération GPU pour OS mono-session Windows

June 27, 2024

Avec HDX 3D Pro, vous pouvez mettre à disposition des applications au graphisme intensif dans le cadre des applications ou bureaux hébergés sur des machines avec OS mono-session. HDX 3D Pro prend en charge les ordinateurs hôtes physiques, (y compris les bureaux, les lames et les stations de travail en rack) et les technologies de virtualisation GPU Passthrough et GPU offertes par les hyperviseurs XenServer, vSphere, Nutanix et Hyper-V (Passthrough uniquement).

HDX 3D Pro offre les fonctionnalités suivantes :

- Compression approfondie H.264 ou H.265 adaptative pour des performances de réseau étendues et sans fil optimales. HDX 3D Pro utilise la compression H.264 plein écran basée sur l'UC en tant que technique de compression par défaut pour le codage. Le codage matériel avec H.264 est utilisé avec les cartes NVIDIA, Intel et AMD qui prennent en charge NVENC. Le codage matériel avec H.265 est utilisé avec les cartes NVIDIA qui prennent en charge NVENC.
- Option de compression sans perte pour les cas d'utilisation spécialisés. HDX 3D Pro offre également un codec UC sans perte pour prendre en charge les applications pour lesquelles

les graphiques gourmands en pixels sont nécessaires, comme l'imagerie médicale. La véritable compression sans perte est recommandée uniquement pour les scénarios d'utilisation spécifiques car elle consomme davantage de ressources réseau et de traitement.

> **Attention :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

- Prise en charge de plusieurs moniteurs haute résolution. Jusqu'à 8 écrans 4K sont pris en charge pour les machines avec système d'exploitation mono-session. Les utilisateurs peuvent organiser leurs moniteurs selon n'importe quelle configuration et peuvent combiner des moniteurs ayant différentes résolutions et orientations. Le nombre de moniteurs n'est limité que par les capacités du processeur graphique de l'ordinateur hôte, de la machine utilisateur et de la bande passante disponible. HDX 3D Pro prend en charge toutes les résolutions de moniteur et n'est limité que par les capacités du processeur graphique sur l'ordinateur hôte.
- Résolution dynamique. Vous pouvez redimensionner la fenêtre de bureau ou d'application virtuel(le) sur n'importe quelle résolution. **Remarque :** la seule méthode prise en charge permettant de changer la résolution consiste à redimensionner la fenêtre de session VDA. La modification de la résolution dans une session VDA (à l'aide de **Panneau de configuration > Apparence** et **Personnalisation > Affichage > Résolution d'écran) n'est pas prise en charge**.
- Prise en charge de l'architecture NVIDIA vGPU. HDX 3D Pro prend en charge les cartes NVIDIA vGPU. Pour plus d'informations, consultez NVIDIA vGPU pour la technologie GPU Passthrough et le partage de GPU. NVIDIA vGPU permet à plusieurs machines virtuelles d'avoir un accès direct simultané à un GPU unique physique, à l'aide des mêmes pilotes graphiques NVIDIA qui sont déployés sur des systèmes d'exploitation non virtualisés.
- Prise en charge de VMware vSphere et VMware ESX à l'aide de l'accélération graphique virtuelle (vDGA) : vous pouvez utiliser HDX 3D Pro avec vDGA pour les RDS et les charges de travail VDI.
- Prise en charge pour VMware vSphere/ESX.
- Prise en charge de Microsoft Hyper-V à l'aide de la technologie DDA de Windows Server 2016.
- Prise en charge des graphiques pour centres de données avec les processeurs Intel Xeon de la gamme E3 et les unités de traitement graphique Intel Data Center de la série Flex. Pour plus d'informations, consultez https://www.intel.com/content/www/us/en/products/details/discrete-gpus/data-center-gpu/flex-series.html.
- Prise en charge des unités de traitement graphique AMD.

> Remarque :
>
> La prise en charge de AMD MxGPU (virtualisation de l'unité de traitement graphique) fonctionne uniquement avec des vGPU VMware vSphere. Citrix Hypervisor et Hyper-V sont pris en charge avec la technologie GPU Passthrough. Pour plus d'informations, consultez https://www.amd.com/en/graphics/workstation-virtual-graphics.

- Accès à un encodeur vidéo hautes performances pour les unités de traitement graphique NVIDIA, AMD et Intel. Un paramètre de stratégie (activé par défaut) contrôle cette fonctionnalité. La fonctionnalité permet d'utiliser le codage matériel pour l'encodage H.264, H.265, ou AV1 (le cas échéant). Si ce matériel n'est pas disponible, le VDA utilise le codage basé sur l'UC avec le codec vidéo logiciel. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie des graphiques.

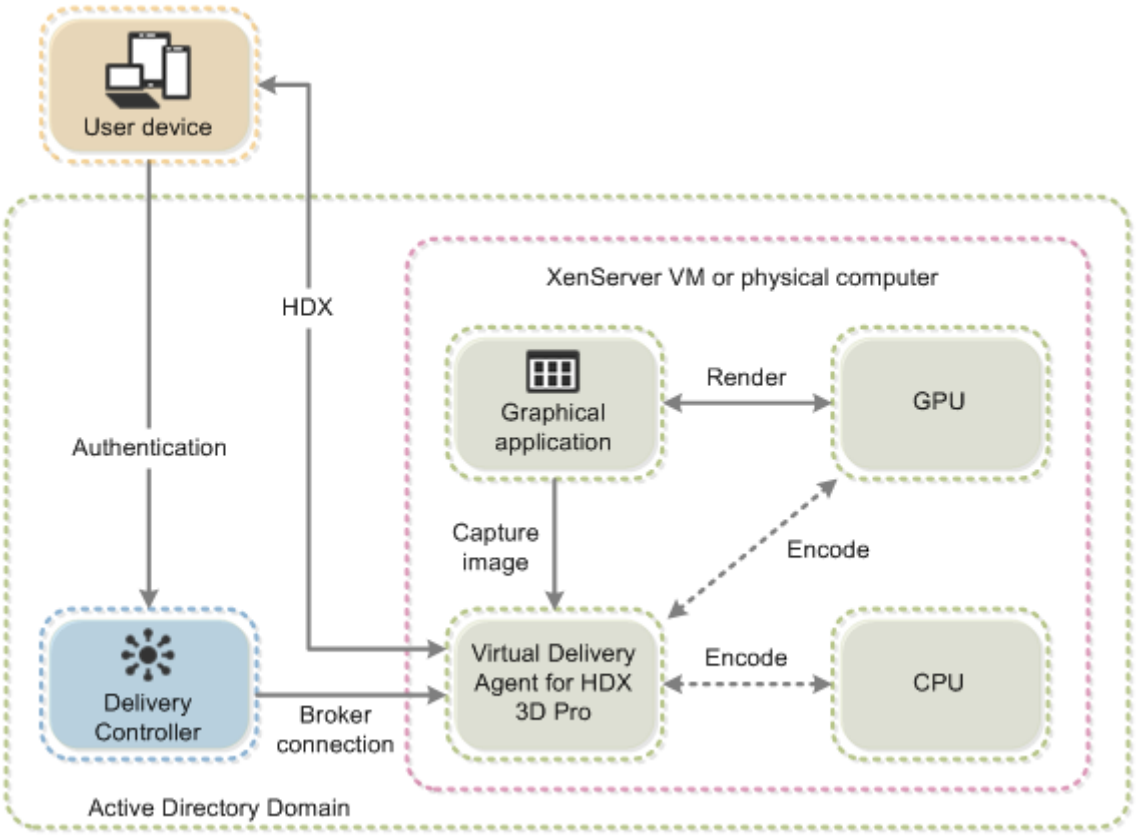
Comme indiqué dans l'illustration suivante :

- Lorsqu'un utilisateur se connecte à l'application Citrix Workspace et accède à l'application ou au bureau virtuel, le Controller authentifie l'utilisateur. Le Controller contacte ensuite le VDA pour HDX 3D Pro pour négocier une connexion à l'ordinateur hébergeant l'application graphique.

Le VDA pour HDX 3D Pro utilise le matériel approprié sur l'hôte pour compresser des vues du bureau complet ou de l'application graphique seule.

- Ces vues de bureau et d'application et les interactions de l'utilisateur avec elles sont transmises entre l'ordinateur hôte et la machine utilisateur. Cette transmission s'effectue via une connexion HDX directe entre l'application Citrix Workspace et le VDA pour HDX 3D Pro.




### Optimiser l'expérience utilisateur de HDX 3D Pro

Lorsque plusieurs utilisateurs partagent une connexion disposant d'une bande passante limitée (par exemple dans une succursale), nous vous recommandons d'utiliser le paramètre de stratégie **Limite de bande passante de session générale** pour limiter la bande passante disponible pour chaque utilisateur. L'utilisation de ce paramètre évite les trop fortes fluctuations de la bande passante au fur et à mesure que les utilisateurs ouvrent une session ou se déconnectent. Comme HDX 3D Pro s'adapte automatiquement pour utiliser toute la bande passante disponible, de fortes variations de celle-ci pendant les sessions des utilisateurs peuvent avoir un impact négatif sur les performances.

Ainsi, si 20 utilisateurs partagent une connexion de 60 Mbps, la bande passante disponible pour chaque utilisateur peut varier entre 3 Mbps et 60 Mbps en fonction du nombre d'utilisateurs simultanés. Pour optimiser l'expérience utilisateur dans ce scénario, déterminez la bande passante requise par utilisateur aux heures de pointe et limitez en permanence les utilisateurs à cette valeur.

Pour les utilisateurs de souris 3D, nous vous recommandons d'augmenter la priorité du canal virtuel Generic USB Redirection à 0. Pour plus d'informations sur la modification de la priorité du canal virtuel, consultez l'article CTX128190 du centre de connaissances.

### Compression sans perte

Lors de l'utilisation de la compression sans perte :

- L'indicateur sans perte, une icône dans la zone de notification, vous avertit si l'écran affiché est une trame avec ou sans perte. Cette icône est utile lorsque le paramètre de stratégie **Qualité visuelle** spécifie **Sans perte si possible**. L'indicateur sans perte devient vert lorsque les images envoyées sont sans perte.
- Le commutateur sans perte permet à l'utilisateur de passer en mode **Toujours sans perte** à tout moment dans la session. Pour sélectionner ou désélectionner le mode sans perte à tout moment au cours d'une session, cliquez avec le bouton droit sur l'icône, puis cliquez sur **Basculer vers au pixel près** ou utilisez le raccourci **Alt + Maj + 1**.
- Pour la compression sans perte : HDX 3D Pro utilise le codec sans perte pour la compression quel que soit le codec sélectionné au travers de la stratégie.
- Pour la compression avec perte : HDX 3D Pro utilise le codec original, soit celui par défaut, soit celui sélectionné via la stratégie.
- les paramètres du commutateur Sans perte ne sont pas conservés pour les sessions ultérieures. Pour utiliser le codec sans perte pour chaque connexion, sélectionnez **Toujours sans perte** dans le paramètre de stratégie **Qualité visuelle**.

### Touche de raccourci sans perte

Vous pouvez utiliser une touche de raccourci pour sélectionner ou désactiver la fonctionnalité **Sans perte** à tout moment au cours d'une session, en utilisant le raccourci par défaut **Alt + Maj + 1**.

Vous pouvez modifier le raccourci par défaut **Alt + Maj + 1** dans le registre Windows.
Pour configurer un nouveau paramètre de registre, définissez les valeurs de registre suivantes :

- **Clé** : `HKEY_CURRENT_USER\SOFTWARE\Citrix\Graphics`
- **Nom** :`HKLM_HotKey`
- **Type** : `String`

Le format pour configurer une combinaison de raccourcis est `C=0|1, A=0|1, S=0|1, W=0|1, K=val`. Les touches doivent être séparées par des virgules sans espace. L'ordre des touches n'est pas important.

A, C, S, W et K correspondent à des touches, où C=Ctrl, A=Alt, S=Maj, W=Win et K=une touche valide où les valeurs autorisées pour K sont 0—9, a—z et n'importe quel code de touche virtuelle.

Par exemple,

- Pour **F10**, définissez K=0x79
- Pour **Ctrl + F10**, définissez C=1, K=0x79

- Pour **Alt + A**, définissez A=1, K=a ou A=1, K=A ou K=A,A=1
- Pour **Ctrl + Alt + 5**, définissez C=1, A=1, K=5 ou A=1,K=5,C=1
- Pour **Ctrl + Maj + F5**, définissez A=1,S=1,K=0x74

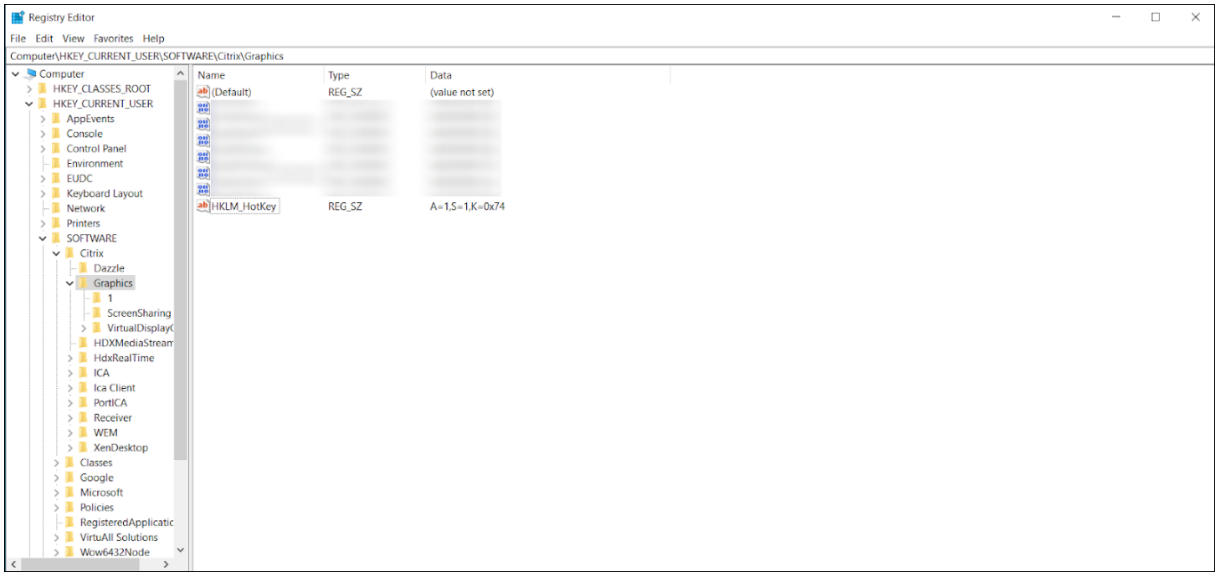
Le tableau suivant présente un exemple de liste de codes de touches virtuelles :

| Clé | Valeur |
|---|---|
| F1 | 0x70 |
| F2 | 0x71 |
| F3 | 0x72 |
| F4 | 0x73 |
| F5 | 0x74 |
| F6 | 0x75 |
| F7 | 0x76 |
| F8 | 0x77 |
| F9 | 0x78 |
| F10 | 0x79 |
| F11 | 0x7A |
| F12 | 0x7B |
| Touche Page haut | 0x21 |
| Touche Page bas | 0x22 |
| Touche Fin | 0x23 |
| Touche Début | 0x24 |
| Flèche gauche | 0x25 |
| Flèche vers le haut | 0x26 |
| Flèche droite | 0x27 |
| Flèche vers le bas | 0x28 |

Assurez-vous qu'il n'y a pas d'espace entre les combinaisons de raccourcis. Par exemple :

Correct :
C=1,K=0x74
Incorrect :
C=1, K=0x74




> **Attention :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

# Thinwire

June 28, 2024

## Introduction

Thinwire, composant de la technologie Citrix HDX, est la technologie de communication à distance d'écran par défaut de Citrix utilisée dans Citrix Virtual Apps and Desktops.

La technologie de communication à distance d'écran permet aux graphiques générés sur une machine d'être transmis, généralement via un réseau, vers une autre machine.

Une solution de communication à distance d'écran performante propose une expérience utilisateur très interactive, similaire à celle d'un PC local. Thinwire y parvient grâce à différentes techniques d'analyse et de compression d'image complexes et efficaces. Thinwire optimise l'évolutivité du serveur et utilise moins de bande passante que les autres technologies de communication à distance d'écran.

Grâce à cet équilibre, Thinwire répond à la plupart des cas d'utilisation d'entreprise et est utilisé comme technologie de communication à distance d'écran par défaut dans Citrix Virtual Apps and Desktops.

### HDX 3D Pro

Dans sa configuration par défaut, Thinwire peut fournir des graphiques 3D ou hautement interactifs et utiliser une unité de traitement graphique (GPU), le cas échéant. Toutefois, nous vous recommandons d'activer le mode HDX 3D Pro à l'aide des stratégies **Optimiser pour la charge des graphiques 3D** ou **Qualité visuelle > Sans perte si possible** lorsque des GPU sont présents. Ces stratégies configurent Thinwire pour utiliser un codec vidéo (H.264, H.265 ou AV1) pour coder l'écran entier à l'aide d'une accélération matérielle si un GPU est présent. Cette configuration offre une expérience plus fluide pour les graphiques 3D de qualité professionnelle. Pour plus d'informations, consultez H.264 Sans perte si possible, HDX 3D Pro et Accélération GPU pour OS mono-session Windows.

### Exigences

Thinwire est optimisé pour les systèmes d'exploitation les plus récents, y compris Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10 et Windows 7. Pour Windows Server 2008 R2, le mode graphique d'ancienne génération est recommandé. Utilisez les modèles de stratégie Citrix intégrés, la grande évolutivité du serveur et le système d'exploitation optimisé pour WAN-Legacy pour mettre à disposition les combinaisons de paramètres de stratégie recommandées par Citrix pour ces cas d'utilisation.

- Le paramètre de stratégie qui détermine le comportement de Thinwire (**Utiliser un codec vidéo pour la compression**) est disponible sur les versions VDA dans Citrix Virtual Apps and Desktops 7 1808 ou version ultérieure et XenApp et XenDesktop 7.6 FP3 et versions ultérieures. L'option **Utiliser un codec vidéo au choix** est le paramètre par défaut pour les versions VDA de Citrix Virtual Apps and Desktops 7 1808 ou version ultérieure et XenApp et XenDesktop 7.9 et versions ultérieures.
- Toutes les applications Citrix Workspace prennent en charge Thinwire. Certaines applications Citrix Workspace peuvent prendre en charge des fonctionnalités de Thinwire que d'autres ne prennent pas en charge, par exemple, des graphiques 8 ou 16 bits pour une utilisation réduite de la bande passante. La prise en charge de ces fonctionnalités est automatiquement gérée par l'application Citrix Workspace.
- Thinwire utilise davantage de ressources serveur (UC, mémoire) dans les scénarios à plusieurs moniteurs et haute résolution. Il est possible d'ajuster la quantité de ressources que Thinwire utilise ; cependant, l'utilisation de la bande passante peut augmenter en conséquence.

- Dans les scénarios à faible bande passante ou à latence élevée, il peut être utile d'activer les graphiques 8 ou 16 bits pour améliorer l'interactivité. La qualité visuelle peut être affectée, plus particulièrement avec un nombre de couleurs de 8 bits.

### Méthodes de codage

Thinwire peut fonctionner dans deux modes d'encodage différents en fonction de la stratégie et des capacités du client :

- Paramètre de stratégie Thinwire avec JPEG adaptatif
  **Utiliser un codec vidéo pour la compression** : **Ne pas utiliser de codec vidéo**
- Paramètre de stratégie Thinwire avec H.264, H.265 ou AV1 sélectif :
  **Utiliser un codec vidéo pour la compression** : **Utiliser le codec vidéo lorsque vous le souhaitez** ou **Pour des régions qui changent activement**
- Paramètre de stratégie Thinwire avec H.264, H.265 ou AV1 mode plein écran :
  **Utiliser un codec vidéo pour la compression** : **Pour la totalité de l'écran**

#### H.265

Le codage vidéo à haute efficacité (HEVC), également connu sous le nom de H.265, est le successeur du H.264.
Le codage matériel avec le codec vidéo H.265 est pris en charge sur les GPU suivants :

- GPU basés sur NVIDIA Maxwell et versions supérieures
- GPU Intel de 6e génération et versions supérieures
- GPU basés sur AMD Raven et versions supérieures

#### AV1

Citrix a ajouté la prise en charge du codec vidéo AV1. L'avantage de l'AV1 est qu'il offre une compression d'image supérieure, une meilleure qualité d'image et une utilisation de bande passante inférieure à celle des formats H.264 et H.265.

Les exigences suivantes doivent être remplies pour l'AV1 :

- VDA 2305 ou version supérieure pour les GPU NVIDIA, ou
- VDA 2308 ou version supérieure pour GPU Intel

Les GPU suivants sont compatibles pour le codage :

- GPU basé sur NVIDIA Ada Lovelace

- GPU Intel ARC ou Intel Data Center série Flex

Pour en savoir plus sur les GPU Ada Lovelace de NVIDIA, consultez Architecture ADA.

Pour en savoir plus sur les GPU Intel pour postes de travail ARC et centres de données de la série Flex, consultez Série Flex et Présentation.

### Sélection automatique du codec vidéo

Vous pouvez détecter automatiquement le meilleur codec vidéo à utiliser lorsque la stratégie **Utiliser un codec vidéo pour la compression** est activée ou Optimiser pour la charge de travail graphique 3D est activée sur le VDA. Lors de l'installation de l'application Citrix Workspace pour Windows, les capacités de décodage du terminal sont évaluées. Sur la base de ces informations, l'application Citrix Workspace pour Windows négocie le meilleur codec à utiliser avec le VDA lors de la connexion. La liste suivante indique l'ordre dans lequel les codecs vidéo sont évalués :

- AV1
- H.265
- H.264

La sélection automatique s'applique uniquement aux variantes 4:2:0 de ces codecs. Si le paramètre de **Qualité visuelle** est réglé sur « Build-to-Lossless » ou « Toujours sans perte » et si Autoriser le mode sans perte visuelle est réglé sur « Activé », la sélection automatique du codec vidéo est désactivée.

Lors de la connexion à une ressource, l'application Citrix Workspace teste la capacité du terminal à décoder H.265 et AV1 et à enregistrer ces fonctionnalités dans le registre. L'application Citrix Workspace sélectionne ensuite automatiquement le meilleur codec vidéo à utiliser et négocie ce choix avec le VDA. Si le VDA et le client peuvent utiliser H.265 et AV1, AV1 est sélectionné comme codec vidéo. Si AV1 n'est disponible ni sur le VDA ni sur le client, H.265 est négocié. Si H.265 n'est pas non plus disponible sur l'un et l'autre, la session utilise H.264 comme codec vidéo.

> **Remarque :**
>
> Cette fonctionnalité est activée par défaut. Ce comportement peut être modifié en définissant le nouveau paramètre de registre côté client `DisableDecoderCaps`.

Pour désactiver la sélection automatique du codec vidéo, définissez « DisableDecoderCaps » sur `HKLM\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1` ou `HKCU\Software\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`.

Si l'une de ces valeurs est définie sur 1, la sélection automatique du codec vidéo n'est pas utilisée. L'indicateur d'état graphique et le moniteur HDX peuvent contrôler le codec vidéo.

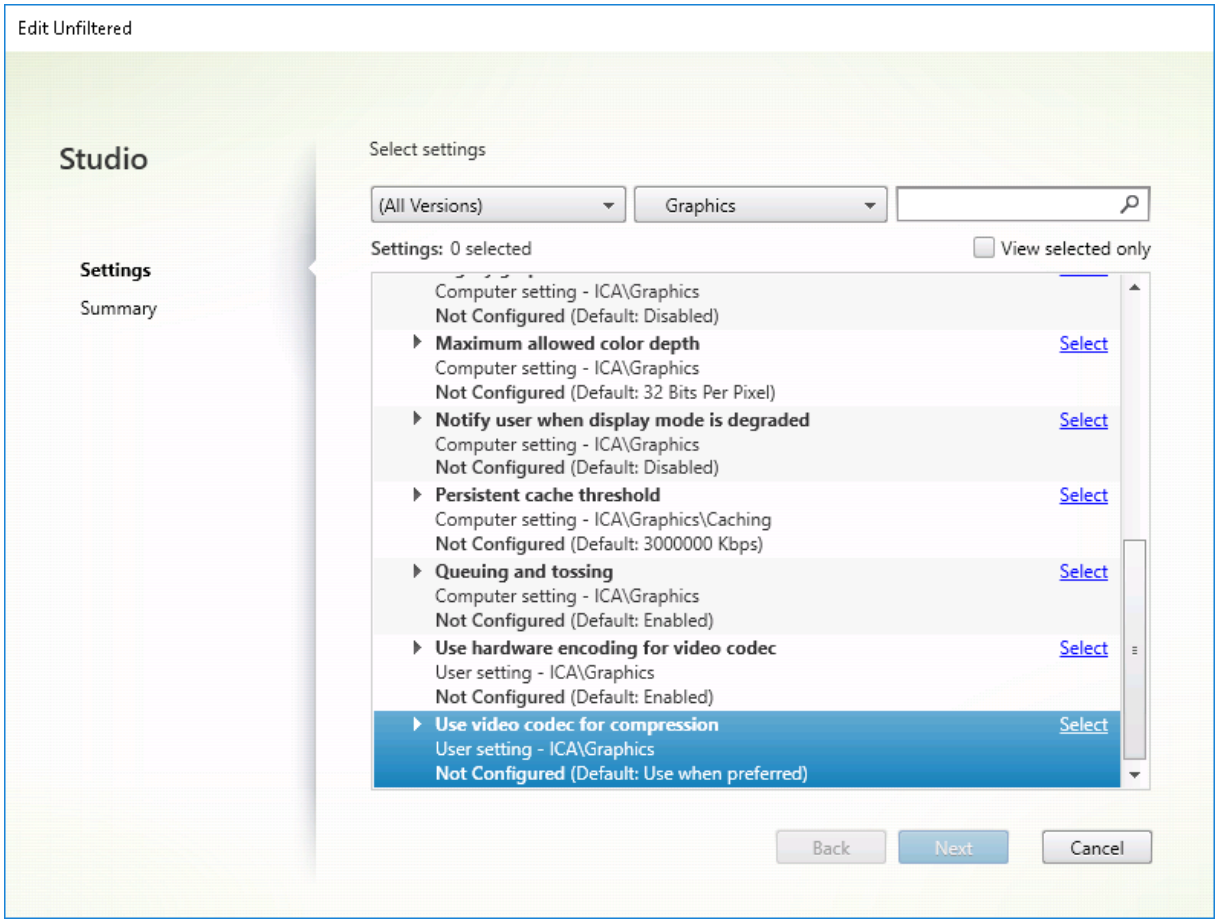
### Configuration

Thinwire est la technologie de communication à distance d'écran par défaut.

Le paramètre de stratégie Graphiques suivant définit la valeur par défaut et fournit d'autres méthodes pour différents scénarios d'utilisation :

- Utiliser codec vidéo pour la compression
  - **Utiliser un codec vidéo au choix**. C'est le réglage par défaut. Aucune configuration supplémentaire n'est requise. Le maintien de ce paramètre en tant que valeur par défaut assure que Thinwire est sélectionné pour toutes les connexions Citrix, et est optimisé pour la capacité à monter en charge, la bande passante et une qualité d'image supérieure pour les charges de travail de bureau standard. Cela est fonctionnellement équivalent à **Pour les zones changeant constamment**.
- Les autres options de ce paramètre de stratégie continuent à utiliser Thinwire avec d'autres technologies pour différents scénarios d'utilisation. Par exemple :
  - **Pour les zones changeant constamment**. La technologie d'affichage adaptatif dans Thinwire identifie les images en mouvement (vidéo, 3D en mouvement) et utilise H.264, H.265 ou AV1 uniquement dans la partie de l'écran sur laquelle l'image est en mouvement.
  - **Pour l'écran entier**. Propose Thinwire avec H.264, H.265 ou AV1 en mode plein écran optimisé pour améliorer l'expérience utilisateur et la bande passante lorsque les graphiques 3D sont fortement sollicités. Dans le cas de H.264 4:2:0 (la stratégie **Compression visuelle sans perte** est désactivée), l'image finale n'est pas au pixel près (sans perte) et peut ne pas convenir à certains scénarios. Pensez alors plutôt à régler H.264 Build ou H.265 Build sur une utilisation sans perte.




Différents autres paramètres de stratégie, y compris les paramètres de stratégie Affichage visuel suivants, peuvent être utilisés pour optimiser les performances de la technologie de communication à distance d'écran. Thinwire les prend tous en charge.

- Nombre de couleurs préféré pour les graphiques simples
- Taux de trames cible
- Qualité visuelle

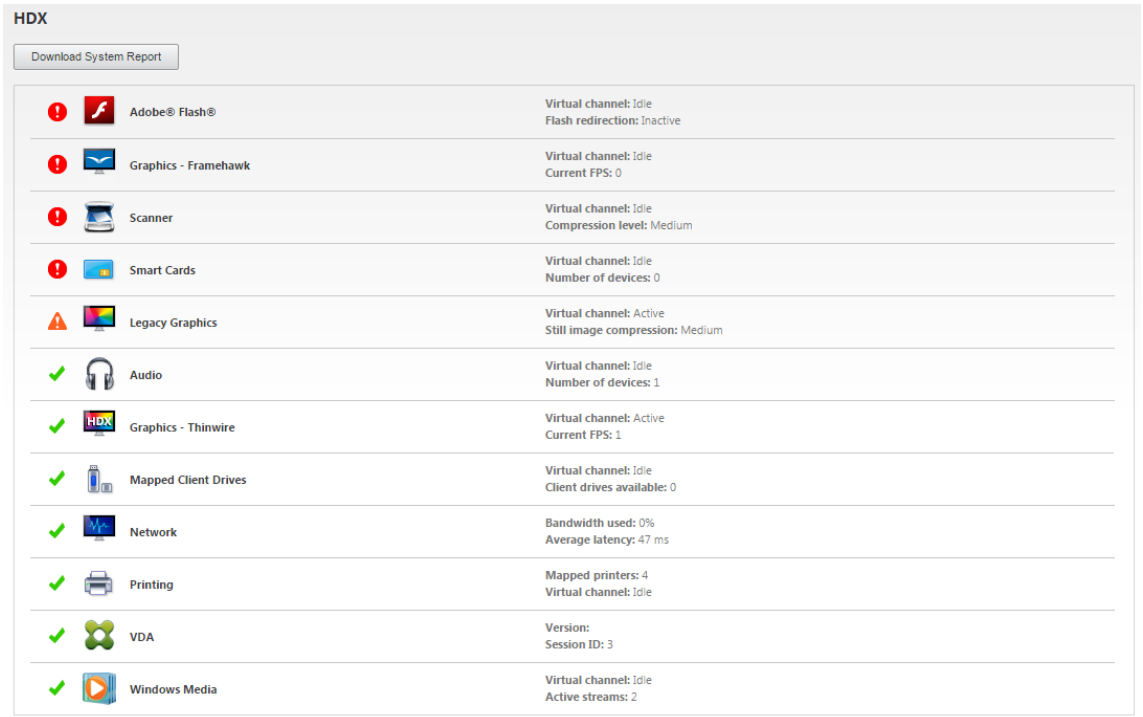
Pour obtenir les combinaisons de paramètres de stratégie recommandées par Citrix pour différents scénarios d'utilisation, utilisez les modèles de stratégie Citrix intégrés. Les modèles **Grande évolutivité du serveur** et **Expérience utilisateur très haute définition** utilisent tous les deux Thinwire avec les combinaisons de paramètres de stratégie les mieux adaptées aux priorités de votre entreprise et aux attentes de vos utilisateurs.

### Contrôle de Thinwire

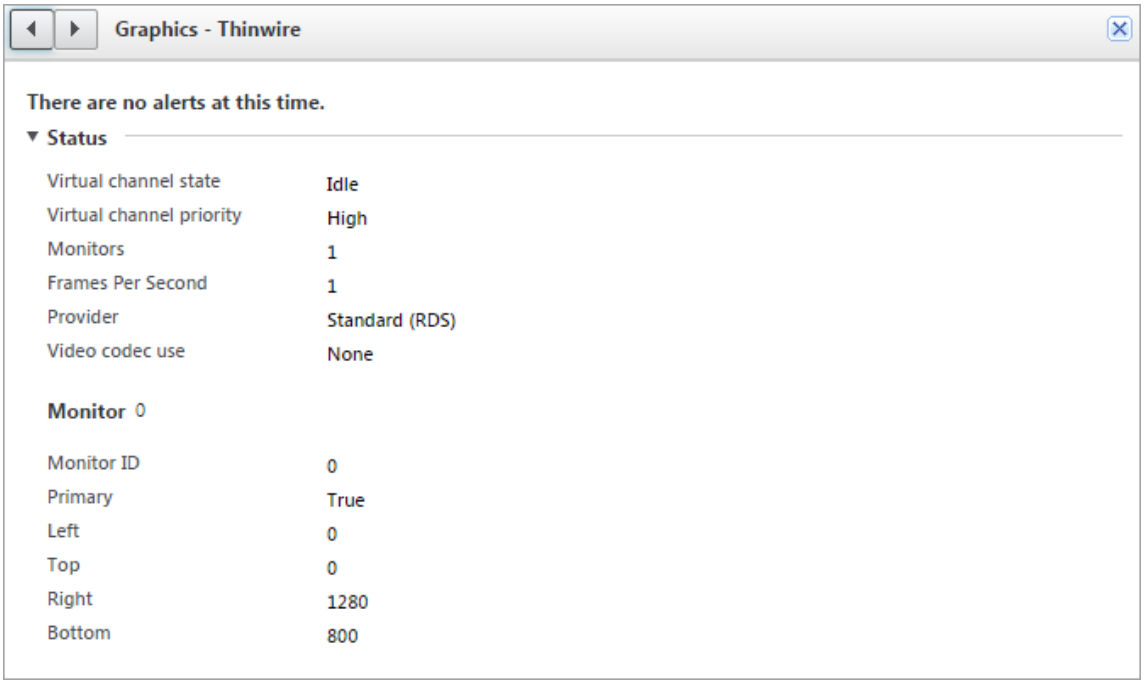
Vous pouvez contrôler l'utilisation et les performances de Thinwire depuis Citrix Director. La vue Détails du canal virtuel HDX contient des informations utiles pour la résolution des problèmes et le contrôle de Thinwire dans une session. Pour afficher les mesures liées à Thinwire :

1. Dans Director, recherchez un utilisateur, un ordinateur ou un point de terminaison, ouvrez une session active, puis cliquez sur **Détails**. Vous pouvez également sélectionner **Filtres** > **Sessions** > **Toutes les sessions**, ouvrir une session active et cliquer sur **Détails**.
2. Faites défiler l'écran vers le bas dans le panneau **HDX**.




3. Sélectionnez **Graphiques - Thinwire**.



### Codec de compression sans perte (MDRLE)

Dans une session de bureau typique, la plupart des images sont des graphiques simples ou des régions de texte. Thinwire détermine où se trouvent ces zones et les sélectionne pour l'encodage sans perte à l'aide du codec 2DRLE. Du côté client de l'application Citrix Workspace, ces éléments sont décodés à l'aide du décodeur 2DRLE de l'application Citrix Workspace pour l'affichage de la session.

Dans XenApp et XenDesktop 7.17, nous avons ajouté un codec MDRLE à taux de compression plus élevé qui consomme moins de bande passante dans les sessions de bureau typiques que le codec 2DRLE. Ce nouveau codec n'a pas d'impact sur la capacité à monter en charge du serveur.

Une bande passante plus faible signifie généralement une meilleure interactivité de session (en particulier sur les liens partagés ou limités) et des coûts réduits.

Aucune configuration n'est requise pour le codec MDRLE. Si l'application Citrix Workspace prend en charge le décodage MDRLE, le VDA utilise le codage MDRLE VDA et le décodage de l'application Citrix Workspace MDRLE. Si l'application Citrix Workspace ne prend pas en charge le décodage MDRLE, le VDA revient automatiquement au codage 2DRLE.

**Configuration requise pour MDRLE :**

- VDA Citrix Virtual Apps and Desktops version minimale 7 1808
- XenApp et XenDesktop version minimale 7.17
- Application Citrix Workspace pour Windows version minimale 1808
- Citrix Receiver pour Windows version minimale 4.11

### Mode progressif

Citrix Virtual Apps and Desktops 1808 a introduit le mode progressif et l'activait par défaut. Dans des conditions réseau limitées (par défaut : bande passante < 2 Mbit/s, ou latence > 200 ms), Thinwire augmentait la compression du texte et de l'imagerie statique pour améliorer l'interactivité pendant l'activité de l'écran. La netteté du texte et des images fortement compressés était ensuite progressivement réglée, de manière aléatoire, lorsque l'activité de l'écran s'arrêtait. Si cette méthode améliorait l'interactivité globale, cela réduisait l'efficacité du cache et augmentait l'utilisation de la bande passante.

À partir de Citrix Virtual Apps and Desktops 1906, le mode progressif est désactivé par défaut. Nous utilisons maintenant une approche différente. La qualité des images fixes est désormais basée sur les conditions du réseau et flotte entre une valeur minimale et maximale prédéfinie pour chaque paramètre **Qualité visuelle**. Étant donné qu'il n'y a pas d'étape explicite de réglage de la netteté, Thinwire optimise la diffusion des images et maintient l'efficacité du cache, tout en offrant presque tous les avantages du mode progressif.

#### Changement du comportement du mode progressif

Vous pouvez changer l'état du mode progressif avec la clé de registre. Pour plus d'informations, reportez-vous à Mode progressif dans la liste des fonctionnalités gérées via le Registre.

### Sans perte si possible

**Sans perte si possible** est une configuration Thinwire spéciale qui optimise la distribution graphique pour l'interactivité et la qualité d'image finale. Vous pouvez activer ce paramètre en définissant la stratégie **Qualité visuelle** sur **Sans perte si possible**.

Build-to-lossless compresse l'écran à l'aide de H.264, H.265 ou AV1 pendant l'activité de l'écran et règle la netteté au pixel près (sans perte) lorsque l'activité s'arrête. La qualité d'image compressée avec perte s'adapte aux ressources disponibles pour maintenir la meilleure fréquence d'images possible. L'amélioration de la netteté s'effectue progressivement. Par exemple, en sélectionnant un modèle et en le faisant pivoter.

**Build-to-lossless**offre tous les avantages de l'utilisation d'un codec vidéo pour la totalité de l'écran, y compris l'accélération matérielle, mais avec l'avantage supplémentaire d'un écran final sans perte garanti. Ceci est essentiel pour les charges de travail de type 3D qui nécessitent une image finale au pixel près. Par exemple, dans le cas de l'imagerie médicale. En outre, **Build-to-lossless** H.264 utilise moins de ressources que H.264 4:4:4 plein écran. Par conséquent, l'utilisation de **Sans perte si possible** entraîne généralement une fréquence d'images plus élevée que la compression visuelle sans perte H.264 4:4:4.

> **Remarque :**
>
> Vous pouvez désactiver l'utilisation d'un codec vidéo lorsque vous utilisez une version sans perte. Définissez simplement la stratégie **Utiliser le codec vidéo** sur `Do not use video codec`. Il en résulte que les images en mouvement sont codées au format JPEG adaptatif à la place.

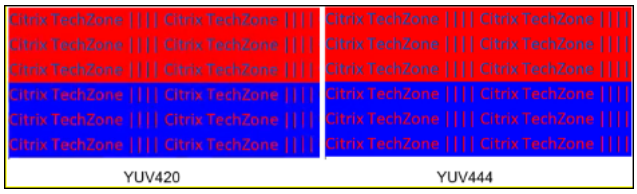
### Codage visuel sans perte

Le codage sans perte visuelle utilise l'espace colorimétrique YUV 4:4:4 au lieu de l'espace colorimétrique YUV 4:2:0 sous-échantillonné en chromatologie pour la compression du codec vidéo. Cela garantit qu'aucune information colorimétrique n'est perdue lors de la conversion de l'espace colorimétrique et, une fois décodée, elle est visuellement imperceptible par rapport à l'image RGB d'origine.

Prenons l'exemple suivant. Si vous utilisez un codec vidéo pour compresser la totalité de l'écran, la compression des couleurs 4:2:0 peut dégrader les détails à contraste élevé tels que le texte, les rendant

flous et plus difficiles à lire. En revanche, le format 4:4:4 préserve presque toutes les informations relatives aux couleurs et ne présente aucune dégradation perceptible visuellement.




Les charges de travail qui nécessitent une qualité parfaite au pixel près ou un affichage couleur précis peuvent bénéficier du codage sans perte visuelle.

Le codage sans perte visuelle est disponible avec H.264 et H.265. Le codage H.264 4:4:4 est une solution purement logicielle et peut donc avoir d'importantes répercussions sur l'utilisation du processeur à la fois sur le VDA et sur le client. Cela peut également affecter la fréquence d'images.

Le support H.265 4:4:4 a été ajouté avec la sortie de l'application Citrix Workspace 2305, permettant à Thinwire d'utiliser à la fois un GPU sur le VDA et un client pour le codage H.265 4:4:4, améliorant ainsi considérablement les performances.

Pour autoriser le codage sans perte visuelle 4:4:4, deux stratégies doivent être activées :

- **Qualité visuelle** : Définissez-la sur `Build to Lossless` ou `Always Lossless`
- **Autoriser le mode sans perte visuelle** : Définissez-la sur `Enabled`

> **Remarque :**
>
> Si **Autoriser le mode sans perte visuelle** n'est pas activé, nous passons à notre encodeur Thinwire dans `Build to lossless` ou `Always Lossless`.

H.265 4:4:4 sans perte visuelle présente les exigences supplémentaires suivantes :

- Les GPU NVIDIA nécessitent la version VDA 2209 ou supérieure
- Les GPU Intel nécessitent la version VDA 2308 ou supérieure

Les GPU suivants sont pris en charge pour H.265 4:4:4 :

- GPU NVIDIA de génération Pascal et versions ultérieures
- GPU Intel de 10e génération et versions ultérieures

Pour le client, l'application Citrix Workspace pour Windows version 2305 est requise (la version 2309.1 est recommandée).

Le décodage matériel du H.265 4:4:4 est possible avec les GPU des périphériques clients suivants :

- GPU NVIDIA de génération Turing et versions ultérieures
- GPU Intel de 10e génération et versions ultérieures

# Filigrane de session textuel

June 27, 2024

Filigranes de session textuels pour dissuader et suivre le vol de données. Ces informations traçables apparaissent sur le bureau de la session comme un moyen de dissuasion pour ceux qui utilisent des photographies et des captures d'écran pour voler des données. Vous pouvez spécifier un filigrane ou une couche de texte qui s'affiche sur l'intégralité de l'écran de session sans modifier le contenu du document d'origine. Les filigranes de session textuels nécessitent un support VDA.

> **Important :**
>
> Le filigrane de session textuel n'est pas un élément de sécurité. Cette solution n'empêche pas complètement le vol de données, mais elle offre un certain niveau de dissuasion et de traçabilité. Bien que nous ne garantissions pas une traçabilité complète des informations lors de l'utilisation de cette fonctionnalité, nous vous recommandons de combiner cette fonctionnalité avec d'autres solutions de sécurité, le cas échéant.

Le filigrane de session est du texte appliqué à la session délivrée à l'utilisateur. Le filigrane de session contient des informations utilisées pour le suivi du vol de données. La donnée la plus importante est l'identité de l'utilisateur de connexion de la session en cours dans laquelle l'image d'écran a été prise. Pour suivre plus efficacement les fuites de données, incluez d'autres informations telles que l'adresse du protocole Internet du serveur ou du client et une heure de connexion.

Pour ajuster l'expérience utilisateur, utilisez les paramètres de stratégie Filigrane de session pour configurer l'emplacement et l'apparence du filigrane sur l'écran.

**Exigences :**

Virtual Delivery Agents :

OS multi-session 7.17
OS mono-session 7.17

**Limitations :**

- Les filigranes de session ne sont pas pris en charge dans les sessions où Local App Access, la redirection Windows Media, MediaStream, la redirection du contenu du navigateur et la redirection vidéo HTML5 sont utilisés. Pour utiliser le filigrane de session, assurez-vous que ces fonctionnalités sont désactivées.
- Le filigrane de session n'est pas pris en charge et n'apparaît pas si la session s'exécute en modes d'accélération matérielle plein écran (codage H.264 ou H.265 en plein écran).
- Si vous définissez ces stratégies HDX, les paramètres de filigrane ne prennent pas effet et un filigrane n'est pas affiché dans l'affichage de la session.

**Utiliser le codage matériel pour le codec vidéo** > **Activé**
**Utiliser codec vidéo pour la compression** > **Pour l'écran entier**

- Si vous définissez ces stratégies HDX, le comportement est indéterminé et le filigrane risque de ne pas s'afficher.

  **Utiliser le codage matériel pour le codec vidéo** > **Activé**
  **Utiliser codec vidéo pour la compression** > **Utiliser un codec vidéo au choix**

  Pour garantir l'affichage du filigrane, réglez **Utiliser le codage matériel pour le codec vidéo** sur **Désactivé** ou réglez **Utiliser codec vidéo pour la compression** sur **Pour les zones changeant constamment** ou **Ne pas utiliser de codec vidéo**.
- Le filigrane de session prend uniquement en charge le mode graphique Thinwire.
- Si vous utilisez l'enregistrement de session, la session enregistrée n'inclut pas le filigrane.
- Si vous utilisez l'assistance à distance Windows, le filigrane n'est pas affiché.
- Si un utilisateur appuie sur la touche **Impr. écran** pour capturer l'écran, l'écran capturé du côté VDA n'inclut pas les filigranes. Nous vous recommandons de prendre des mesures pour éviter la copie de l'image capturée.

## Partage d'écran

June 27, 2024

Le partage d'écran permet à un utilisateur de partager une session Citrix Virtual Desktop avec d'autres personnes, notamment le contenu de l'écran, les commandes du clavier et de la souris.

### Configuration système requise

- Windows : VDA avec OS mono-session ou multi-session
- Linux : consultez la documentation Linux VDA pour plus d'informations sur le partage de sessions Linux.
- Seules les sessions de bureau peuvent être partagées.
- Il doit y avoir une connectivité réseau entre le VDA hébergeant la session et les machines qui se connectent aux sessions partagées. Les exigences relatives aux ports réseau dépendent des ports ICA utilisés (TCP/UDP 1494 ou 2598) et de la configuration de la stratégie de partage d'écran (TCP 52525 à 52625 par défaut).

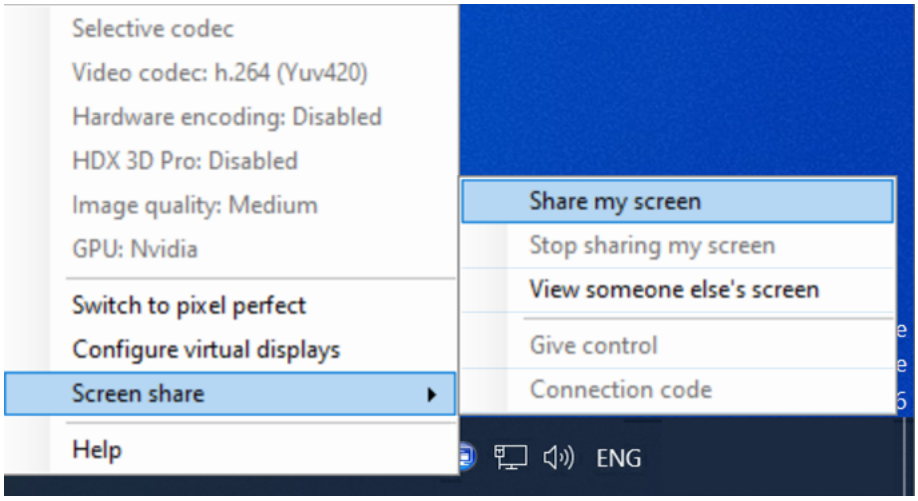
### Configuration

Le partage d'écran doit être activé à l'aide de stratégies Citrix. Le partage d'écran est désactivé par défaut. Configurez la stratégie de partage d'écran pour activer ou désactiver la fonction et attribuer la plage de ports réseau utilisable.

Activez la stratégie Indicateur d'état des graphiques pour afficher l'interface utilisateur qui inclut les commandes de partage et de connexion aux sessions.

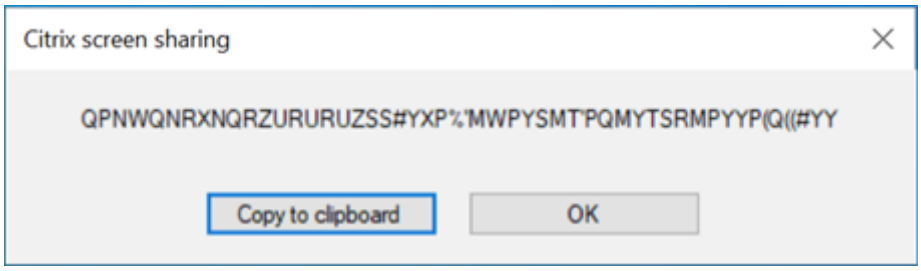
### Partager une session

Pour partager une session, recherchez l'icône de l'indicateur d'état des graphiques HDX dans la zone de notification Windows. Cliquez dessus avec le bouton droit de la souris pour afficher le menu et sélectionnez **Partage d'écran > Partager mon écran**.




Cliquez sur **Copier dans le presse-papiers** ou sélectionnez et copiez manuellement la chaîne entière affichée dans la boîte de dialogue. La chaîne peut ensuite être collée dans l'application de votre choix, telle qu'un client d'e-mail ou de messagerie instantanée, pour être distribuée à d'autres utilisateurs.

Cliquez sur **OK** ou sur **x** pour fermer la boîte de dialogue. Le code de connexion peut être récupéré à partir de l'option de menu **Partage d'écran > Code de connexion** à tout moment pendant le partage de la session.

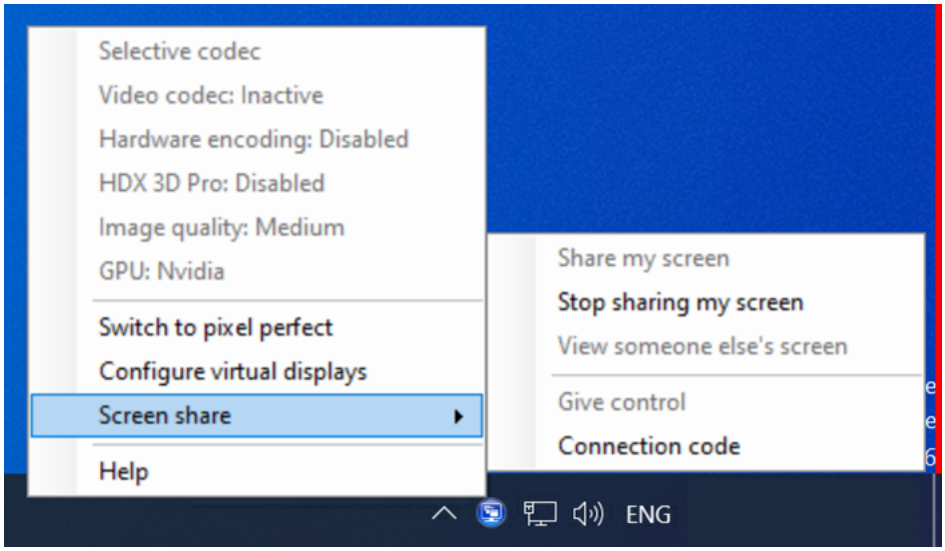


Un contour rouge apparaît autour de l'écran pour indiquer que la session est maintenant partagée et qu'elle est visible par les autres utilisateurs.

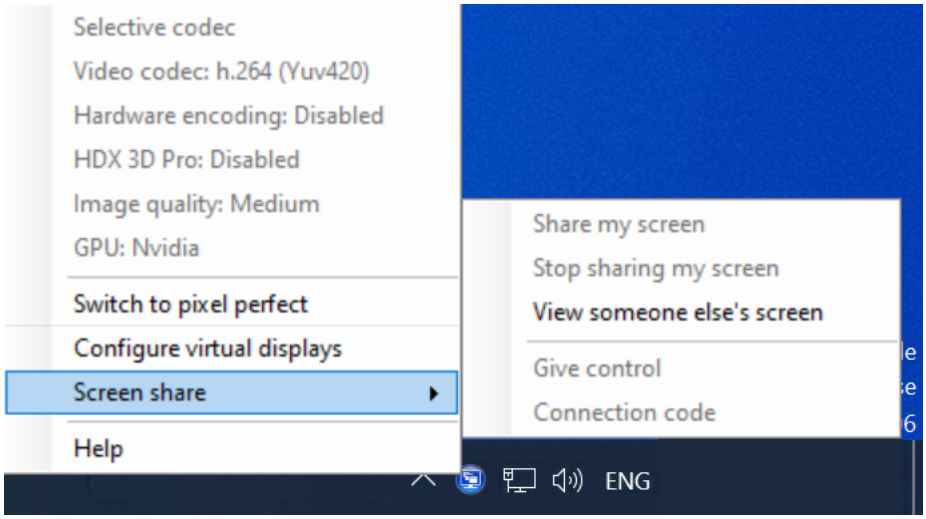
Les commandes du clavier et de la souris peuvent également être partagées avec d'autres utilisateurs via l'option de menu **Partage d'écran > Donner le contrôle**.

Utilisez l'option de menu **Partage d'écran > Arrêter de partager mon écran** pour arrêter de partager la session et déconnecter tous les utilisateurs.




### Se connecter à une session partagée

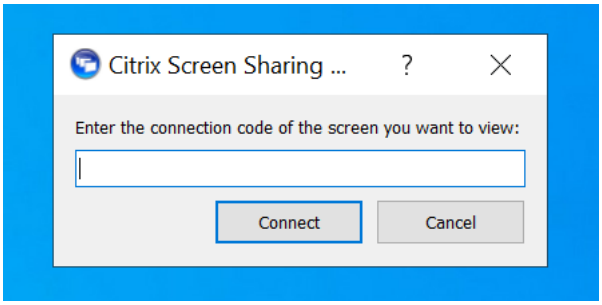
Pour vous connecter aux sessions d'un autre utilisateur, recherchez l'icône d'indicateur d'état des graphiques HDX dans la zone de notification Windows. Cliquez dessus avec le bouton droit de la souris pour afficher le menu et sélectionnez **Partage d'écran > Afficher l'écran de quelqu'un d'autre**.




Entrez ou collez la chaîne de connexion fournie par l'utilisateur partageant la session dans la zone de

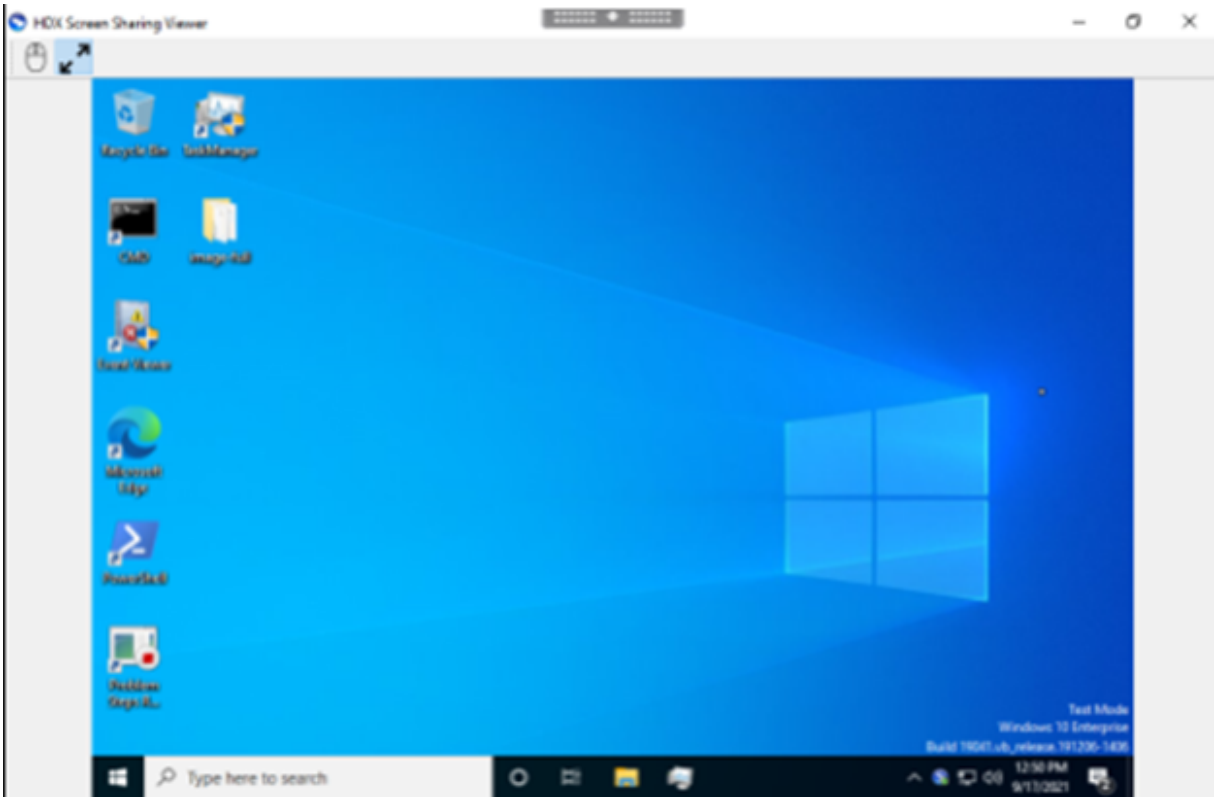
 

texte. Cliquez sur **Connecter** pour établir la connexion.




Vous pouvez demander les commandes du clavier et de la souris en cliquant sur l'icône de la souris dans le coin supérieur gauche de la fenêtre **Visionneuse de partage d'écran HDX**.

Fermez la fenêtre **Visionneuse de partage d'écran HDX** pour vous déconnecter de la session partagée à tout moment.




### Autres considérations

- L'application de visionneuse de partage d'écran est incluse avec le VDA dans *C:\Program Files\Citrix\HDX\bin\TwPlayer.exe* et peut être déployée en tant qu'application publiée à l'aide d'un serveur d'applications virtuelles. Ce modèle de déploiement alternatif permet la collaboration avec des utilisateurs qui n'ont pas accès à un bureau virtuel.

- Le nombre d'utilisateurs autorisés à se connecter à une session partagée peut être limité à l'aide de la plage de ports réseau définie dans la stratégie de partage d'écran. Chaque utilisateur requiert un port. La plage par défaut autorise 100 utilisateurs au maximum.
- Tous les moniteurs connectés à la session sont partagés. Vous ne pouvez pas sélectionner de moniteurs individuels.
- Le codec vidéo H.265 n'est pas pris en charge.

## Disposition d'affichage virtuel

June 27, 2024

L'interface utilisateur Configuration de l'affichage virtuel vous permet de définir une disposition d'affichage virtuel par moniteur de session sur le VDA, au sein d'une session active. Cette fonctionnalité vous permet de diviser chaque moniteur de session de façon indépendante en plusieurs moniteurs virtuels. Vous pouvez les diviser en un total de 8 moniteurs virtuels sur le bureau distant. Vous pouvez également mettre à jour le moniteur principal de la session et les paramètres DPI pour les écrans.

La configuration d'affichage virtuel est stockée par utilisateur et par appareil client. La configuration s'appliquera à toutes les connexions suivantes à partir d'un client donné pour un utilisateur particulier. Elle est conservée lors du redimensionnement de session, de la déconnexion ou reconnexion de session et de la fermeture ou ouverture de session. La réinitialisation de la disposition de l'affichage virtuel configurée se produit lorsqu'une session est redimensionnée et que le nombre de moniteurs de session est modifié.

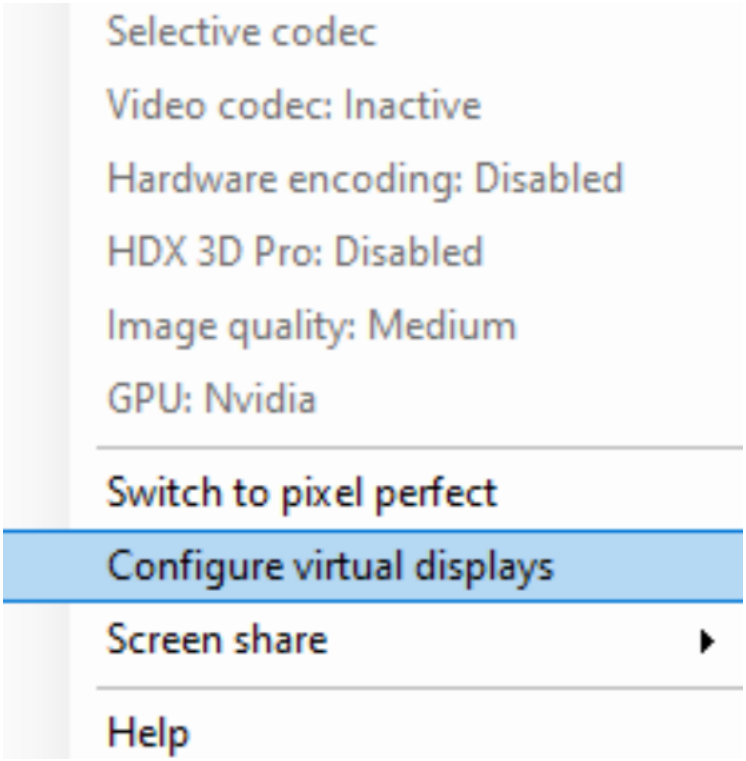
### Configuration système requise

- Windows : VDA avec OS mono-session ou multi-session
- La stratégie Indicateur d'état des graphiques doit être activée
- Seules les sessions de bureau peuvent être configurées.

### Configuration

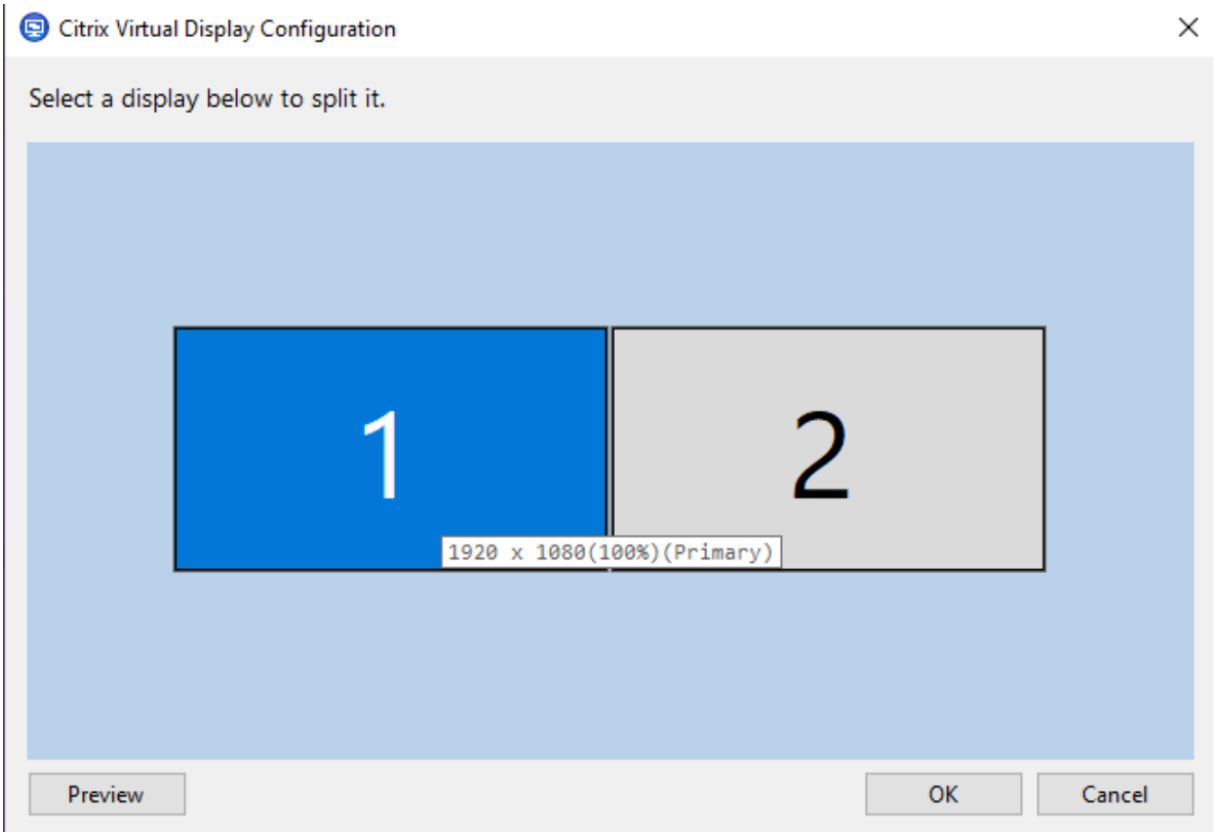
Pour configurer la disposition d'affichage virtuel, cliquez avec le bouton droit sur l'icône de l'indicateur d'état graphique et sélectionnez l'option Configurer les écrans virtuels. L'interface utilisateur Configuration de l'affichage virtuel est lancée.

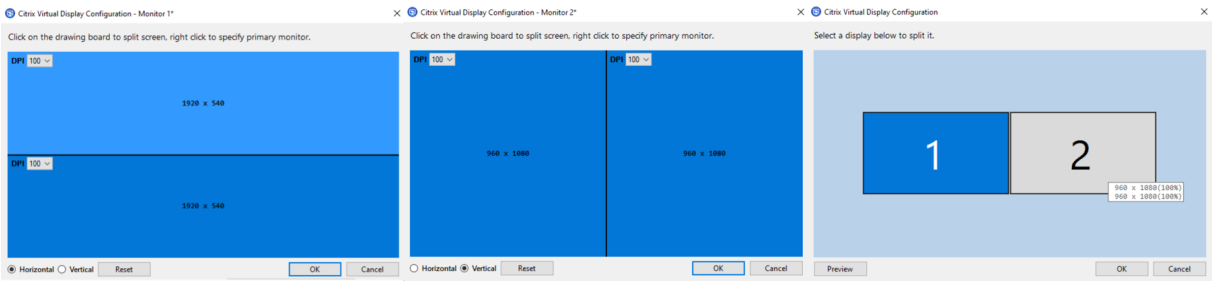



L'interface utilisateur affiche la disposition de l'affichage de la session en cours, le bleu désignant le moniteur principal de la session. Vous pouvez voir l'infobulle Paramètres d'affichage lorsque vous survolez un écran. L'infobulle fournit des informations sur la disposition de l'affichage virtuel actuelle définie sur un moniteur de session donné.

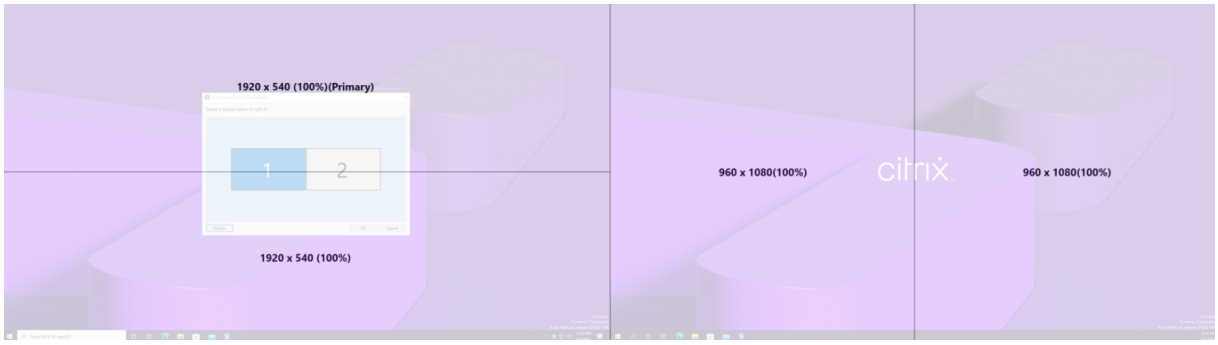



Sélectionnez un affichage pour passer à une interface utilisateur interactive, qui vous permet de configurer des affichages virtuels pour le moniteur de session sélectionné. Vous pouvez dessiner des lignes horizontales ou verticales pour séparer l'écran en moniteurs virtuels. L'écran est divisé en fonction des pourcentages spécifiés pour les résolutions des moniteurs de session. Cliquez avec le bouton droit de la souris sur un affichage virtuel pour le marquer comme moniteur principal et utilisez la liste déroulante DPI pour définir un facteur d'échelle préféré pour l'affichage virtuel. Après avoir défini une disposition d'affichage virtuelle, cliquez sur **OK** pour enregistrer temporairement la disposition ou sur **Annuler** pour annuler toute modification. Vous pouvez utiliser **Réinitialiser** pour annuler la configuration et restaurer la disposition d'origine du moniteur de session.

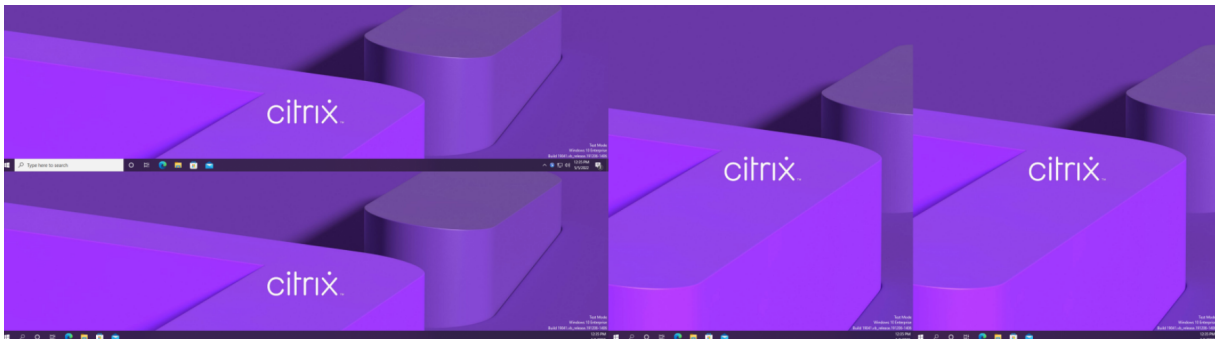


Pour prévisualiser la disposition d'affichage virtuel actuellement configurée, cliquez sur le bouton **Aperçu**. Une fenêtre apparaît pour mettre en évidence la position et la résolution attendues des affichages virtuels dans la session.




Cliquez sur **OK** pour appliquer et enregistrer immédiatement la disposition de l'affichage virtuel. Cliquez sur **Annuler** pour fermer l'interface utilisateur et annuler toutes les modifications.



### Autres considérations

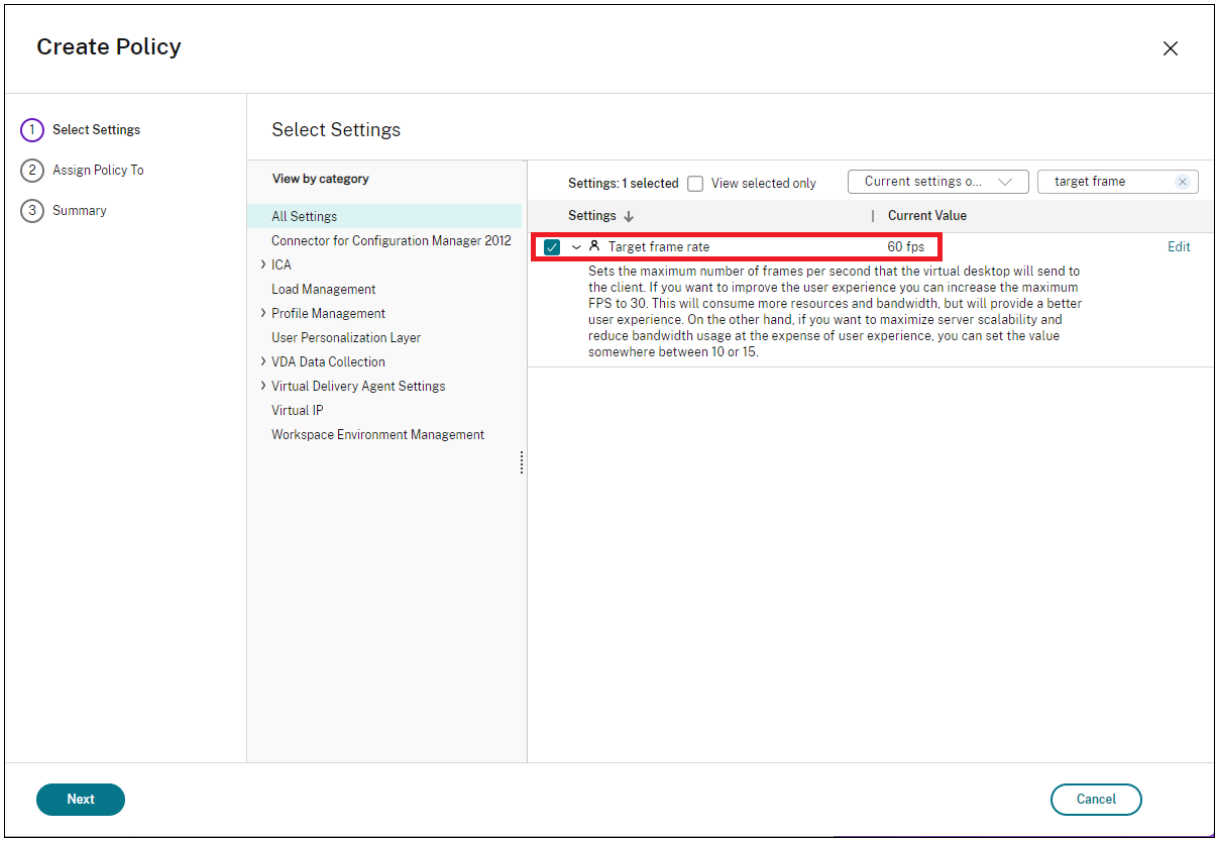
- La résolution minimale requise pour l'affichage virtuel est 640 x 480.
- Le DPI d'affichage virtuel défini via l'interface utilisateur dépend de la prise en charge de la mise à l'échelle du système d'exploitation pour la résolution d'affichage donnée.
- N'utilisez pas cette fonctionnalité simultanément avec la fonctionnalité d'affichage virtuel existante dans l'application Citrix Workspace.
- La fonctionnalité d'aperçu n'est pas prise en charge sur Server 2016.

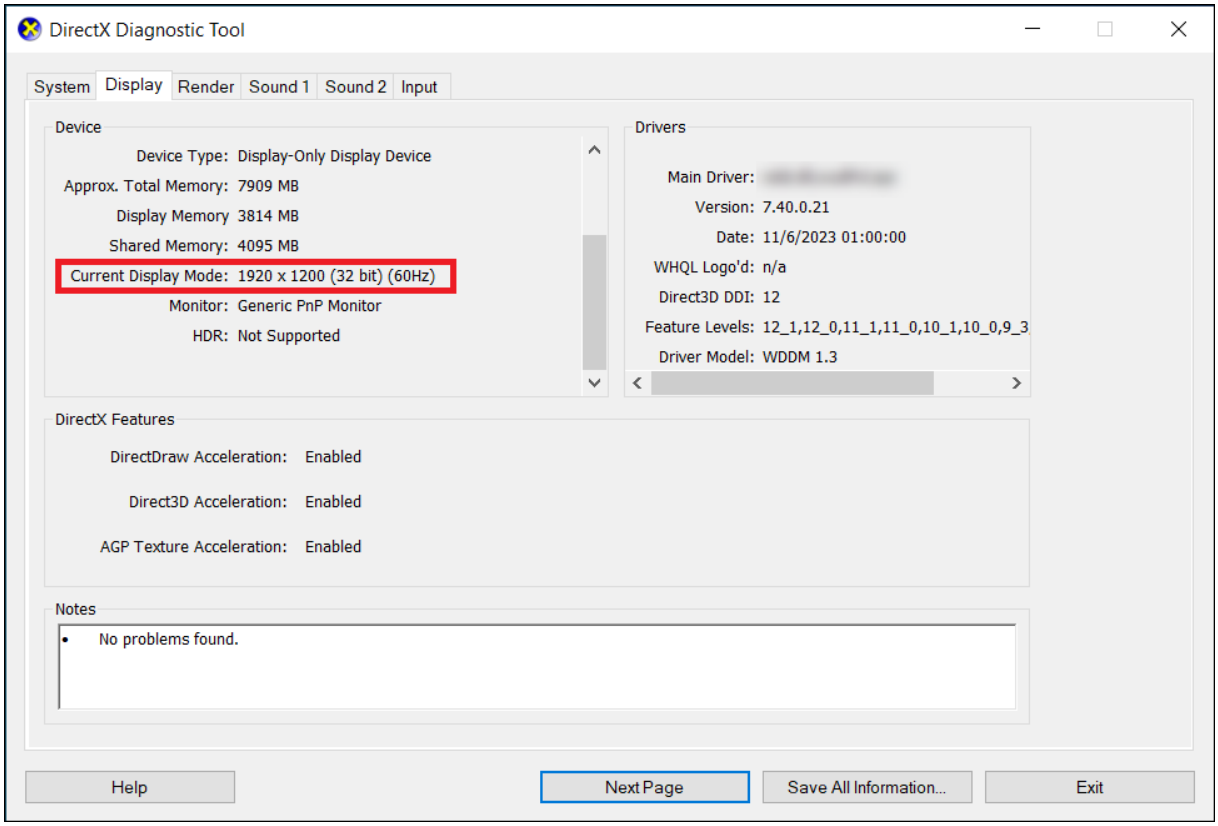
## Taux de rafraîchissement adaptatif

June 27, 2024

Grâce aux nouvelles améliorations d'évolutivité, HDX adapte le taux de rafraîchissement des moniteurs virtuels à la stratégie FPS cible définie. Le taux de rafraîchissement adaptatif (ARR) est disponible pour les VDA mono-session et multi-sessions, et fonctionne à la fois pour les scénarios accélérés par unité de traitement graphique et sans unité de traitement graphique.



> **Remarque**
>
> Le taux de rafraîchissement adaptatif n'est disponible que lorsque Citrix Indirect Display ou IDD est utilisé (selon la valeur par défaut de Citrix Virtual Apps and Desktops) et n'est pas disponible avec les adaptateurs d'affichage fournis par le fournisseur.

## Mode de tolérance aux pertes pour les graphiques

June 27, 2024

Le mode de tolérance aux pertes pour les graphiques a été complètement retravaillé pour garantir que la session reste interactive lorsqu'une perte de paquets est détectée. Lorsque les conditions du réseau se dégradent au-delà des seuils prédéfinis de bande passante, de latence et de perte de paquets, l'encodeur graphique Citrix passe automatiquement à un mode de distribution de paquets plus agressif pour surmonter les effets de la perte de paquets. L'utilisation de la bande passante augmente donc proportionnellement à la quantité de paquets perdus. Si les conditions s'améliorent par la suite, l'encodeur graphique Citrix revient en arrière de manière fluide. Les seuils peuvent être configurés via une stratégie, les valeurs par défaut étant une latence de 300 ms et une perte de paquets de 5 %.

L'application Citrix Workspace pour Windows 2311 est actuellement prise en charge. La prise en charge d'autres plateformes sera ajoutée dans les versions ultérieures de l'application Citrix Workspace. Comme pour les versions précédentes de cette fonctionnalité, le transport adaptatif HDX (EDT) doit être activé pour que cette fonctionnalité fonctionne. En outre, si vous vous connectez via le Citrix Gateway Service, le mode de tolérance aux pertes pour les graphiques doit également être activé sur Gateway.

## Multimédia

June 27, 2024

La pile de la technologie HDX prend en charge la mise à disposition d'applications multimédias via deux approches complémentaires :

- Mise à disposition multimédia avec restitution côté serveur
- Redirection multimédia avec restitution côté client

Cette stratégie permet de vous assurer que vous pouvez mettre à disposition une gamme complète de formats multimédias, avec une expérience utilisateur optimale, lorsque vous maximisez la capacité à monter en charge du serveur pour réduire le coût par utilisateur.

Avec la mise à disposition de multimédia restitué par le serveur, le contenu audio et vidéo est décodé et restitué sur le serveur Citrix Virtual Apps and Desktops par l'application. Le contenu est ensuite compressé et distribué via le protocole ICA à l'application Citrix Workspace sur la machine utilisateur. Cette méthode fournit le taux de compatibilité le plus élevé avec différentes applications et différents formats multimédia. Le traitement des vidéos étant consommateur de ressources, la mise à disposition de multimédia par restitution sur le serveur bénéficie de l'accélération matérielle intégrée. Par exemple, la prise en charge de l'accélération de vidéo DirectX (DXVA) diminue la charge de l'UC en effectuant le décodage H.264 sur un matériel distinct. Les technologies Intel Quick Sync, AMD RapidFire et NVIDIA NVENC fournissent l'encodage H.264 avec accélération matérielle.

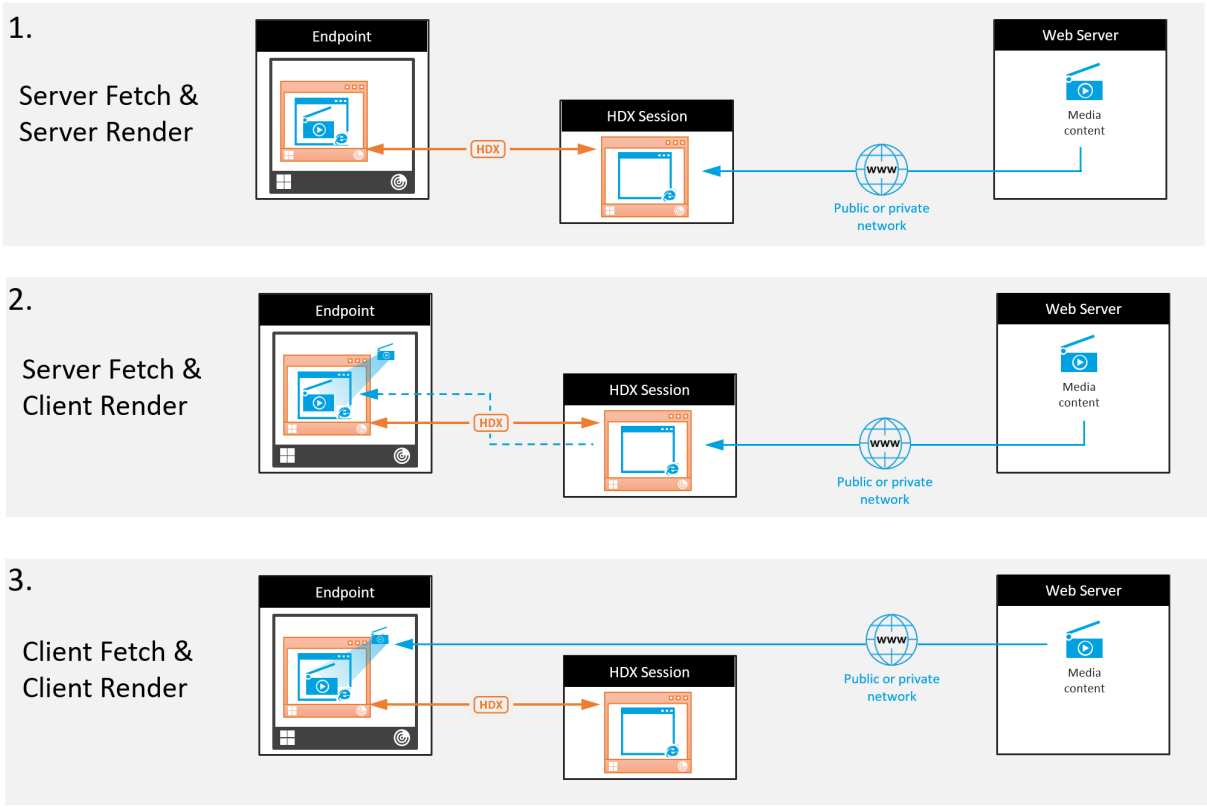
Étant donné que la plupart des serveurs ne proposent pas l'accélération matérielle pour la compression vidéo, la capacité à monter en charge du serveur est affectée si l'intégralité du traitement vidéo est effectué sur l'UC du serveur. Vous pouvez conserver une capacité à monter en charge élevée du serveur, en redirigeant de nombreux formats multimédias vers la machine utilisateur pour une restitution locale.

- La redirection Windows Media déleste le serveur pour un large éventail de formats multimédia généralement associés avec Windows Media Player.
- La vidéo HTML5 est devenue populaire et Citrix a introduit une technologie de redirection pour ce type de contenu. Nous recommandons la redirection du contenu du navigateur pour les sites Web utilisant HTML5, HLS, DASH ou WebRTC.
- Vous pouvez appliquer les technologies de redirection de contact générales Redirection hôte vers client et Local App Access au contenu multimédia.

En combinant ces technologies, si vous ne configurez pas la redirection, HDX effectue la restitution côté serveur.
Si vous configurez la redirection, HDX utilise la méthode Récupération serveur et restitution client ou Récupération client et restitution client. Si ces méthodes échouent, HDX retourne à la restitution du côté serveur si nécessaire et est régi par la stratégie de prévention du retour.

### Exemples de scénarios




**Scénario 1. (Récupération serveur, restitution serveur) :**

1. Le serveur récupère le fichier multimédia à partir de sa source, décode et présente le contenu sur un périphérique audio ou un périphérique d'affichage.
2. Le serveur extrait l'image ou le son présenté(e) depuis le périphérique d'affichage ou le périphérique audio respectivement.
3. Le serveur peut aussi le compresser et le transmettre ensuite au client.

Cette approche entraîne des coûts d'UC élevés, des coûts de bande passante élevés (si l'image ou le son extrait(e) n'est pas compressé(e) efficacement) et ne permet qu'une faible capacité à monter en charge.

Les canaux virtuels Audio et Thinwire utilisent cette approche. Cette approche a pour avantage de réduire la configuration matérielle et logicielle requise pour les clients. Avec cette approche, le décodage se produit sur le serveur et il fonctionne pour une plus grande variété de périphériques et de formats.

**Scénario 2. (Récupération serveur, restitution client) :**

Avec cette approche, le contenu multimédia doit pouvoir être intercepté avant d'être décodé et présenté au périphérique audio ou d'affichage. Le contenu audio/vidéo compressé est envoyé au

client sur lequel il est ensuite décodé et présenté localement. L'avantage de cette approche est que le décodage et la présentation sont déchargés vers les machines clientes, réduisant les cycles d'UC sur le serveur.

Toutefois, elle requiert une configuration logicielle et matérielle supplémentaire pour le client. Le client doit pouvoir décoder chaque format qu'il est susceptible de recevoir.

**Scénario 3. (Récupération client, restitution client) :**

Avec cette approche, l'adresse URL du contenu multimédia doit pouvoir être interceptée avant d'être récupérée depuis la source. L'URL est envoyée au client sur lequel le contenu multimédia est récupéré, décodé et présenté localement. Cette approche repose sur un concept simple. Elle a pour avantage de diminuer les cycles d'UC sur le serveur et la bande passante car le serveur envoie uniquement des commandes. Toutefois, le contenu multimédia n'est pas toujours accessible par les clients.

**Infrastructure et plate-forme :**

Les systèmes d'exploitation mono-session (Windows, Mac OS X et Linux) offrent des infrastructures multimédias permettant le développement plus rapide d'applications multimédias. Ce tableau répertorie certaines des infrastructures multimédias les plus populaires. Chaque infrastructure divise le traitement multimédia en plusieurs étapes et utilise une architecture basée sur pipeline.

| Infrastructure | Plateforme |
|---|---|
| DirectShow | Windows (98 et versions ultérieures) |
| Media Foundation | Windows (Vista et versions ultérieures) |
| Gstreamer | Linux |
| QuickTime | Mac OS X |

## Prise en charge double hop avec les technologies de redirection multimédia

| | | |
|---|---|---|
| | Redirection audio | Non |
| | Redirection de contenu du navigateur | Non |
| | Redirection de webcam HDX | Oui |
| | Redirection vidéo HTML5 | Oui |
| | Redirection Windows Media | Oui |

# Fonctionnalités audio

June 27, 2024

Vous pouvez configurer et ajouter les paramètres de stratégie Citrix suivants pour une stratégie qui optimise les fonctionnalités audio HDX. Pour de plus amples informations sur l'utilisation et les relations et dépendances avec d'autres paramètres de stratégie, consultez la section Paramètres de stratégie audio et Paramètres de stratégie de bande passante et Paramètres de stratégie Connexions Multi-Stream.

## Audio adaptatif

Avec l'audio adaptatif, vous n'avez pas besoin de configurer manuellement les stratégies de qualité audio sur le VDA. L'audio adaptatif optimise les paramètres de votre environnement et remplace les formats de compression audio obsolètes pour offrir une excellente expérience utilisateur.

L'audio adaptatif est activé par défaut. Pour désactiver l'audio adaptatif, consultez la section Paramètres de stratégie audio.

> **Important :**
>
> Citrix recommande de diffuser l'audio à l'aide du protocole UDP (User Datagram Protocol) plutôt que TCP lorsque des applications audio en temps réel sont nécessaires. Les options de transport audio suivantes sont disponibles via UDP :
>
> - Audio sur UDP
> - Transport adaptatif HDX (Enlightened Data Transport)
>
> Le chiffrement audio UDP à l'aide de DTLS n'est disponible qu'entre Citrix Gateway et l'application Citrix Workspace. Par conséquent, il peut parfois être préférable d'utiliser le transport TCP. TCP prend en charge le cryptage TLS de bout en bout depuis le VDA vers l'application Citrix Workspace.
>
> Pour plus d'informations sur le transport audio adaptatif et UDP, reportez-vous à la section Transport audio en temps réel via UDP et plage de ports audio UDP.

## Prise en charge de l'audio via le mode de tolérance aux pertes

Le mode de tolérance aux pertes prend en charge l'audio. Cette fonctionnalité améliore l'expérience utilisateur pour le streaming en temps réel et améliore la qualité audio par rapport à l'EDT lorsque les utilisateurs se connectent via des réseaux à latence élevée et à perte de paquets. Cette fonctionnalité

est désactivée par défaut et la stratégie audio **mode de tolérance aux pertes** doit être activée.

#### Configuration système requise

Assurez-vous que les produits suivants sont aux versions minimales compatibles avec le mode tolérance de pertes :

- Citrix Virtual Delivery Agent (VDA) 2308
- Application Citrix Workspace pour Windows 2309

En outre, les fonctionnalités suivantes doivent être activées :

- Stratégie Transport adaptatif HDX
- (Facultatif) Pour les connexions à distance, Citrix Gateway Service est requis.

> **Remarque :**
>
> Si les conditions ci-dessus ne sont pas remplies, l'audio est envoyé via le transport EDT Reliable.

#### Informations supplémentaires

Le mode tolérance de pertes est un protocole de transport tolérant les pertes qui permet de perdre des paquets lors de la transmission sans renvoyer le contenu multimédia, ce qui se traduit par une meilleure expérience en temps réel pour les utilisateurs.

Enlightened Data Transport (EDT) est un protocole de transport exclusif à Citrix qui offre une expérience utilisateur supérieure sur les connexions longue distance difficiles tout en préservant la capacité à monter en charge des serveurs. Le mode tolérance de pertes est une fonctionnalité de Citrix Gateway Service qui utilise le mode tolérance de pertes comme protocole de transport pour maintenir une connexion stable même en cas de congestion du réseau. Cela garantit une expérience cohérente et stable pour les télétravailleurs. Dans des conditions normales, EDT et le mode tolérance de pertes fournissent des résultats similaires. Toutefois, en cas de perte de paquets sur le réseau, le mode tolérance de pertes offre une meilleure expérience audio par rapport à EDT. Cela en fait une fonctionnalité essentielle pour les télétravailleurs qui utilisent le multimédia en temps réel pour leur travail.

### Qualité audio

En règle générale, une qualité sonore plus élevée consomme plus de bande passante et a une utilisation de l'UC serveur supérieure par le volume des données audio envoyées aux machines utilisateur. La compression du son vous permet d'équilibrer la qualité sonore sur les performances générales

de session ; utilisez les paramètres de stratégie Citrix pour configurer les niveaux de compression à appliquer aux fichiers sonores.

Par défaut, le paramètre de **stratégie de qualité audio** est défini sur Élevée : audio à définition élevée lorsque le transport UDP est utilisé. La stratégie est définie sur Moyen - Optimisé pour la reconnaissance vocale lorsque le transport UDP (recommandé) est utilisé. Le paramètre **Élevée : audio à définition élevée** offre une qualité audio stéréo haute fidélité mais consomme plus de bande passante que les autres paramètres de qualité audio. N'utilisez pas cette qualité audio pour des applications de chat vocal ou de chat vidéo non optimisées (telles que les logiciels de téléphonie). Elle risque d'introduire une latence dans le chemin audio ne convenant pas aux communications en temps réel. Le paramètre de stratégie Optimisée pour le son de la voix est recommandé pour l'audio en temps réel, quel que soit le protocole de transport sélectionné.

Lorsque la bande passante est limitée, pour les connexions par satellite ou par modem par exemple, définir la qualité audio sur **Faible** permet de consommer le minimum de bande passante. Dans ce cas, créez des stratégies distinctes pour les utilisateurs sur connexions à faible bande passante afin que les utilisateurs sur connexions à bande passante élevée ne soient pas affectés.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio. N'oubliez pas d'activer les paramètres audio du client sur la machine utilisateur.

Recommandations de bande passante pour la lecture et l'enregistrement audio :

- Audio adaptatif (par défaut)
  - Bitrate : adaptatif variable
  - Nombre de canaux : 2 (stéréo) pour la lecture, 1 (mono) pour la capture du microphone
  - Fréquence : 48000 Hz
  - Profondeur de bit : 16 bits
- Qualité élevée
  - Débit : ~100 Kbit/s (min 75, max 175 Kbit/s) pour la lecture/~70 Kbit/s pour la capture du microphone
  - Nombre de canaux : 2 (stéréo) pour la lecture, 1 (mono) pour la capture du microphone
  - Fréquence : 44100 Hz
  - Profondeur de bit : 16 bits
- Qualité moyenne (recommandée pour VoIP)
  - Débit : ~16 Kbit/s (min 20, max 40 Kbit/s) pour la lecture, ~16 Kbit/s pour la capture du microphone
  - Nombre de canaux : 1 (mono) pour la lecture et la capture
  - Fréquence : 16000 Hz (large bande)
  - Profondeur de bit : 16 bits

- Qualité inférieure
  - Débit : ~11 Kbit/s (min 10, max 25 Kbit/s) pour la lecture, ~11 Kbit/s pour la capture du microphone
  - Nombre de canaux : 1 (mono) pour la lecture et la capture
  - Fréquence : 8000 Hz (bande étroite)
  - Profondeur de bit : 16 bits

### Redirection audio cliente

Pour autoriser des utilisateurs à recevoir l'audio d'une application sur un serveur au travers de haut-parleurs ou autres périphériques audio sur la machine utilisateur, laissez le paramètre **Redirection audio du client** sur **Autorisée**. Il s'agit de l'option par défaut.

Le mappage audio du client entraîne une charge supplémentaire sur les serveurs et sur le réseau. Cependant, l'interdiction de la redirection audio du client désactive toutes les fonctionnalités HDX audio.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio. N'oubliez pas d'activer les paramètres audio du client sur la machine utilisateur.

### Redirection du microphone client

Pour permettre aux utilisateurs d'enregistrer de l'audio à l'aide de périphériques d'entrée tels que des microphones sur la machine utilisateur, laissez le paramètre **Redirection du microphone client**, sur sa valeur par défaut (Autorisée).

Pour des raisons de sécurité, les machines clientes avertissent leurs utilisateurs si des serveurs non approuvés essaient d'accéder à leurs micros. Les utilisateurs peuvent choisir d'accepter ou de refuser l'accès avant d'utiliser le microphone. Les utilisateurs peuvent désactiver cette alerte sur l'application Citrix Workspace.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio. N'oubliez pas d'activer les paramètres audio du client sur la machine utilisateur.

### Audio Plug N Play

Le paramètre de stratégie Plug N Play audio permet d'autoriser ou d'empêcher l'utilisation de plusieurs périphériques audio pour enregistrer et lire les sons. Cette option est **activée** par défaut. Audio Plug N Play permet de reconnaître les périphériques audio. Les périphériques sont reconnus même s'ils sont connectés une fois que la session de l'utilisateur a été démarrée.

Ce paramètre s'applique uniquement aux machines équipées du système d'exploitation multi-session Windows.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie audio.

### Limite de bande passante de redirection audio et Pourcentage de limite de bande passante de redirection audio

Le paramètre de stratégie de Limite de bande passante de redirection audio spécifie la bande passante maximale (en kilobits par seconde) pour la lecture et l'enregistrement audio dans une session.

Le paramètre Pourcentage de limite de bande passante de la redirection audio spécifie la bande passante maximale pour la redirection audio sous forme de pourcentage de la bande passante totale disponible.

Par défaut, aucun maximum (zéro) n'est spécifié pour les deux paramètres. Si les deux paramètres sont configurés, celui possédant la limite de bande passante la plus basse est utilisé.

Pour plus d'informations sur le paramètre, veuillez consulter la section Paramètres de stratégie de bande passante. N'oubliez pas d'activer les paramètres audio du client sur la machine utilisateur.

### Transport en temps réel audio via UDP et Plage de port UDP audio

Par défaut, le transport en temps réel audio via UDP est autorisé (lorsqu'il est sélectionné au moment de l'installation). Il ouvre un port UDP sur le serveur pour les connexions qui utilisent le transport en temps réel audio via UDP. En cas de surcharge du réseau ou de perte de paquets, nous vous recommandons de configurer l'audio UDP/RTP pour vous assurer la meilleure expérience utilisateur possible. Pour les fonctionnalités d'audio en temps réel telles que les applications softphone, l'audio UDP est préférable à EDT. UDP permet une perte de paquets sans retransmission, évitant ainsi une latence supplémentaire sur les connexions avec perte de paquets élevée.

> **Important :**
>
> Lorsque Citrix Gateway ne se trouve pas sur le chemin, les données audio transmises via UDP ne sont pas cryptées. Si Citrix Gateway est configuré pour accéder aux ressources Citrix Virtual Apps and Desktops, le trafic audio entre la machine de point de terminaison et Citrix Gateway est sécurisé à l'aide du protocole DTLS.

La plage de port UDP audio spécifie la plage de numéros de ports que le VDA pour Windows utilise pour échanger des données de paquet audio avec la machine utilisateur.

Par défaut, la plage se situe entre 16500 et 16509.

> **Remarque :**
>
> Si le transport en temps réel audio via UDP n'est pas requis pour l'audio adaptatif, Citrix recommande de configurer le paramètre de stratégie sur Désactivé. Cela permet d'éviter que les clients de l'application Citrix Workspace ne demandent des connexions UDP ouvertes ou ne déclenchent l'affichage de boîtes de dialogue de configuration du pare-feu du client de l'application Citrix Workspace.

Pour définir les détails relatifs à l'audio via le transport UDP en temps réel, reportez-vous à la section Paramètres de stratégie audio. Pour plus d'informations sur la plage de ports audio UDP, reportez-vous à la section Paramètres de stratégie Connexions Multi-Stream. N'oubliez pas d'activer les paramètres audio du client sur la machine utilisateur.

L'audio via UDP nécessite le VDA Windows. Pour connaître les stratégies prises en charge sur le Linux VDA, consultez la section Liste des stratégies prises en charge.

### Stratégies de configuration audio pour les machines utilisateur

1. Chargez les modèles de stratégie de groupe en suivant les instructions de Configuration avec le modèle d'administration d'objet de stratégie de groupe.
2. Dans l'éditeur de stratégie de groupe, développez **Modèles d'administration > Composants Citrix > Citrix Workspace > Expérience utilisateur**.
3. Pour les **paramètres audio du client**, sélectionnez **Non configuré**, **Activé** ou **Désactivé**.
   - **Non configuré.** Par défaut, la redirection audio est activée avec une qualité audio supérieure ou des paramètres audio personnalisés configurés précédemment.
   - **Activé**. Active la redirection audio à l'aide des options sélectionnées.
   - **Désactivé**. Désactive la redirection audio.
4. Si vous sélectionnez **Activé**, choisissez une qualité audio. Pour l'audio UDP, utilisez **Moyenne** (valeur par défaut).
5. Pour l'audio UDP, sélectionnez **Activer le transport en temps réel** et définissez la plage de ports entrants à ouvrir dans le pare-feu Windows.
6. Pour utiliser l'audio UDP avec Citrix Gateway, sélectionnez **Autoriser le transport en temps réel via Gateway**. Configurez Citrix Gateway avec DTLS. Pour en savoir plus, consultez cet article.

En tant qu'administrateur, si vous n'avez pas de contrôle sur les machines de point de terminaison pour effectuer ces modifications, utilisez le fichier des attributs default.ica de StoreFront pour activer l'audio UDP. Par exemple, si les utilisateurs apportent leurs propres appareils ou ordinateurs personnels.

1. Sur la machine StoreFront, ouvrez C:\inetpub\wwwroot\Citrix\<Nom magasin>\App_Data\default.ica à l'aide d'un éditeur de texte tel que Bloc-notes.
2. Ajoutez les entrées ci-dessous dans la section [Application].

   ; Ce texte active le transport en temps réel

   EnableRtpAudio=true

   ; Ce texte permet le transport en temps réel par passerelle

   EnableUDPThroughGateway=true

   ; Ce texte définit la qualité audio sur Moyen

   AudioBandwidthLimit=1

   ; Plage de ports UDP

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

Si vous activez l'audio UDP en modifiant le fichier default.ica, l'audio UDP est activé pour tous les utilisateurs qui utilisent ce magasin.

### Éviter l'écho pendant les conférences multimédia

Les utilisateurs dans des conférences audio ou vidéo peuvent entendre un écho. Des échos se produisent généralement lorsque les haut-parleurs et les microphones sont trop proches l'un de l'autre. Pour cette raison, nous recommandons l'utilisation de casques pour les conférences audio et vidéo.

HDX offre une option d'annulation de l'écho (activée par défaut), qui réduit l'écho. L'efficacité de l'annulation de l'écho est liée à la distance entre les haut-parleurs et le microphone. Assurez-vous que les machines ne sont pas trop proches ou trop éloignées les unes des autres.

Vous pouvez modifier un paramètre de registre pour désactiver l'annulation de l'écho. Pour plus d'informations, reportez-vous à Éviter l'écho pendant les conférences multimédia dans la liste des fonctionnalités gérées via le Registre.

### Softphones

Un softphone est un logiciel agissant en tant qu'interface téléphonique. Vous utilisez un softphone pour effectuer des appels via Internet à partir d'un ordinateur ou tout autre appareil intelligent. Avec un softphone, vous pouvez composer des numéros de téléphone et effectuer d'autres fonctions téléphoniques depuis un écran.

Citrix Virtual Apps and Desktops prend en charge plusieurs méthodes de mise à disposition de softphone.

- **Mode de contrôle**. Le softphone hébergé contrôle un téléphone physique. Dans ce mode, aucun trafic audio ne transite via le serveur Citrix Virtual Apps and Desktops.
- **Prise en charge de softphone optimisé de HDX RealTime (recommandé)**. Le moteur multimédia est exécuté sur la machine utilisateur et le trafic VoIP circule en mode égal à égal. Par exemple, voir :
  - Optimisation HDX pour Microsoft Teams
  - HDX RealTime Optimization Pack, qui optimise la mise à disposition de Microsoft Skype Entreprise.
  - Cisco Jabber Softphone for VDI (anciennement VXME)
  - Cisco Webex Meetings pour VDI
  - Avaya VDI Equinox (anciennement VDI Communicator)
  - Zoom VDI Plugin
  - Genesys PureEngage Cloud
  - Dictaphone Nuance Dragon PowerMic
- **Local App Access**. Fonctionnalité de Citrix Virtual Apps and Desktops qui permet à une application telle qu'un softphone de s'exécuter localement sur une machine utilisateur Windows tout en semblant être intégré au bureau virtuel/publié. L'intégralité du traitement audio s'effectue sur la machine utilisateur. Pour plus d'informations, voir Local App Access et redirection d'adresse URL.
- **Prise en charge de softphone générique de HDX RealTime.** VoIP sur ICA.

***Prise en charge de softphone générique***

La prise en charge de softphone générique vous permet d'héberger un softphone non modifié sur XenApp ou XenDesktop dans le centre de données. Le trafic audio transite via le protocole Citrix ICA (de préférence à l'aide d'UDP/RTP) vers la machine utilisateur exécutant l'application Citrix Workspace.

La prise en charge de softphone générique est une fonction de HDX RealTime. Cette approche est particulièrement utile lorsque :

- Une solution optimisée pour la mise à disposition du softphone n'est pas disponible et l'utilisateur n'est pas sur une machine Windows sur laquelle Local App Access peut être utilisé.
- Le moteur multimédia requis pour la mise à disposition optimisée du softphone n'a pas été installé sur la machine utilisateur ou n'est pas disponible pour la version de système d'exploitation exécutée sur la machine utilisateur. Dans ce scénario, Generic HDX RealTime fournit une solution alternative.

Deux points doivent être prise en compte concernant la mise à disposition de softphone à l'aide de Citrix Virtual Apps and Desktops :

- La manière dont l'application softphone est mise à disposition sur le bureau virtuel/publié.
- La manière dont l'audio est mis à disposition vers et depuis le casque, le microphone et les haut-parleurs de l'utilisateur ou le téléphone USB.

Citrix Virtual Apps and Desktops inclut de nombreuses technologies pour prendre en charge la mise à disposition de softphone générique :

- Codec optimisé pour le son de la voix pour un codage rapide de l'audio en temps réel et une bande passante efficace.
- Pile audio avec latence faible.
- Tampon de gigue du côté serveur pour réguler l'audio lorsque la latence réseau fluctue.
- Identification des paquets (DSCP et WMM) pour la qualité de service.
  - Identification DSCP pour les paquets RTP (Couche 3)
  - Identification WMM pour le Wi-Fi

Les versions de l'application Citrix Workspace pour Windows, Linux, Chrome et Mac sont également compatibles avec VoIP. L'application Citrix Workspace pour Windows offre ces fonctionnalités :

- Tampon de gigue du côté serveur : régule l'audio lorsque la latence réseau fluctue.
- Annulation de l'écho : permet une plus grande variation de distance entre le micro et les haut-parleurs pour les travailleurs qui n'utilisent pas de casque.
- Audio Plug-n-Play : les appareils audio n'ont pas besoin d'être branchés avant le démarrage d'une session. Ils peuvent être branchés à tout moment.
- Routage du périphérique audio : les utilisateurs peuvent diriger la sonnerie vers les haut-parleurs, mais la voix vers leur casque.
- ICA Multi-stream : permet un routage flexible basé sur la qualité de service à travers le réseau.
- ICA prend en charge quatre flux TCP et deux flux UDP. Un des flux UDP prend en charge l'audio en temps réel sur RTP.

Vous trouverez un récapitulatif des fonctionnalités de l'application Citrix Workspace dans le tableau des fonctionnalités de Citrix Receiver.

***Configuration système recommandée***

*Logiciel et matériel client :*
pour une qualité audio optimale, nous vous recommandons la dernière version de application Citrix Workspace et un casque de bonne qualité avec annulation de l'écho acoustique (AEC). Les versions de l'application Citrix Workspace pour Windows, Linux et Mac prennent en charge VoIP. Dell Wyse offre également la prise en charge de VoIP pour ThinOS (WTOS).

*Unité centrale :*
surveillez l'utilisation de l'UC sur le VDA pour déterminer s'il est nécessaire d'attribuer deux UC virtuelles à chaque machine virtuelle. La voix et la vidéo en temps réel consomment un grand nombre

de données. La configuration de deux UC virtuelles réduit la latence causée par le basculement de thread. Par conséquent, nous vous recommandons de configurer deux UC virtuelles dans un environnement VDI Citrix Virtual Desktops.

Avoir deux UC virtuelles ne signifie pas nécessairement que le nombre d'UC physiques est doublé, car les UC physiques peuvent être partagées par différentes sessions.

Citrix Gateway Protocol (CGP), qui est utilisé pour la fonction de fiabilité de session, augmente également la consommation d'UC. Sur les connexions réseau de qualité élevée, vous pouvez désactiver cette fonctionnalité pour réduire la consommation d'UC sur le VDA. Les étapes précédentes peuvent ne pas être nécessaires sur un serveur puissant.

*Audio UDP :*
la fonctionnalité Audio sur UDP fournit une excellente tolérance face aux congestions du réseau et à la perte de paquets. Nous vous recommandons de la préférer à TCP si elle est disponible.

*Configuration LAN/WAN :*
une configuration correcte du réseau est indispensable à une bonne qualité audio en temps réel. En général, vous devez configurer des réseaux LAN virtuels (VLAN) car des paquets de diffusion excessifs peuvent introduire des effets de gigue. Les machines compatibles IPv6 peuvent générer de nombreux paquets de diffusion. Si la prise en charge IPv6 n'est pas nécessaire, vous pouvez désactiver IPv6 sur ces machines. Effectuez une configuration qui prendra en charge la qualité de service.

*Paramètres pour les connexions WAN :*
vous pouvez utiliser les chats audio via des connexions LAN et WAN. Sur une connexion WAN, la qualité audio dépend de la latence, de la perte de paquets et de la gigue sur la connexion. En cas de mise à disposition de softphones pour les utilisateurs d'une connexion WAN, nous recommandons l'utilisation de NetScaler SD-WAN entre le centre de données et le bureau à distance. Cela permet de maintenir une haute qualité de service. NetScaler SD-WAN prend en charge l'ICA multi-stream, y compris UDP. De plus, pour un flux TCP unique, il est possible de distinguer les priorités de plusieurs canaux virtuels ICA pour vous assurer que les données audio en temps réel à priorité élevée soient traitées en priorité.

Utilisez Director ou HDX Monitor pour valider votre configuration HDX.

*Connexions utilisateur à distance :*
Citrix Gateway prend en charge DTLS pour mettre à disposition le trafic UDP/RTP en mode natif (sans encapsulation dans TCP).
Ouvrez les pare-feu de façon bidirectionnelle pour le trafic UDP sur le port 443.

*Sélection codec et consommation de bande passante* :
entre la machine utilisateur et le VDA dans le centre de données, nous recommandons d'utiliser le paramètre de codec **optimisé pour le son de la voix**, également appelé audio de qualité moyenne. Entre la plate-forme VDA et l'adresse IP-PBX, le softphone utilise le codec configuré ou négocié, quel qu'il soit. Par exemple :

- G711 fournit un son de voix de bonne qualité mais la bande passante doit être de 80 à 100 kilobits par seconde par appel (selon les charges de réseau Layer2).
- G729 fournit un son de voix de bonne qualité et la bande passante requise est faible, de 30 à 40 kilobits par seconde par appel (selon les charges de réseau Layer2).

***Mise à disposition d'applications softphone sur le bureau virtuel***

Il existe deux méthodes que vous pouvez utiliser pour mettre à disposition un softphone sur le bureau virtuel XenDesktop :

- L'application peut être installée sur l'image du bureau virtuel.
- L'application peut être distribuée en streaming sur le bureau virtuel à l'aide de Microsoft App-V. Cette approche présente des avantages en termes de gestion car elle évite d'encombrer l'image du bureau virtuel. Une fois diffusée en streaming sur le bureau virtuel, l'application s'exécute dans cet environnement comme si elle avait été installée de la manière habituelle. Les applications ne sont pas toutes compatibles avec App-V.

***Mise à disposition audio vers et depuis la machine utilisateur***

Generic HDX RealTime prend en charge deux méthodes de mise à disposition de contenu audio vers et depuis la machine utilisateur :

- **Canal virtuel audio Citrix**. Nous recommandons généralement le canal virtuel audio Citrix car il est conçu spécifiquement pour le transport audio.
- **Redirection USB générique**. Prend en charge les périphériques audio avec boutons et/ou les périphériques d'interface utilisateur (HID) à écran, si la machine utilisateur se trouve sur un réseau LAN ou une connexion de type LAN vers le serveur Citrix Virtual Apps and Desktops.

***Canal virtuel audio Citrix***

Le canal virtuel audio Citrix (CTXCAM) bidirectionnel permet une mise à disposition efficace de l'audio via le réseau. Generic HDX RealTime récupère l'audio à partir du casque ou du microphone de l'utilisateur et le compresse. Ensuite, il l'envoie sur ICA à l'application softphone sur le bureau virtuel. De même, la sortie audio du softphone est compressée et envoyée dans l'autre direction vers le casque ou les haut-parleurs de l'utilisateur. Cette compression est indépendante de la compression utilisée par le softphone lui-même (telle que G.729 ou G.711). Elle est effectuée à l'aide du codec optimisé pour le son de la voix (qualité moyenne). Ses caractéristiques sont idéales pour le voice-over-IP (VoIP). Elle propose des temps de codage rapides et consomme uniquement environ 56 Kilobits par seconde de bande passante réseau (28 Kbit/s dans chaque direction), en utilisation maximale. Ce codec doit être explicitement sélectionné dans la console Studio car il ne s'agit pas du codec audio par défaut. La valeur par défaut est le codec HD Audio (haute qualité). Ce codec est excellent pour les pistes audio stéréo haute fidélité mais le codage est plus lent qu'avec le codec optimisé pour le son de la voix.

***Redirection USB générique***

La technologie de redirection USB générique Citrix (canal virtuel CTXGUSB) offre un moyen générique d'accéder à distance aux périphériques USB, y compris les périphériques composites (audio plus HID) et les périphériques USB isochrones. Cette approche est limitée aux utilisateurs connectés au réseau local. En effet, le protocole USB a tendance à être sensible à la latence du réseau et requiert une bande passante réseau considérable. La redirection USB isochrone fonctionne également bien lors de l'utilisation de certains softphones. Cette redirection fournit une excellente qualité de voix et une faible latence. Toutefois, le canal audio virtuel Citrix est préférable car il est optimisé pour le trafic audio. La principale exception est lorsque vous utilisez un périphérique audio avec boutons. Par exemple, un téléphone USB connecté à la machine utilisateur qui est connectée via LAN au centre de données. Dans ce cas, la redirection USB générique prend en charge les boutons du téléphone ou du casque permettant de contrôler les fonctionnalités en envoyant un signal au softphone. Cela n'est pas un problème avec les boutons qui fonctionnent localement sur la machine.

## Outil de ligne de commande de diagnostic audio

L'outil de ligne de commande de diagnostic audio du VDA peut être utilisé pour interroger les données de session liées aux stratégies audio, à la configuration et au transport de données.

### Utilisation

Ouvrez une invite de commande et exécutez `CtxAudio.exe` à partir du dossier `C:\Program Files\Citrix\HDX\bin`.

- L'exécution de l'outil en tant qu'administrateur affiche toutes les informations audio des sessions ICA actives.
- L'exécution de l'outil en tant que non administrateur affiche les informations audio de la session ICA de l'utilisateur actuel.

### Sortie

L'outil génère divers paramètres de configuration qui peuvent aider à diagnostiquer les problèmes audio au cours d'une session.

| Section | Description |
|---|---|
| Informations sur la stratégie | Stratégies audio appliquées aux sessions en cours |
| Informations sur les paramètres | Paramètres de configuration liés à l'audio stockés dans le registre |

| Section | Description |
| --- | --- |
| Informations sur l'état | État audio, version, codecs et transport appliqués aux sessions en cours |
| Informations sur l'appareil | Noms des appareils, rôles et états utilisés au cours de la session. |

> **Remarque :**
>
> La sortie varie selon que vous exécutez l'outil sur un VDA multi-session (TS) ou un VDA mono-session (WSVDA).

### Limitation

Vous installez un périphérique audio sur votre client, activez la redirection audio et démarrez une session RDS. La lecture des fichiers audio peut échouer et un message d'erreur apparaît.

Pour résoudre ce problème, ajoutez la clé de Registre sur la machine RDS, puis redémarrez la machine. Pour plus d'informations, reportez-vous à Limitation audio dans la liste des fonctionnalités gérées via le Registre.

## Redirection de contenu du navigateur

June 27, 2024

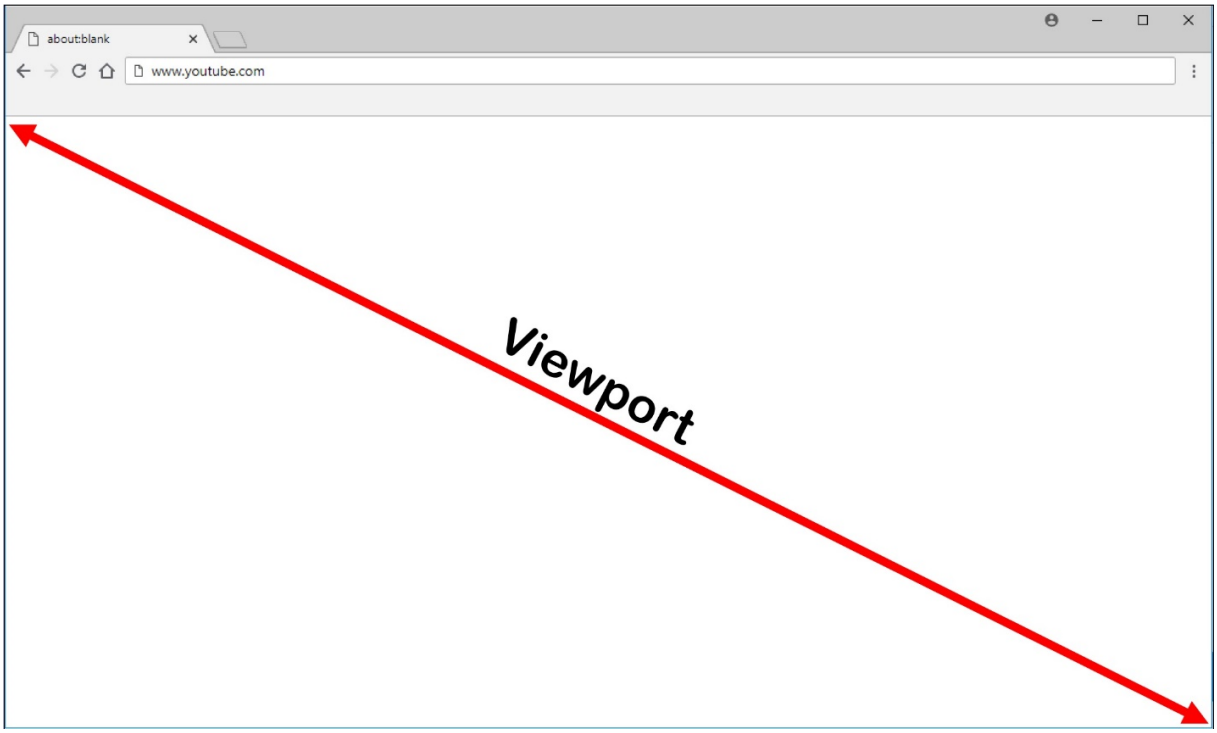
La redirection du contenu du navigateur empêche le rendu des pages Web sur liste d'autorisation du côté VDA. Cette fonctionnalité utilise l'application Citrix Workspace pour Windows ou Citrix Workspace pour Linux pour instancier un moteur de rendu correspondant côté client, qui récupère le contenu HTTP et HTTPS de l'URL.

> **Remarque :**
>
> Vous pouvez spécifier la redirection des pages Web vers le côté VDA (et non la redirection sur le côté client) en utilisant une liste de blocage.

Ce moteur d'affichage Web en superposition est exécuté sur la machine de point de terminaison plutôt que sur le VDA et utilise l'UC, le GPU, la RAM et le réseau du point de terminaison.

Seule la fenêtre d'affichage du navigateur est redirigée. La fenêtre d'affichage est la zone rectangulaire de votre navigateur dans laquelle le contenu s'affiche. La fenêtre d'affichage n'inclut pas certains éléments tels que la barre d'adresses, la barre d'outils **Favoris**, la barre **d'état**. Ces éléments se trouvent dans l'interface utilisateur, qui s'exécute toujours sur le navigateur dans le VDA.




1. Configurez une stratégie Studio qui spécifie une liste de contrôle d'accès contenant les URL sur liste d'autorisation pour la redirection ou une liste de blocage qui désactive la redirection pour des chemins d'URL spécifiques. Pour que le navigateur sur le VDA puisse détecter que l'URL à laquelle l'utilisateur accède figure dans la liste d'autorisation ou ne figure pas dans une liste de blocage, une extension de navigateur effectue la comparaison. Pour Chrome, l'extension de navigateur est disponible dans le Chrome Web Store. Vous pouvez la déployer à l'aide des fichiers de stratégie de groupe et ADMX. Les extensions Chrome sont installées utilisateur par utilisateur. La mise à jour d'une image principale pour ajouter ou supprimer une extension n'est pas requise. Pour Microsoft Edge, l'extension n'est pas disponible directement. Vous devez autoriser les extensions du magasin Chrome pour les rechercher et les installer.
2. Si une correspondance est trouvée dans la liste d'autorisation (par exemple `https://www.mycompany.com/`) et qu'il n'y a pas de correspondance avec une URL dans la liste de blocage (par exemple `https://www.mycompany.com/engineering`), un canal virtuel (CTXCSB) indique à l'application Citrix Workspace qu'une redirection est requise et relaie l'URL. L'application Citrix Workspace instancie alors un moteur de rendu local et affiche le site Web.
3. L'application Citrix Workspace reproduit ensuite de manière transparente le site Web dans la zone de contenu du navigateur de bureau virtuel.

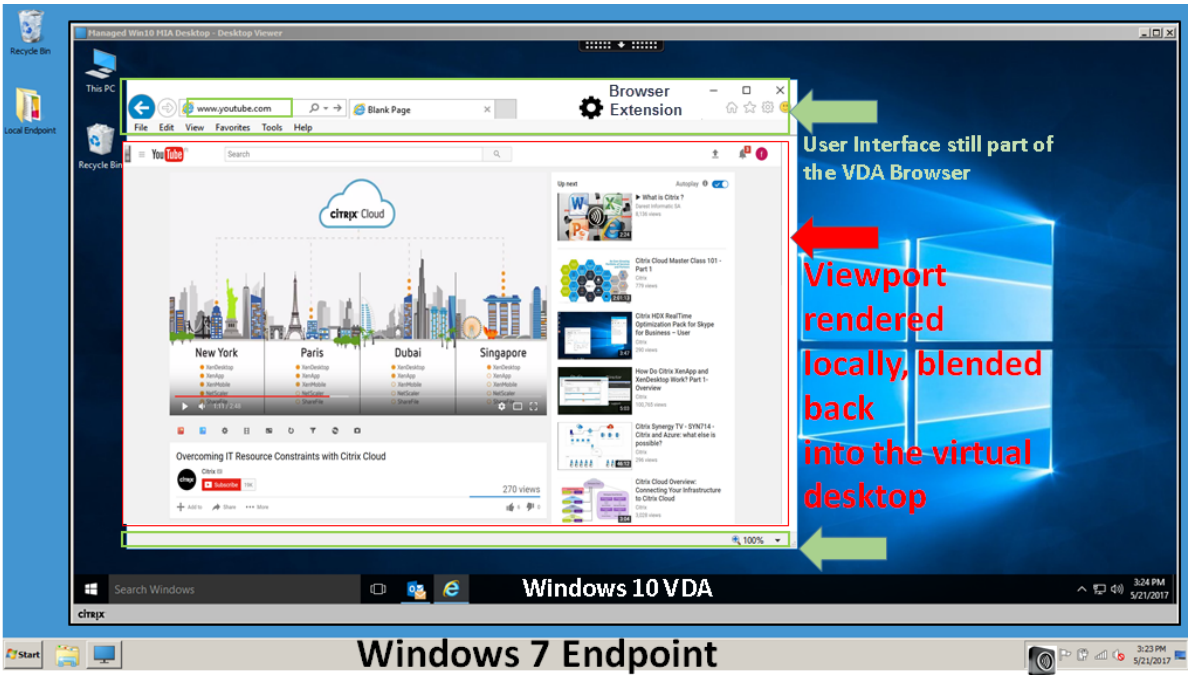
> **Remarque :**
>
> Pour plus d'informations sur les nouveautés et les correctifs relatifs à l'extension de redirection de contenu du navigateur, accédez au Chrome Web Store et recherchez `citrix bcr` pour trouver l'extension.

La couleur du logo indique l'état de l'extension Chrome. Les trois couleurs possibles sont les suivantes :

- Vert : active et connectée.
- Gris : inactive sur l'onglet actuel.
- Rouge : interrompue/ne fonctionne pas.

Vous pouvez enregistrer le débogage en utilisant **Options** dans le menu des extensions.




L'application Citrix Workspace peut récupérer le contenu de trois façons :

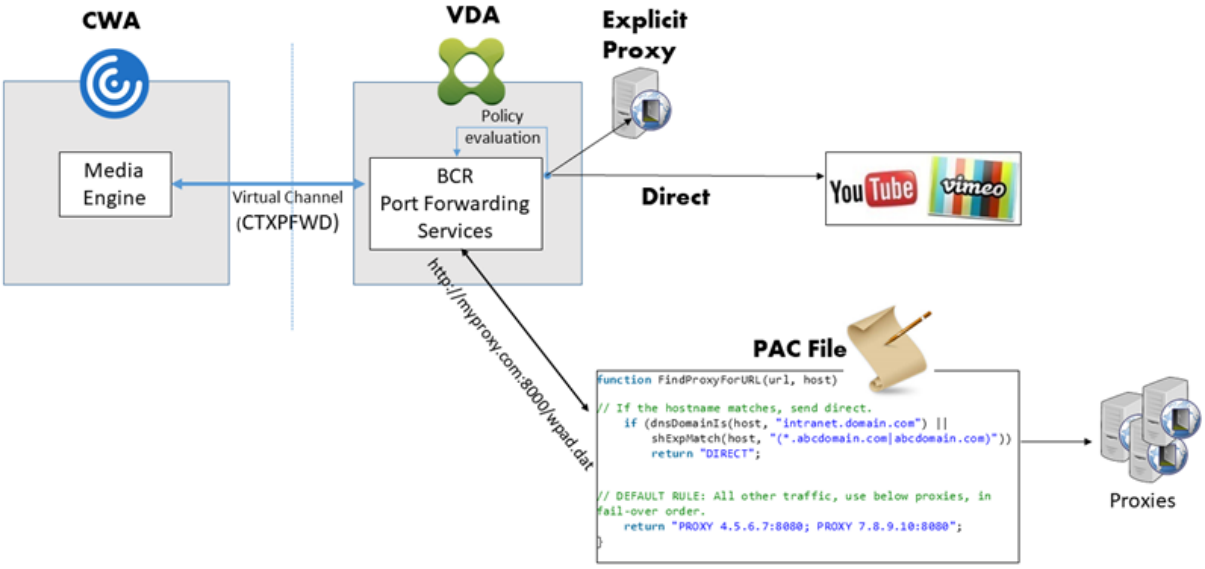
- **Récupération serveur et rendu serveur :** il n'y a pas de redirection car vous n'avez pas ajouté le site à la liste d'autorisation ou la redirection a échoué. Nous revenons au rendu de page Web sur le VDA et utilisons Thinwire pour supprimer les graphiques. Utiliser les stratégies pour contrôler le comportement de secours. Consommation élevée de CPU, de RAM et de bande passante sur le VDA.
- **Récupération serveur et restitution client :** l'application Citrix Workspace contacte et récupère le contenu depuis le serveur Web via le VDA à l'aide d'un canal virtuel (CTXPFWD). Cette option est utile lorsque le client n'a pas accès à Internet (par exemple, les clients légers). Consommation CPU et RAM faible sur le VDA, mais la bande passante est consommée sur le canal virtuel ICA.

  Il existe trois modes de fonctionnement pour ce scénario. Le terme proxy fait référence à un périphérique proxy auquel le VDA accède pour se connecter à Internet.

  Quelle option de stratégie choisir :

- **Proxy explicite :** si vous avez un seul proxy explicite dans votre centre de données.
- **Direct ou Transparent :** si vous n'avez pas de proxy ou si vous utilisez des proxys transparents.
- **Fichiers PAC :** si vous utilisez des fichiers PAC pour que les navigateurs du VDA puissent automatiquement choisir le serveur proxy approprié pour récupérer une URL spécifiée.

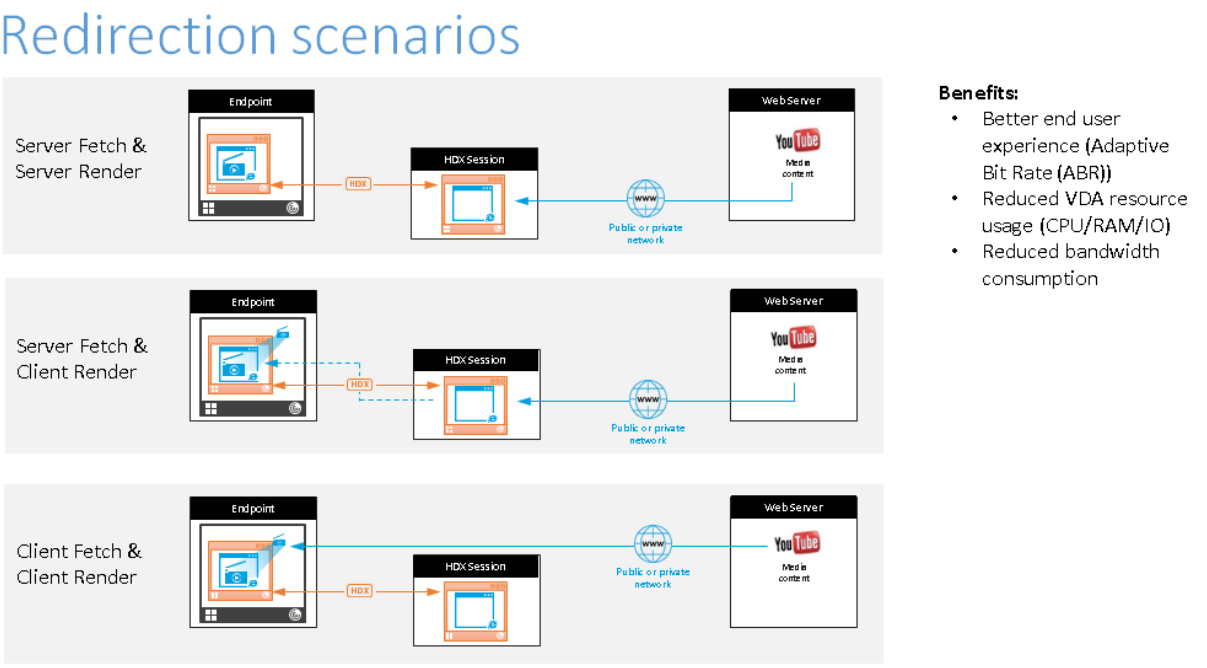



- **Récupération client et rendu client :** l'application Citrix Workspace contacte directement le serveur Web, ce qui nécessite un accès Internet. Ce scénario décharge toute l'utilisation du réseau, du processeur et de la RAM de vos sites XenApp et XenDesktop.

  Avantages :

  - Meilleure expérience pour l'utilisateur final (débit binaire adaptatif (ABR))
  - Réduction de l'utilisation des ressources VDA (CPU/RAM/IO)
  - Réduction de la consommation de bande passante




**Mécanisme de secours :**

Il peut arriver que la redirection du client échoue. Par exemple, si la machine client n'a pas d'accès direct à Internet, une réponse d'erreur peut revenir au VDA. Dans ce cas, le navigateur du VDA peut recharger et afficher la page sur le serveur.

Vous pouvez supprimer la restitution serveur des éléments vidéo à l'aide de la stratégie **Prévention du retour à Windows Media**. Définissez cette règle sur **Lire tout le contenu uniquement sur le client** ou **Lire uniquement le contenu accessible par le client sur le client**. Ces paramètres bloquent la lecture des éléments vidéo sur le serveur en cas d'échec de la redirection vers le client. Cette stratégie prend effet uniquement lorsque vous activez la redirection du contenu du navigateur et que la stratégie **Liste de contrôle d'accès** contient l'URL concernée. L'URL ne peut pas figurer dans la stratégie de liste de blocage.

## Configuration système requise

### Citrix Virtual Apps and Desktops

- Citrix Virtual Apps and Desktops 7 1808 ou version ultérieure
- XenApp et XenDesktop 7.15 CU5 ou version ultérieure
- Système d'exploitation VDA : Windows 10 et 11, Windows Server 2016/2019/2022
- Navigateur sur VDA :
  - Dernière version de Google Chrome
  - Dernière version de Microsoft Edge

- Extension BCR du Chrome Web Store installée sur le navigateur dans le VDA

#### Points de terminaison Windows

- Windows 10 et 11
- Application Citrix Workspace 1809 pour Windows ou version ultérieure

> **Remarque :**
>
> La redirection de contenu du navigateur n'est pas prise en charge pour les versions 1912 et 2203.1 LTSR de l'application Citrix Workspace.

#### Points de terminaison Linux

- Application Citrix Workspace 1808 pour Linux ou version ultérieure
- Les terminaux clients légers doivent inclure WebKitGTK+

#### Points de terminaison Mac (Technical Preview)

- macOS 11 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma (jusqu'à 14.2.1) avec la version minimale de l'application Citrix Workspace 2311

### Dépannage

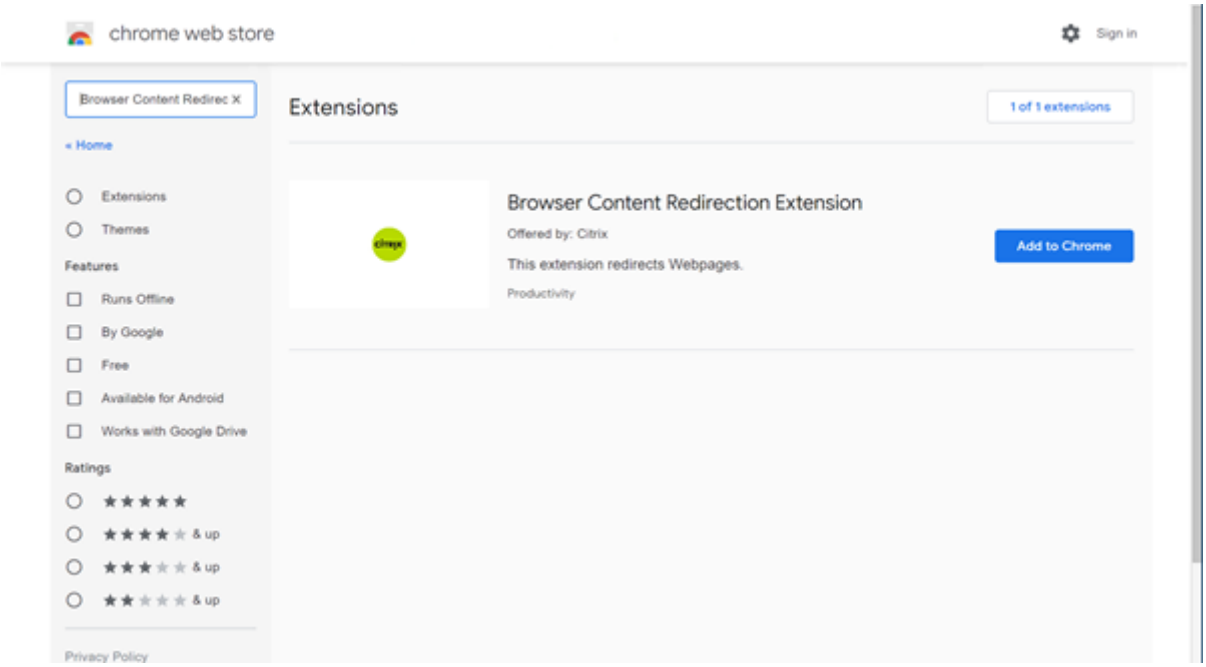
Pour obtenir des informations de dépannage, consultez l'article du Centre de connaissances How to troubleshoot browser content redirection.

### Extension Chrome de redirection du contenu du navigateur

Pour utiliser la redirection du contenu du navigateur avec Chrome, ajoutez l'extension correspondante à partir du Chrome Web Store. Cliquez sur **Ajouter à Chrome** dans l'environnement Citrix Virtual Apps and Desktops.

L'extension **n'est pas** requise sur la machine cliente de l'utilisateur - uniquement dans le VDA.

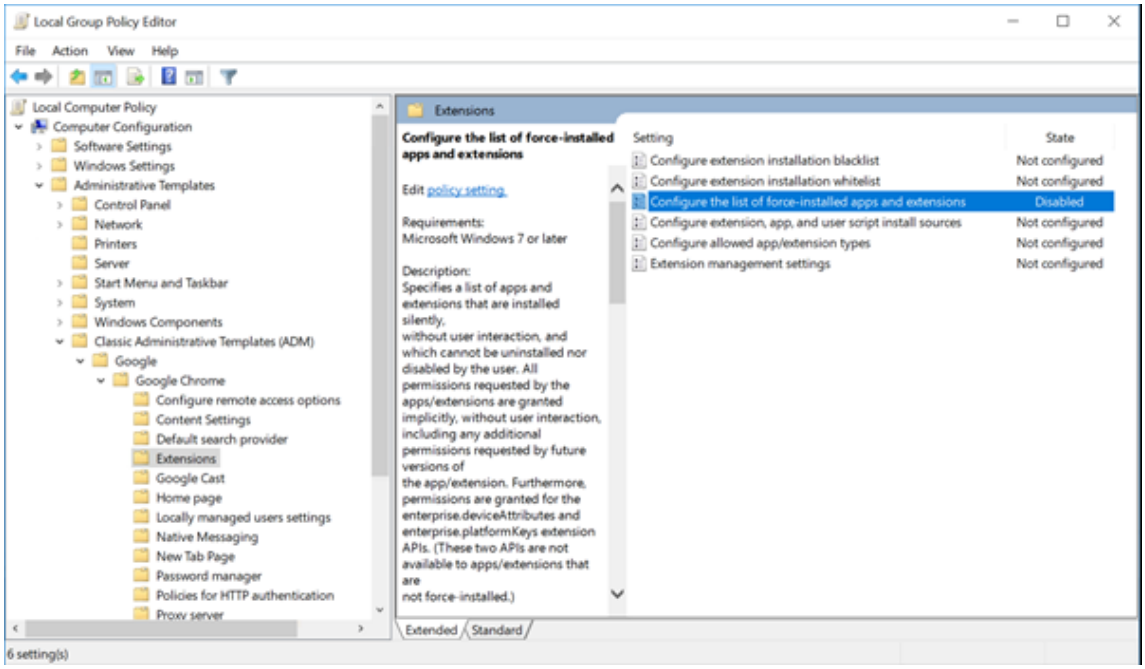



Cette méthode fonctionne pour des utilisateurs individuels. Pour déployer l'extension sur un grand groupe d'utilisateurs de votre organisation, déployez l'extension à l'aide d'une stratégie de groupe.

**Déployer l'extension à l'aide d'une stratégie de groupe**

1. Importez les fichiers ADMX Google Chrome dans votre environnement. Pour plus d'informations sur le téléchargement de modèles de stratégie ainsi que sur l'installation et la configuration de ces modèles dans votre éditeur de stratégie de groupe, voir Définir les stratégies du navigateur Chrome sur les PC gérés.
2. Ouvrez votre console de gestion des stratégies de groupe et accédez à **Configuration utilisateur\Modèles d'administration\Modèles d'administration classiques (ADM)\Google\Google Chrome\Extensions**. Activez le paramètre **Configurer la liste des applications et des extensions installées d'office**.

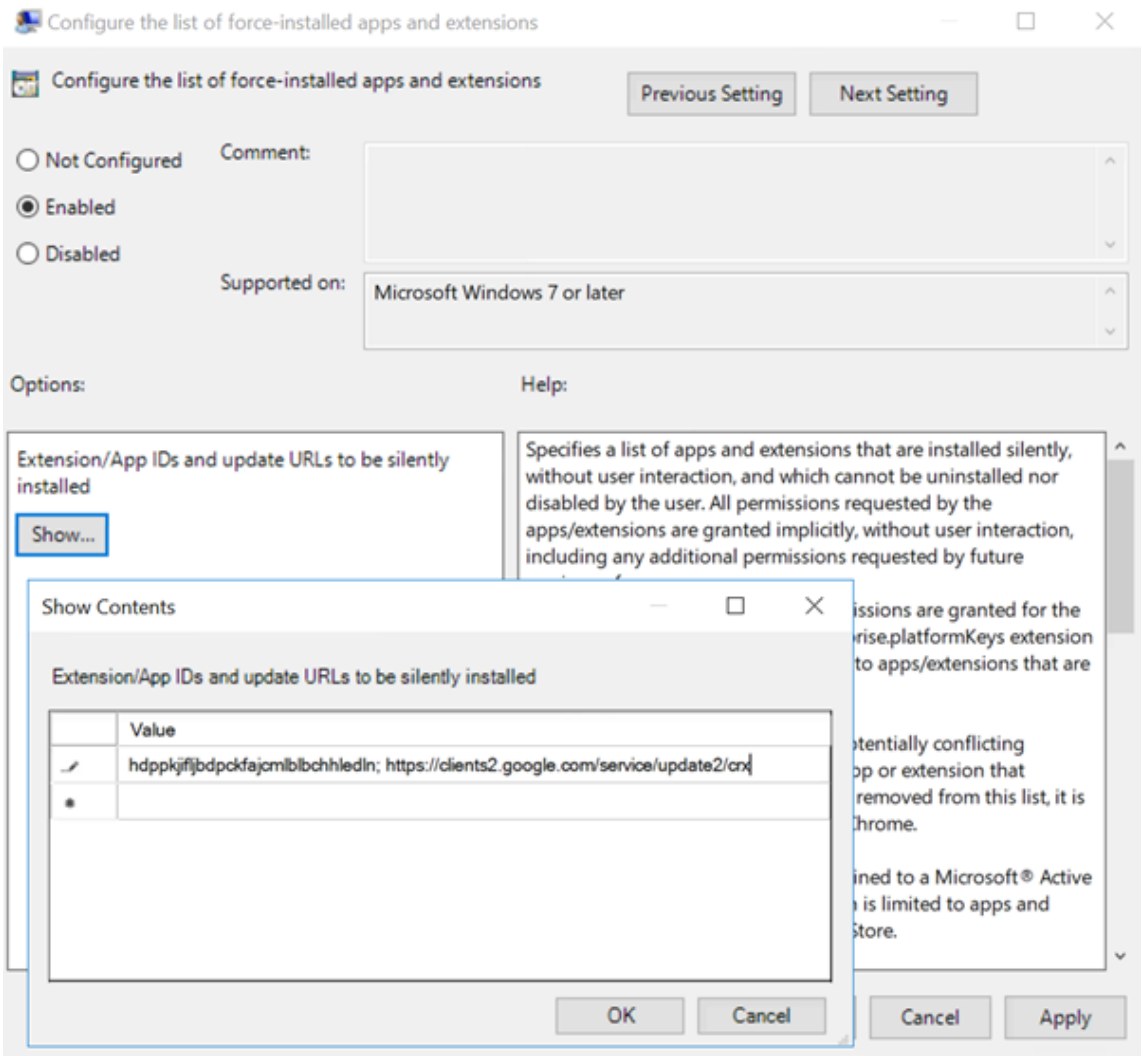
 




3. Cliquez sur **Afficher** et entrez la chaîne suivante, qui correspond à l'ID d'extension. Mettez à jour l'URL de l'extension de redirection du contenu du navigateur.

   ```
   hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
   ```




4. Appliquez le réglage et après une actualisation **gpudate**, l'utilisateur reçoit automatiquement l'extension. Si vous lancez le navigateur Chrome dans la session de l'utilisateur, l'extension est déjà appliquée et il ne peut pas la supprimer.

   Toutes les mises à jour de l'extension sont automatiquement installées sur les ordinateurs des utilisateurs via l'URL de mise à jour que vous avez spécifiée dans le paramètre.

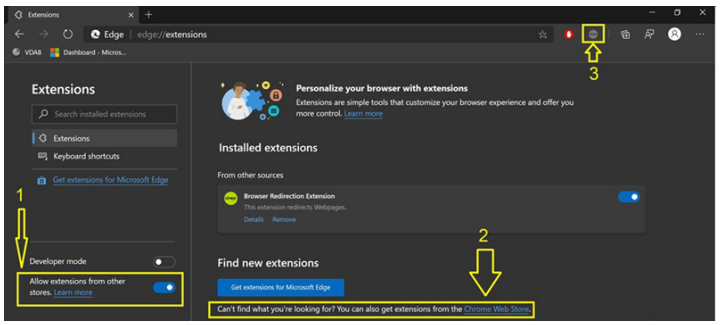
   Si le paramètre **Configurer la liste des applications et des extensions installées d'office** est réglé sur **Désactivé**, l'extension est automatiquement supprimée de Chrome pour tous les utilisateurs.

### Extension de redirection du contenu du navigateur Edge Chromium

Pour installer l'extension de redirection de contenu du navigateur dans Edge, assurez-vous que la version **83.0.478.37** ou supérieure du navigateur Edge est installée.

1. Cliquez sur l'option **Extensions**. Choisissez **Gérer les extensions**. Activez l'option **Autoriser les extensions provenant d'autres magasins**.
2. Cliquez sur le lien **Chrome Web Store** et l'extension apparaît dans la barre en haut à droite. Pour plus d'informations sur les extensions de Microsoft Edge, consultez Extensions.




## Redirection du contenu du navigateur et DPI

Lorsque vous utilisez la redirection de contenu du navigateur avec la mise à l'échelle DPI définie sur une valeur supérieure à 100 % sur la machine de l'utilisateur, l'écran de contenu du navigateur redirigé s'affiche de manière incorrecte. Pour éviter ce problème, ne définissez pas la mise à l'échelle DPI lors de l'utilisation de la redirection de contenu du navigateur. Vous pouvez également éviter ce problème en désactivant l'accélération graphique de redirection de contenu du navigateur pour Chrome et en créant la clé de Registre sur la machine de l'utilisateur. Pour plus d'informations, reportez-vous à Redirection du contenu du navigateur et DPI dans la liste des fonctionnalités gérées via le Registre.

## Authentification unique avec authentification Windows intégrée

La redirection de contenu du navigateur améliore la superposition pour utiliser le schéma **Negotiate** pour l'authentification auprès de serveurs Web configurés avec l'authentification Windows intégrée (IWA) dans le même domaine que le VDA.

Par défaut, la redirection de contenu du navigateur utilise un schéma d'authentification de base qui exige que les utilisateurs s'authentifient avec leurs informations d'identification VDA chaque fois qu'ils accèdent au serveur Web. Pour l'authentification unique, vous pouvez activer le paramètre de stratégie **Browser content redirection Integrated Windows Authentication support** ou créer une clé de Registre sur le VDA.

Avant d'activer l'authentification unique, procédez comme suit :

- Configurez l'infrastructure Kerberos pour émettre des tickets pour les noms principaux de service (SPN) construits à partir du nom d'hôte. Par exemple, `HTTP/serverhostname.com`.
- Pour la récupération serveur : lorsque vous utilisez la redirection de contenu du navigateur en mode récupération serveur, assurez-vous que DNS est correctement configuré sur le VDA.

- Pour la récupération client : lorsque vous utilisez la redirection de contenu du navigateur en mode récupération client, assurez-vous que DNS est correctement configuré sur la machine cliente et que vous autorisez les connexions TCP de la superposition à l'adresse IP du serveur Web.

Pour configurer l'authentification unique à l'aide de la stratégie de redirection de contenu du navigateur, reportez-vous au paramètre Prise en charge de l'authentification Windows intégrée à la redirection de contenu du navigateur.

Vous pouvez également activer l'authentification unique à un serveur Web en ajoutant une clé de Registre sur le VDA. Pour de plus amples informations, consultez la section Authentification unique avec authentification Windows intégrée pour la redirection de contenu du navigateur dans la liste des fonctionnalités gérées via le registre.

### En-tête de requête agent-utilisateur

L'en-tête agent-utilisateur permet d'identifier les requêtes HTTP envoyées à partir de la redirection du contenu du navigateur. Ce paramètre peut être utile lorsque vous configurez des règles de proxy et de pare-feu. Par exemple, si le serveur bloque les requêtes envoyées à partir de la redirection du contenu du navigateur, vous pouvez créer une règle contenant l'en-tête agent-utilisateur pour contourner certaines exigences.

Seuls les périphériques Windows prennent en charge l'en-tête de requête agent-utilisateur.

Par défaut, la chaîne d'en-tête de requête agent-utilisateur est désactivée. Pour activer l'en-tête agent-utilisateur pour le contenu rendu par le client, utilisez l'éditeur du Registre. Pour plus d'informations, reportez-vous à En-tête de requête agent-utilisateur dans la liste des fonctionnalités gérées via le Registre.

### Compatibilité du client avec la redirection du contenu du navigateur

Vous pouvez utiliser WMI pour vérifier si votre client est compatible avec la redirection du contenu du navigateur. Utilisez n'importe quelle méthode d'accès à WMI. Voici un exemple d'utilisation de PowerShell.

1. Ouvrez PowerShell.
2. Exécutez `Get-WmiObject -Class CTXBCRStatus`.
3. Vérifiez le paramètre `BCR_Capable`.
    - Si le paramètre est défini sur `True`, le client est compatible avec la redirection du contenu du navigateur.
    - Si le paramètre est défini sur `False`, le client n'est pas compatible avec la redirection du contenu du navigateur.

**Informations supplémentaires**

- Si `CtxBrowserSvc` n'est pas disponible, aucun résultat n'est affiché lors de l'exécution de la commande.
- Si le paramètre `CtxBrowserSvc` n'a jamais été exécuté, les résultats renvoient une erreur de classe non valide.

### Limitations de la redirection de contenu du navigateur

La redirection de contenu du navigateur ne peut pas prendre en charge les cas d'utilisation suivants :

- Les applications Web qui nécessitent des fenêtres contextuelles ne sont pas prises en charge.
- Les applications Web qui nécessitent la persistance des cookies de session ne sont pas non plus prises en charge.
  Les applications qui dépendent du service d'authentification Google (par exemple, Google Meet) peuvent potentiellement être bloquées.
- Le plug-in d'extension n'est pas officiellement publié sur le magasin Microsoft Edge. Vous pouvez toutefois utiliser le magasin Chrome pour installer les extensions.
- La stratégie de redirection vidéo HTML5 doit être désactivée lorsque la redirection du contenu du navigateur est utilisée.
- La redirection de contenu du navigateur n'est pas prise en charge sur l'infrastructure ARMhf (ARM hard float).
- Les utilisateurs peuvent parfois être déconnectés de leurs sessions en raison d'un manque de fiabilité réseau, de latence réseau très variable ou d'une limite de la portée des périphériques sans fil. À l'heure actuelle, la redirection de contenu du navigateur ne dispose pas de mécanismes de repli ou de reporting suffisants pour de tels scénarios.
- Vous ne pouvez pas télécharger de fichiers ni imprimer sur le navigateur de superposition BCR.

## Conférences vidéo et compression vidéo de webcam HDX

June 27, 2024

> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie

> de sauvegarde de votre registre avant de le modifier.

Les webcams peuvent être utilisées par les applications s'exécutant dans la session virtuelle à l'aide de la compression vidéo de webcam HDX ou de la redirection USB générique plug-n-play HDX. Utilisez **Application Citrix Workspace > Préférences > Périphériques** pour basculer entre les modes. Citrix vous conseille de toujours utiliser la compression vidéo de webcam HDX si possible. La redirection USB générique HDX n'est recommandée que lorsqu'il y a des problèmes de compatibilité des applications avec la compression vidéo HDX ou lorsque vous avez besoin de fonctionnalités natives avancées de la webcam. Pour de meilleures performances, Citrix recommande que le Virtual Delivery Agent dispose d'au moins deux processeurs virtuels.

Pour empêcher les utilisateurs de basculer depuis la compression vidéo de webcam HDX, désactivez la redirection du périphérique USB en utilisant **Paramètres de stratégie sous ICA > Périphériques USB**. Toutefois, les utilisateurs de l'application Citrix Workspace peuvent remplacer le comportement par défaut en choisissant le paramètre Mic & Webcam de Desktop Viewer : **Ne pas utiliser mon micro ou ma webcam**.

### Compression vidéo pour Webcam HDX

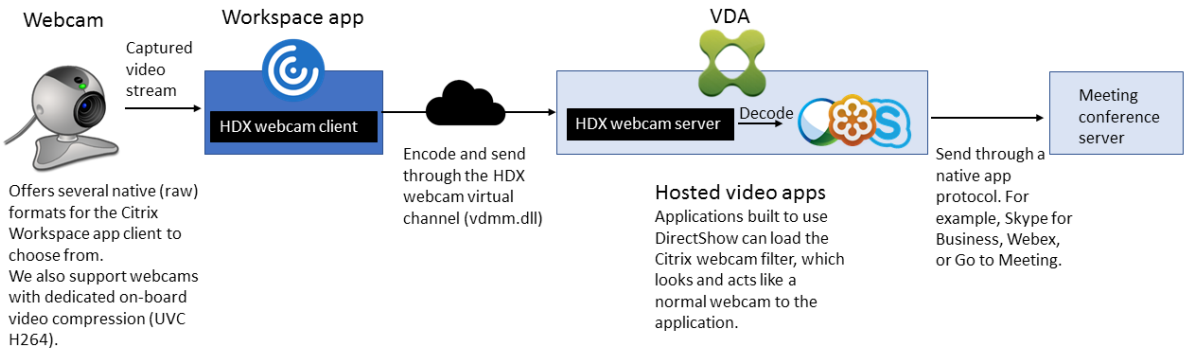
La compression vidéo de webcam HDX est également appelée mode webcam **optimisé**. Ce type de compression vidéo de webcam envoie la vidéo H.264 directement à l'application de visioconférence exécutée dans la session virtuelle. Pour optimiser les ressources VDA, la compression de webcam HDX n'effectue pas de codage, de transcodage ni de décodage de la vidéo webcam. Cette fonctionnalité est activée par défaut.

Pour désactiver la diffusion vidéo directe du serveur vers l'application de visioconférence, définissez la clé de Registre sur 0 sur le VDA. Pour plus d'informations, reportez-vous à Compression vidéo de webcam dans la liste des fonctionnalités gérées via le Registre.

Si vous désactivez la fonctionnalité par défaut pour la diffusion de ressources vidéo en continu, la compression vidéo de webcam HDX utilise la technologie d'infrastructure multimédia faisant partie du système d'exploitation client pour intercepter les vidéos provenant des périphériques de capture, les transcoder et les compresser. Les fabricants de périphériques de capture fournissent des pilotes qui s'intègrent à l'architecture de streaming du noyau du système d'exploitation.

Le client gère la communication avec la webcam. Le client envoie alors la vidéo uniquement au serveur qui peut l'afficher correctement. Le serveur ne communique pas directement avec la webcam, mais il est intégré pour vous offrir la même expérience sur votre bureau. L'application Workspace compresse la vidéo pour économiser de la bande passante et améliorer la résilience avec les scénarios WAN.




La stratégie **Conférences multimédia** doit être activée pour la compression vidéo de webcam HDX. Cette stratégie est activée par défaut.

Si une webcam prend en charge le codage matériel, la compression vidéo HDX utilise le codage matériel par défaut. Le codage matériel peut consommer plus de bande passante que le logiciel de codage. Pour forcer la compression logicielle, modifiez la clé de Registre sur le client. Pour de plus amples informations, consultez la section Compression logicielle webcam dans la liste des fonctionnalités gérées via le registre.

### Configuration requise pour la compression vidéo de webcam HDX

La compression vidéo webcam HDX prend en charge les versions suivantes de l'application Citrix Workspace :

| Plateforme | Processeur |
|---|---|
| Application Citrix Workspace pour Windows | L'application Citrix Workspace pour Windows prend en charge la compression vidéo webcam pour les applications 32 bits et 64 bits sur XenApp et XenDesktop 7.17 et versions ultérieures. Sur les versions antérieures, l'application Citrix Workspace pour Windows ne prend en charge que les applications 32 bits. |
| Application Citrix Workspace pour Mac | L'application Citrix Workspace pour Mac 2006 ou version ultérieure prend en charge la compression vidéo webcam pour les applications 64 bits sur XenApp et XenDesktop 7.17 et versions ultérieures. Sur les versions antérieures, l'application Citrix Workspace pour Mac ne prend en charge que les applications 32 bits. |

| Plateforme | Processeur |
| --- | --- |
| Application Citrix Workspace pour Linux | L'application Citrix Workspace pour Linux prend en charge les applications 32 bits et 64 bits sur le bureau virtuel. |
| Application Citrix Workspace pour Chrome | Étant donné que certains Chromebooks ARM ne prennent pas en charge le codage H.264, seules les applications 32 bits peuvent utiliser la compression vidéo webcam HDX optimisée. |

Les applications vidéo Media Foundation prennent en charge la compression vidéo webcam HDX sur Windows 8.x ou supérieur et Windows Server 2012 R2 et supérieur. Pour plus d'informations, consultez l'article CTX132764 du centre de connaissances.

Autres configurations requises pour la machine utilisateur :

- Un matériel approprié pour produire des sons.
- Une webcam compatible DirectShow (utilisez les paramètres par défaut de la webcam). Des webcams avec encodeur matériel capable de réduire l'utilisation de l'UC du côté client.
- Pour la compression vidéo de webcam HDX, installez les pilotes de webcam sur le client, obtenus auprès du fabricant de la caméra, si possible. L'installation des pilotes de périphériques n'est pas requise sur le serveur.

Différentes webcams offrent des fréquences d'images différentes et ont différents niveaux de luminosité et de contraste. Le réglage du contraste de la webcam peut réduire considérablement le trafic en amont. Citrix utilise les webcams suivantes pour la validation initiale des fonctionnalités :

- Modèles Microsoft LifeCam VX (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600, C920
- Webcam HP Deluxe

Pour ajuster la fréquence d'images vidéo préférée, modifiez la clé de Registre sur le client : Pour plus d'informations, reportez-vous à Fréquence d'images de compression vidéo webcam dans la liste des fonctionnalités gérées via le Registre.

### Streaming de webcam haute définition

L'application de visioconférence sur le serveur sélectionne le format et la résolution de la webcam en fonction des types de format pris en charge. Lors du démarrage d'une session, le client envoie les informations de la webcam au serveur. Choisissez une webcam dans l'application. Lorsque la webcam

et l'application de visioconférence prennent en charge le rendu haute définition, l'application utilise une résolution haute définition. Nous prenons en charge toutes les résolutions de webcam.

Cette fonctionnalité requiert l'application Citrix Workspace pour Windows, version minimale 1808 ou Citrix Receiver pour Windows, version minimale 4.10.

Vous pouvez utiliser une clé de registre pour activer et désactiver la fonctionnalité. Pour de plus amples informations, consultez Streaming de webcam haute définition dans la liste des fonctionnalités gérées via le registre.

Si la négociation du type de média échoue, HDX revient à la résolution VGA par défaut (640 x 480 pixels). Vous pouvez utiliser des clés de Registre sur le client pour configurer la résolution par défaut. Assurez-vous que la caméra prend en charge la résolution spécifiée. Pour de plus amples informations, consultez la section Résolution de webcam haute définition dans la liste des fonctionnalités gérées via le registre.

La compression vidéo webcam HDX utilise beaucoup moins de bande passante par rapport à la redirection USB générique Plug-n-Play et fonctionne bien sur les connexions WAN. Pour ajuster la bande passante, définissez la clé de Registre sur le client. Pour de plus amples informations, consultez Bande passante de webcam haute définition dans la liste des fonctionnalités gérées via le registre.

Entrez une valeur en bits par seconde. Si vous ne spécifiez pas la bande passante, les applications de visioconférence utilisent 350000 bits/s par défaut.

### Redirection USB générique HDX plug-n-play

La redirection USB générique plug-n-play HDX (isochrone) est également appelée mode webcam **générique**. L'avantage de la redirection USB générique plug-n-play HDX est que vous n'avez pas besoin d'installer de pilotes sur votre client léger/terminal. La pile USB est virtualisée de sorte que tout ce que vous branchez sur le client local est envoyé à la machine virtuelle distante. Le bureau distant agit comme si vous l'aviez branché en mode natif. Le bureau Windows gère toutes les interactions avec le matériel et exécute la logique plug-n-play pour trouver les pilotes appropriés. La plupart des webcams fonctionnent si les pilotes existent sur le serveur et peuvent fonctionner sur ICA. Le mode webcam générique utilise beaucoup plus de bande passante (plusieurs mégabits par seconde) car vous envoyez des vidéos non compressées avec le protocole USB sur le réseau.

## Redirection multimédia HTML5

June 27, 2024

La redirection multimédia HTML5 étend les fonctionnalités de redirection multimédia de HDX MediaStream pour inclure des fonctions audio et vidéo HTML5. Face à la croissance de la distribution en

ligne de contenu multimédia, plus particulièrement pour les périphériques mobiles, l'industrie du navigateur a développé des manières plus efficaces de présenter du contenu audio et vidéo.

Flash a longtemps été la norme, mais ce logiciel requiert un plug-in, ne fonctionne pas sur tous les périphériques et consomme davantage de batterie sur les périphériques mobiles. Les sociétés telles que Youtube ou NetFlix et les versions plus récentes des navigateurs de Mozilla, Google et Microsoft se tournent vers HTML5, qui est devenu la nouvelle norme.

Le contenu multimédia basé sur HTML5 présente de nombreux avantages par rapport aux plug-ins propriétaires, y compris :

- Normes indépendantes de la société (W3C)
- Flux de travail DRM (Digital Rights Management) simplifié
- Meilleures performances sans les problèmes de sécurité causés par les plug-ins

### Téléchargements HTTP progressifs

Le téléchargement HTTP progressif constitue une méthode de pseudo-streaming basée sur HTTP qui prend en charge HTML5. Dans un téléchargement progressif, le navigateur lit un seul fichier (codé selon une seule qualité) alors qu'il est en cours de téléchargement à partir d'un serveur Web HTTP. La vidéo est stockée sur le disque au fur et à mesure qu'elle est reçue et lue depuis le disque. Si vous regardez de nouveau la vidéo, le navigateur peut charger la vidéo à partir du cache.

Pour un exemple de téléchargement progressif, veuillez consulter la page de test de redirection vidéo HTML5. Pour inspecter les éléments vidéo dans la page Web et trouver les sources (un format de conteneur mp4) dans les balises vidéo HTML5, utilisez les outils de développement de votre navigateur :

### Comparaison entre HTML5 et Flash

| Fonctionnalité | HTML5 | Flash |
|---|---|---|
| Requiert un lecteur propriétaire | Non | Oui |
| S'exécute sur les périphériques mobiles | Oui | Certains |
| Vitesse de fonctionnement sur différentes plates-formes | Élevé | Slow (Lent) |
| Pris en charge par iOS | Oui | Non |
| Utilisation des ressources | Moins | Plus |
| Chargement plus rapide | Oui | Non |

### Exigences

Nous prenons en charge la redirection uniquement pour les téléchargements progressifs au format mp4. Nous ne prenons pas en charge les technologies WebM et ABS comme DASH/HLS.

Nous prenons en charge les fonctions suivantes et utilisons des stratégies pour les contrôler. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie multimédia.

- Restitution côté serveur
- Restitution client de récupération serveur
- Récupération et restitution côté client

Versions minimales de l'application Citrix Workspace et Citrix Receiver :

- Application Citrix Workspace 1808 pour Windows
- Citrix Receiver pour Windows 4.5
- Application Citrix Workspace 1808 pour Linux
- Citrix Receiver pour Linux 13.5

| Version minimale du navigateur VDA | Version du système d'exploitation Windows/build/SP |
|---|---|
| Internet Explorer 11.0 | Windows 10 x86 (1607 RS1) et x64 (1607 RS1) ; Windows 7 x86 et x64; Windows Server 2016 RTM 14393 (1607) ; Windows Server 2012 R2 |
| Firefox 47 Ajoutez manuellement les certificats au magasin de certificats Firefox ou configurez Firefox pour rechercher les certificats à partir d'un magasin de certificats de confiance Windows. Pour plus d'informations, consultez `https://wiki.mozilla.org/CA:AddRootToFirefox` | Windows 10 x86 (1607 RS1) et x64 (1607 RS1) ; Windows 7 x86 et x64; Windows Server 2016 RTM 14393 (1607) ; Windows Server 2012 R2 |
| Chrome 51 | Windows 10 x86 (1607 RS1) et x64 (1607 RS1) ; Windows 7 x86 et x64; Windows Server 2016 RTM 14393 (1607) ; Windows Server 2012 R2 |

### Composants de la solution de redirection vidéo HTML5

- **HdxVideo.js :** hook JavaScript interceptant les commandes de vidéo sur le site Web. HdxVideo.js communique avec WebSocketService à l'aide de Secure WebSockets (SSL/TLS).
- **Certificats SSL WebSocket**

  - Pour l'autorité de certification (racine) : **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX In-Product CA)
    Emplacement : **Certificats (ordinateur local) > Autorités de certification racines de confiance > Certificats**.
  - Pour l'entité de fin (feuille) : **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp and XenDesktop Engineering; CN = Citrix XenApp and XenDesktop HDX Service)
    Emplacement : **Certificats (ordinateur local) > Personnel > Certificats**.

- **WebSocketService.exe :** s'exécute sur le système local et effectue le mappage de session utilisateur et d'arrêt SSL. TLS Secure WebSocket écoutant le port 9001 127.0.0.1.
- **WebSocketAgent.exe :** s'exécute sur la session utilisateur et restitue la vidéo comme indiqué dans les commandes WebSocketService.

### Activation de la redirection vidéo HTML5

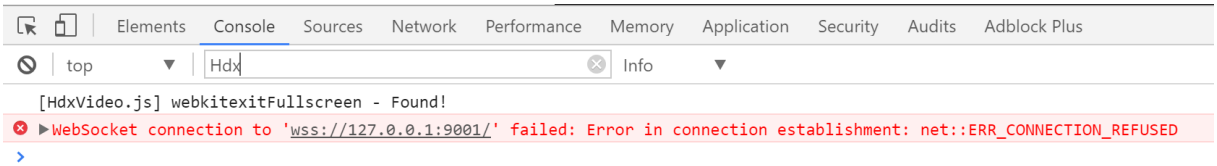
Dans cette version, cette fonctionnalité est disponible pour les pages Web contrôlées uniquement. Elle requiert l'ajout de JavaScript HdxVideo.js (fournie sur le support d'installation de Citrix Virtual Apps and Desktops) aux pages web sur lesquelles le contenu multimédia HTML5 est disponible. Par exemple, des vidéos sur un site de formation interne.

Les sites Web tels que youtube.com, basés sur les technologies à débit adaptatif (par exemple, HTTP Live Streaming (HLS) et Dynamic Adaptive Streaming over HTTP (DASH)), ne sont pas pris en charge.

Pour plus d'informations, veuillez consulter la section *Paramètres de stratégie multimédia*.

### Conseils de dépannage

Des erreurs peuvent se produire lorsque la page Web tente d'exécuter HdxVideo.js. Si JavaScript ne se charge pas, le mécanisme de redirection HTML5 échoue. Assurez-vous qu'il n'existe aucune erreur liée à HdxVideo.js en inspectant la console dans les fenêtres d'outil de développeur de votre navigateur. Par exemple :



# Optimisation pour Microsoft Teams

June 27, 2024

> **Remarque :**
>
> Microsoft Teams 2.1 est désormais généralement disponible pour VDA. Cette version de Microsoft Teams est compatible avec l'optimisation Citrix Microsoft Teams à l'aide de WebRTC (VDI 1.0).
>
> À partir de Citrix Virtual Apps and Desktops 2402, vous n'avez pas besoin de configurer manuellement l'entrée de registre `msedgewebview2.exe`, car elle est mise sur liste verte par défaut.
>
> Les applications publiées sont désormais prises en charge par la nouvelle version de Microsoft Teams.

Citrix offre une optimisation pour Microsoft Teams avec l'application Citrix Workspace et Citrix Virtual Apps and Desktops. Par défaut, nous regroupons tous les composants nécessaires dans l'application Citrix Workspace et le Virtual Delivery Agent (VDA).

Notre optimisation pour Microsoft Teams inclut des services et une API HDX côté VDA afin de créer une interface avec l'application hébergée Microsoft Teams pour recevoir des commandes. Ces composants ouvrent un canal virtuel de contrôle (CTXMTOP) vers Media Engine côté application Citrix Workspace. Le point de terminaison décode et fournit le contenu multimédia localement, en déplaçant la fenêtre de l'application Citrix Workspace vers l'application Microsoft Teams hébergée.

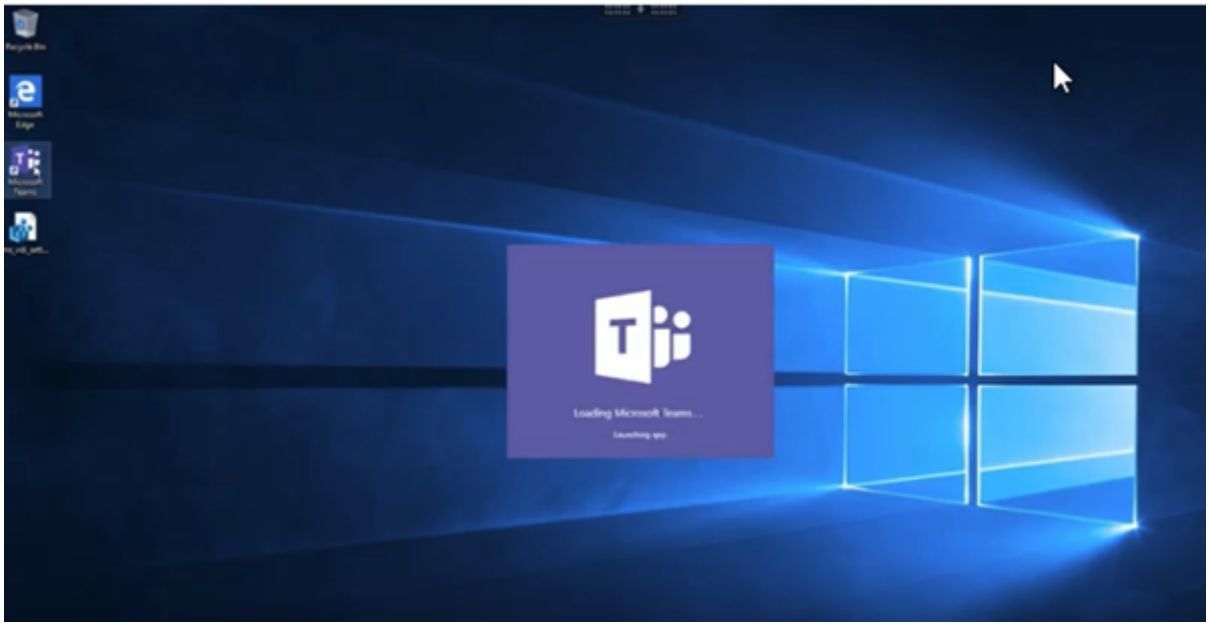
L'authentification et la signalisation se produisent en mode natif sur l'application hébergée par Microsoft Teams, tout comme les autres services Microsoft Teams (par exemple le chat ou la collaboration). La redirection audio/vidéo ne les affecte pas.

`CTXMTOP` est un canal virtuel de commande et de contrôle. Cela signifie que le média n'est pas échangé entre l'application Citrix Workspace et le VDA.

Seule la récupération/restitution client est disponible.

Cette vidéo de démonstration vous donne une idée du fonctionnement de Microsoft Teams dans un environnement virtuel Citrix.



### Installation de Microsoft Teams

Citrix et Microsoft recommandent d'utiliser la dernière version disponible de Microsoft Teams et de la maintenir à jour.
Les versions de l'application de bureau Microsoft Teams dont la date de publication est antérieure de plus de 90 jours à la date de publication de la version actuelle ne sont pas prises en charge.
Les versions non prises en charge de l'application de bureau Microsoft Teams affichent une page de blocage et invitent les utilisateurs à mettre à jour l'application.

Pour plus d'informations sur les dernières versions disponibles, consultez Historique des mises à jour pour l'application Microsoft Teams (ordinateur de bureau et Mac).

Nous vous recommandons de suivre les instructions d'installation de Microsoft Teams à l'échelle de la machine. Évitez d'utiliser le programme d'installation .exe qui installe Microsoft Teams dans `AppData`. Au lieu de cela, effectuez l'installation dans `C:\Program Files (x86)\Microsoft\Teams` en utilisant l'indicateur `ALLUSER=1` de la ligne de commande.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

Cet exemple utilise également le paramètre `ALLUSERS=1`. Lorsque vous définissez ce paramètre, le programme d'installation de Microsoft Teams à l'échelle de la machine s'affiche dans **Programmes et fonctionnalités** du **Panneau de configuration**, ainsi que dans **Applications et fonctionnalités** des Paramètres Windows pour tous les utilisateurs de l'ordinateur. Tous les utilisateurs peuvent ensuite désinstaller Microsoft Teams s'ils possèdent des informations d'identification d'administrateur.

Il est important de comprendre la différence entre `ALLUSERS=1` et `ALLUSER=1`. Vous pouvez utiliser

le paramètre ALLUSERS=1 dans des environnements non-VDI et VDI. Utilisez le paramètre ALLUSER =1 uniquement dans les environnements VDI pour spécifier une installation par machine.

Dans le mode ALLUSER=1, l'application Microsoft Teams ne se met pas à jour automatiquement chaque fois qu'il y a une nouvelle version. Nous recommandons ce mode pour les environnements non persistants, tels que les applications ou bureaux partagés hébergés à partir d'un catalogue Windows Server ou Windows 10 aléatoire/regroupé. Pour plus d'informations, consultez Installer Microsoft Teams à l'aide de MSI (section Installation de VDI).

Supposons que vous disposez d'un environnement VDI permanent dédié Windows 10. Vous souhaitez que l'application Microsoft Teams se mette à jour automatiquement et que Microsoft Teams s'installe par utilisateur sous Appdata/Local. Dans ce cas, utilisez le programme d'installation de .exe ou le MSI sans ALLUSER=1.

> **Remarque :**
>
> Citrix recommande d'installer le VDA avant d'installer Microsoft Teams dans l'image principale. Cet ordre d'installation est nécessaire pour que l'indicateur ALLUSER=1 prenne effet. Si vous avez installé Microsoft Teams sur la machine virtuelle avant le VDA, désinstallez et réinstallez Teams.

### Pour Remote PC Access

Citrix recommande d'installer Microsoft Teams 1.4.00.22472 ou version ultérieure, après avoir installé le VDA. Sinon, vous devez vous déconnecter et vous reconnecter pour que Microsoft Teams détecte le VDA comme prévu. La version 1.4.00.22472 ou supérieure inclut une logique augmentée exécutée au moment du lancement de Microsoft Teams et au moment de la connexion pour la détection du VDA. Ces versions incluent également l'identification du type de session active (HDX, RDP ou connecté localement à la machine cliente). Si vous êtes connecté localement, les versions précédentes de Microsoft Teams peuvent ne pas détecter et désactiver certaines fonctionnalités ou certains éléments de l'interface utilisateur. Par exemple, les salles pour petit groupe, les fenêtres contextuelles pour les réunions et les discussions, ou les réactions aux réunions.

> **Important :**
>
> Lorsque vous passez d'une session locale à une session HDX et que Microsoft Teams reste ouvert et exécuté en arrière-plan, vous devez quitter et relancer Microsoft Teams pour bénéficier de l'optimisation HDX.
> Inversement, si vous utilisez Microsoft Teams à distance via une session HDX optimisée, déconnectez la session HDX et reconnectez-vous à la même session Windows localement sur le périphérique. Lorsque vous travaillez depuis le bureau, vous devez relancer Microsoft Teams afin qu'il puisse détecter correctement l'état Remote PC Access (HDX ou local). Cela est dû au fait que Microsoft Teams peut uniquement évaluer le mode VDI au moment du lancement de l'appli-

> cation, et non lorsqu'elle est déjà en cours d'exécution en arrière-plan. Sans redémarrage, Microsoft Teams risque de ne pas charger des fonctionnalités telles que les fenêtres contextuelles, les salles pour petit groupe ou les réactions dans les réunions.

### Pour App Layering

Si vous utilisez Citrix App Layering pour gérer les installations de VDA et de Microsoft Teams dans différentes couches, vous devez créer une clé de registre sur les VDA Windows avant d'installer Microsoft Teams avec l'indicateur `ALLUSER=1` de la ligne de commande. Pour plus d'informations, consultez la section *Optimisation pour Microsoft Teams avec Citrix App Layering* sous Multimédia.

### Recommandations pour Profile Management

Nous vous recommandons d'utiliser le programme d'installation à l'échelle de la machine pour les environnements Windows Server et VDI Windows 10 regroupés.

Lorsque l'indicateur **ALLUSER =1** est transmis au MSI à partir de la ligne de commande (programme d'installation à l'échelle de la machine), l'application Microsoft Teams s'installe sous `C:\Program Files (x86)` (~300 Mo). L'application utilise `AppData\Local\Microsoft\TeamsMeetingAddin` pour les journaux et `AppData\Roaming\Microsoft\Teams` (entre 600 et 700 Mo approximativement) pour les configurations spécifiques à l'utilisateur, la mise en cache des éléments dans l'interface utilisateur, etc.

> **Important :**
>
> Si vous ne transmettez pas l'indicateur **ALLUSER=1**, le MSI place le programme d'installation de Teams.exe et `setup.json` sous `C:\Program Files (x86)\Teams Installer`. Une clé de registre (TeamsMachineInstaller) est ajoutée sous : `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
>
> La prochaine ouverture de session utilisateur déclenche l'installation finale dans **AppData** à la place.

#### Programme d'installation à l'échelle de la machine

Voici un exemple de dossiers, de raccourcis de bureau et de registres créés par l'installation du programme d'installation de Microsoft Teams sur une machine virtuelle Windows Server 2016 64 bits :

*Dossier :*

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*Raccourci sur le Bureau :*

```
C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe
```

*Registre :*

- `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Nom :`Teams`
- Type : `REG_SZ`
- Valeur : `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **Remarque :**
>
> L'emplacement du Registre varie en fonction des systèmes d'exploitation sous-jacents et du nombre de bits.

#### Recommandations

- Nous vous recommandons de désactiver le démarrage automatique en supprimant les clés de registre Microsoft Teams. Cela empêche les nombreuses ouvertures de session qui se produisent en même temps (par exemple, au début de votre journée de travail) d'augmenter le processeur de la machine virtuelle.
- Si le bureau virtuel ne dispose pas d'un GPU/VGPU, nous vous recommandons d'utiliser le paramètre **Désactiver l'accélération matérielle du GPU** dans les **paramètres** de Microsoft Teams pour améliorer les performances. Ce paramètre (`"disableGpu":true`) est stocké sous `%Appdata%\Microsoft\Teams` dans `desktop-config.json`. Vous pouvez utiliser un script d'ouverture de session pour modifier ce fichier et définir la valeur sur `true`.
- Si vous utilisez Citrix Workspace Environment Management (WEM), activez la **protection contre les pics CPU** pour gérer la consommation de processeur pour Microsoft Teams.

#### Programme d'installation par utilisateur

Lors de l'utilisation du programme d'installation de `.exe`, le processus d'installation diffère. Tous les fichiers sont placés dans AppData.

*Dossier :*

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`

- C:\Users\<username>\AppData\Local\SquirrelTemp
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

*Raccourci sur le Bureau :*

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --
processStart "Teams.exe"
```

*Registre :*

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

#### Recommandations

Les recommandations sont basées sur les scénarios de cas d'utilisation.
L'utilisation de Microsoft Teams avec une configuration non persistante nécessite un gestionnaire de mise en cache des profils pour une synchronisation efficace des données d'exécution de Microsoft Teams. Lorsqu'un gestionnaire de mise en cache des profils est utilisé, les informations utilisateur appropriées sont mises en cache pendant la session utilisateur. Par exemple, les informations spécifiques à l'utilisateur incluent les données utilisateur, le profil et les paramètres. Synchronisez les données dans ces deux dossiers :

- C:\Users\<username>\AppData\Local\Microsoft\IdentityCache
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

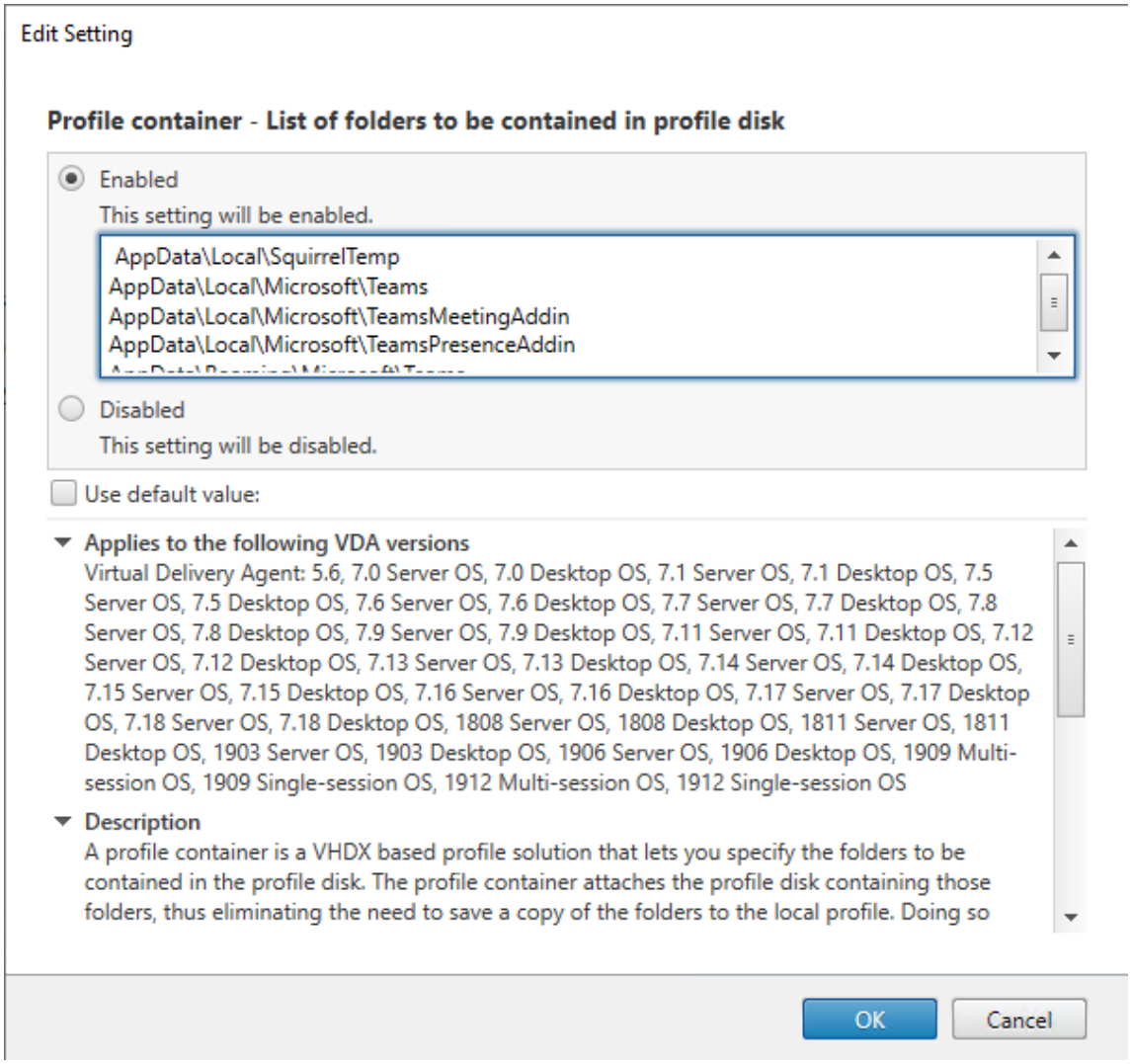
**Liste d'exclusion de contenu mis en cache par Microsoft Teams pour une configuration non persistante** Excluez les fichiers et les répertoires du dossier de mise en cache Microsoft Teams, comme décrit dans la documentation Microsoft. Cette action vous permet de réduire la taille de la mise en cache des utilisateurs afin d'optimiser davantage votre configuration non persistante.

**Cas d'utilisation : scénario de mono-session** Dans ce scénario, l'utilisateur final utilise Microsoft Teams dans un seul emplacement à la fois. Il n'a pas besoin d'exécuter Microsoft Teams dans deux sessions Windows en même temps. Dans un déploiement de bureau virtuel commun, chaque utilisateur est affecté à un bureau, et Microsoft Teams est déployé dans le bureau virtuel en tant qu'application unique.
Nous vous recommandons d'activer le conteneur Citrix Profile et de rediriger les répertoires par utilisateur répertoriés dans Programme d'installation par utilisateur dans le conteneur.

1. Déployez le programme d'installation de Microsoft Teams (**ALLUSER=1**) dans l'image principale.
2. Activez Citrix Profile Management et configurez le magasin de profils utilisateur avec les autorisations appropriées.

3. Activez le paramètre de stratégie Profile Management suivant : **Système de fichiers > Synchronisation > Conteneur de profil —Liste des dossiers devant figurer dans le disque de profil**.




   Liste tous les répertoires par utilisateur dans cette configuration. Vous pouvez également configurer ces paramètres à l'aide du service Citrix Workspace Environment Management (WEM).

4. Appliquez les paramètres au groupe de mise à disposition approprié.
5. Connectez-vous pour valider le déploiement.

## Configuration système requise

### Version minimale recommandée - Delivery Controller (DDC) 1906.2

Si vous utilisez une version antérieure, consultez Activer l'optimisation pour Microsoft Teams :

Systèmes d'exploitation pris en charge :

- Windows Server 2022, 2019, 2016, 2012R2 éditions Standard et Datacenter, avec option Server Core

**Version minimale - Virtual Delivery Agents (VDA) 1906.2**

Systèmes d'exploitation pris en charge :

- Windows 11
- Windows 10 64 bits, versions 1607 et supérieures. Les applications hébergées par des machines virtuelles sont prises en charge par l'application Citrix Workspace pour Windows 2109.1 ou version ultérieure
- Windows Server 2022, 2019, 2016 et 2012 R2 (éditions Standard et Datacenter)

Exigences :

- BCR_x64.msi - MSI qui inclut le code d'optimisation pour Microsoft Teams et démarre automatiquement à partir de l'interface graphique. Si vous utilisez l'interface de ligne de commande pour l'installation du VDA, ne l'excluez pas.

**Version recommandée : application Citrix Workspace pour Windows version la plus récente et version minimale, application Citrix Workspace 1907 pour Windows**

- Windows 11.
- Windows 10 (éditions 32 bits et 64 bits, y compris les éditions Embedded) (la prise en charge de Windows 7 a été abandonnée à la version 2006) (la prise en charge de Windows 8.1 a été abandonnée à la version 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (v1607) et 2019 LTSC (v1809).
- Architectures de processeur (CPU) prises en charge : x86 et x64 (ARM n'est pas pris en charge).
- Exigences pour le point de terminaison : CPU double cœur d'environ 2,2 - 2,4 GHz pouvant prendre en charge la résolution HD 720p lors d'une visioconférence égal à égal.
- CPU double ou quadruple cœur avec des vitesses de base plus faibles (~1,5 GHz) équipés d'Intel Turbo Boost ou AMD Turbo Core pouvant augmenter jusqu'à 2,4 GHz au moins.
- Clients légers HP vérifiés : t630/t640, t730/t740, mt44/mt45.
- Clients légers Dell vérifiés : 5070, 5470 Mobile TC et AIO.
- Clients légers 10ZiG vérifiés : 4510 et 5810q.
- Pour obtenir la liste complète des points de terminaison vérifiés, reportez-vous à Clients légers.
- L'application Citrix Workspace requiert une capacité minimale de 600 Mo d'espace disque disponible et 1 Go de RAM.
- La configuration minimale requise pour Microsoft .NET Framework est la version 4.8. L'application Citrix Workspace télécharge et installe automatiquement .NET Framework s'il n'est pas présent dans le système.

Les administrateurs peuvent activer/désactiver le démarrage en mode optimisé de Microsoft Teams en modifiant la stratégie Optimisation pour Microsoft Teams. Les utilisateurs qui démarrent en mode optimisé dans l'application Citrix Workspace ne peuvent pas désactiver Microsoft Teams.

#### Version minimale - Application Citrix Workspace 2006 pour Linux

Pour plus d'informations, consultez la section Optimisation pour Microsoft Teams dans la documentation de l'application Citrix Workspace pour Linux.

Logiciel :

- `GStreamer` 1.0 ou version ultérieure ou Cairo 2
- `libc++-9.0` ou version ultérieure
- `libgdk` 3.22 ou version ultérieure
- OpenSSL 1.1.1d
- `libnsl`
- Ubuntu 20.04 ou version ultérieure

Amélioration de l'authentification :

- Bibliothèque libsecret
- Bibliothèque libunwind-12 Pour de plus amples informations, consultez la section Ajouter la dépendance de la bibliothèque libunwind-12 pour llmachine virtuelle-12.

Matériel :

- CPU double cœur de 1,8 GHz minimum pouvant prendre en charge une résolution HD 720p lors d'une vidéoconférence pair à pair
- CPU double ou quadricœur avec une vitesse de base de 1.8 GHz et une vitesse Intel Turbo Boost élevée d'au moins 2.9 GHz

Pour obtenir la liste complète des points de terminaison vérifiés, reportez-vous à Clients légers.

Pour plus d'informations, consultez la section Conditions préalables à l'installation de l'application Citrix Workspace.

Vous pouvez désactiver l'optimisation pour Microsoft Teams en définissant la valeur du champ **VDWEBRTC** sur Off dans le fichier `/opt/Citrix/ICAClient/config/module.ini`. La valeur par défaut est VDWebRTC=On. Une fois la mise à jour terminée, redémarrez la session. ( L'autorisation racine est requise).

#### Version minimale - Application Citrix Workspace 2012 pour Mac

Systèmes d'exploitation pris en charge :

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 ou supérieur.
- macOS Monterey.

Fonctions prises en charge :

- Audio
- Vidéo
- Optimisation du partage d'écran (entrant et sortant)

> **Remarque :**
>
> L'application Citrix Viewer nécessite l'accès aux préférences Sécurité et confidentialité de macOS pour que le partage d'écran fonctionne. Les utilisateurs configurent cette préférence dans le **menu Apple > Préférences système > Sécurité et confidentialité > onglet Confidentialité > Enregistrement d'écran** et sélectionnez **Citrix Viewer**.

L'optimisation Microsoft Teams fonctionne par défaut avec l'application Citrix Workspace 2012 ou version ultérieure et macOS 10.15.

Si vous souhaitez désactiver l'optimisation Microsoft Teams, exécutez cette commande dans un terminal et redémarrez l'application Citrix Workspace :

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

#### Version minimale : dernière version de l'application Citrix Workspace pour ChromeOS exécutée sur la dernière version de ChromeOS

Matériel :

- Processeurs dont les performances sont égales ou supérieures à celles d'Intel i3, quadricœur 2,4 GHz.

Fonctions prises en charge :

- Audio
- Vidéo
- Optimisation du partage d'écran (entrant et sortant) - désactivée par défaut. Consultez ces paramètres pour obtenir des instructions sur la façon de l'activer.

### Capacité du serveur à monter en charge

Cette section fournit des recommandations et des conseils pour estimer le nombre d'utilisateurs ou de machines virtuelles (machine virtuelle) pouvant être pris en charge sur un seul hôte physique.

Cette fonction est généralement appelée Citrix Virtual Apps and Desktops Single Server Scalability (SSS). Dans le contexte de Citrix Virtual Apps (CVA) ou de virtualisation de session, elle est également connue sous le nom de densité utilisateur. L'idée est de savoir combien d'utilisateurs ou de machines virtuelles peuvent être exécutés sur un seul matériel exécutant un hyperviseur majeur.

> **Remarque :**
>
> Cette section inclut des conseils pour estimer le SSS. Les conseils sont généraux et ne sont pas nécessairement spécifiques à votre situation ou à votre environnement unique. La seule façon de véritablement comprendre la fonction Citrix Virtual Apps and Desktops SSS est d'utiliser un outil de test de capacité à monter en charge ou de charge tel que Login VSI. Citrix recommande d'utiliser ces conseils et ces règles simples pour estimer rapidement le SSS uniquement. Citrix recommande toutefois d'utiliser Login VSI ou l'outil de test de charge de votre choix pour valider les résultats, en particulier avant d'acheter du matériel ou de prendre des décisions financières.

#### Matériel (système en cours de test)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 à 2,60 GHz (max Turbo 3,70 GHz), 12 cœurs par socket, double socket avec hyper-threading activé
- 382 Go de RAM
- Stockage SSD RAID 0 local (11 disques) 6 To

#### Logiciel

Une machine virtuelle unique (40 processeurs logiques) avec Windows 2019 (TSVDA) exécutant Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

#### Terminologie

- Charge de travail des travailleurs du savoir : comprend Acrobat Reader, Freemind/Java, la visionneuse de photos, Edge et les applications MS Office telles qu'Excel, Outlook, PowerPoint et Word
- Charge de travail de base : tests de capacité du serveur à monter en charge exécutés avec la charge de travail des travailleurs du savoir (sans Microsoft Teams)
- Charge de travail Microsoft Teams : charge de travail type des travailleurs du savoir + Microsoft Teams

**Comment Microsoft Teams est soumis à des tests de contrainte**

- Microsoft Teams est optimisé avec HDX. Par conséquent, tout le traitement multimédia est déchargé vers le terminal ou le client et ne fait pas partie de la mesure.
- Tous les processus Microsoft Teams sont arrêtés avant le début de la charge de travail.
- Ouvrez Microsoft Teams (démarrage à froid).
- Mesurez le temps mis par Microsoft Teams pour charger et sélectionner le focus de la fenêtre principale de Microsoft Teams.
- Passez à la fenêtre de chat à l'aide des raccourcis clavier.
- Passez à la fenêtre de calendrier à l'aide des raccourcis clavier.
- Envoyez le message de chat à un utilisateur spécifique à l'aide des raccourcis clavier.
- Accédez à la fenêtre Microsoft Teams à l'aide des raccourcis clavier.

**Résultats**

- Un impact de 40 % est observé sur la capacité à monter en charge avec la charge de travail Microsoft Teams (81 utilisateurs) par rapport à la charge de travail de base (137 utilisateurs).
- L'augmentation de la capacité du serveur d'environ 40 % (en CPU) restaure le nombre d'utilisateurs comme avec la charge de travail de base.
- 20 % de mémoire supplémentaire est requise avec la charge de travail Microsoft Teams par rapport à la charge de travail de base.
- La taille de stockage par utilisateur a augmenté de 512 à 1 024 Mo.
- Une augmentation d'environ 50 % du nombre d'E/S par seconde en écriture et une augmentation d'environ 100 % du nombre d'E/S par seconde en lecture ont été observées. Microsoft Teams peut avoir un impact significatif dans un environnement où le stockage est plus lent.

## Tableau des fonctionnalités et versions prises en charge

| Fonctionnalité | Microsoft Teams (version minimale) | VDA (version minimale) | Application Citrix Workspace pour Windows CR (version minimale) | Application Citrix Workspace pour Mac (version minimale) | Application Citrix Workspace pour Linux (version minimale) | Application Citrix Workspace pour ChromeOS (version minimale) |
|---|---|---|---|---|---|---|
| Audio/Vidéo (P2P et conférence) | Version actuelle moins 90 jours | 1906 | 1907 | 2009 | 2004 | 2105.5 |
| Partage d'écran | Version actuelle moins 90 jours | 1906 | 1907 | 2012 | 2006 | 2105.5 |
| i. Bordure rouge indicateur d'écran | Version actuelle moins 90 jours | 1906 | 2002 | 2012 | 2006 | Non |
| ii. Limitation de la capture à Desktop Viewer | Version actuelle moins 90 jours | 1906 | 2009.5 | 2012 | 2006 | Non |
| iii. Moniteurs multiples | Version actuelle moins 90 jours | 1912 CU6+ | 2106 (1) | 2106 | 2106 | Non |
| DTMF | Version actuelle moins 90 jours | S/O | 2102 | 2101 | 2101 | 2111.1 |
| Prise en charge de serveur proxy | Version actuelle moins 90 jours | S/O | 2012 (2) | 2104 (3) | 2101 (3) | 2305 |

| Fonctionnalité | Microsoft Teams (version minimale) | VDA (version minimale) | Application Citrix Workspace pour Windows CR (version minimale) | Application Citrix Workspace pour Mac (version minimale) | Application Citrix Workspace pour Linux (version minimale) | Application Citrix Workspace pour ChromeOS (version minimale) |
|---|---|---|---|---|---|---|
| Partage d'applications | Version actuelle moins 90 jours | 2109 | 2109.1 | 2203.1 | 2209 | Non |
| Sous-titres instantanés | Version actuelle moins 90 jours | S.O. (4) | 2109.1 | 2109 | 2109 | 2303 |
| Appels d'urgence dynamiques | Version actuelle moins 90 jours | S/O | 2112.1 | 2112 | 2112 | 2112 |
| Donner le contrôle | Version actuelle moins 90 jours | S/O | 2112.1 | 2203.1 | Non | Non |
| Demander le contrôle | Version actuelle moins 90 jours | S/O | 2112.1 | 2203.1 | 2203 | 2303 |
| Fenêtres multiples | 1.5.00.11865 | 2112, 1912 CU6 (5) | 2112.1 | 2203.1 | 2203 | 2303 |
| Transcriptions des réunions | Version actuelle moins 90 jours | 2112.1, 1912 CU6+ | 2112 | 2203.1 | 2203 | 2303 |
| Flou d'arrière-plan | Version actuelle moins 90 jours | 2112, 1912 CU6+ | 2207 | 2301 | 2212 | 2303 |

1. CD Viewer en mode plein écran uniquement. MAJ+F2 n'est pas pris en charge.
2. Négociation/Kerberos, NTLM, Basic et Digest. Les fichiers Pac sont également pris en charge.
3. Anonyme uniquement.
4. Si le VDA est de version 2112 ou supérieure, les sous-titres instantanés ne fonctionnent que si la version de l'application Citrix Workspace est 2203.1 pour Mac, 2203 pour Linux ou 2112 pour Windows. En effet, les sous-titres instantanés se comportent différemment si Microsoft Teams est en mode d'interface utilisateur à fenêtre unique ou en mode multi-fenêtres.
5. Le mode multi-fenêtres a été introduit dans le VDA 2112 mais a été rétroporté vers la version VDA 1912 LTSR CU6.

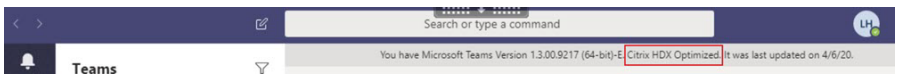
> **Remarque :**
>
> - Toutes les fonctionnalités répertoriées dans l'**application Citrix Workspace pour Windows 1912 CU6 (ou version ultérieure)** s'appliquent à l'application Citrix Workspace pour Windows 2203.1 LTSR CU1.
> - Microsoft a abandonné la prise en charge du mode fenêtre unique dans Microsoft Teams. Pour vous conformer, vous devez mettre à niveau votre VDA vers 1912 CU6+ LTSR et vers l'application Citrix Workspace 2203 CU2+ ou version ultérieure qui prennent en charge le mode multi-fenêtres.

### Activer l'optimisation pour Microsoft Teams

Pour activer l'optimisation pour Microsoft Teams, utilisez la stratégie de la console Gérer décrite dans Stratégie de redirection Microsoft Teams. Cette stratégie est **activée** par défaut. Outre l'activation de cette stratégie, HDX vérifie que la version de l'application Citrix Workspace est au moins à la version minimale requise. Si la stratégie est activée et que la version de l'application Citrix Workspace est prise en charge, la clé **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** est définie sur **1** de manière automatique sur le VDA. Microsoft Teams lit la clé à charger en mode VDI.

> **Remarque :**
>
> Si vous utilisez des VDA version 1906.2 ou ultérieure avec des versions de Controller plus anciennes (par exemple, la version 7.15), qui ne disposent pas de la stratégie disponible dans la console Gérer (Studio), vous pouvez toujours les optimiser. L'optimisation HDX pour Microsoft Teams est activée par défaut dans le VDA.

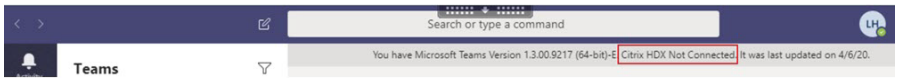
Si vous cliquez sur **About > Version**, la légende **Citrix HDX Optimized** affiche :



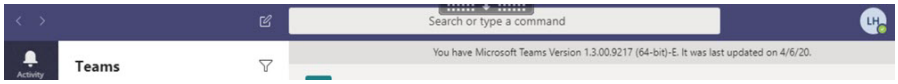

Si **Citrix HDX Not Connected** s'affiche, l'API Citrix est chargée dans Microsoft Teams. Le chargement

de l'API est la première étape de la redirection. Mais il y a une erreur dans les parties ultérieures de la pile. L'erreur se situe probablement dans les services VDA ou l'application Citrix Workspace.




Si aucune légende ne s'affiche, Microsoft Teams n'a pas pu charger l'API Citrix. Quittez Microsoft Teams en cliquant avec le bouton droit sur l'icône de la zone de notification et redémarrez. Assurez-vous que la stratégie de la console Gérer n'est pas définie sur **Interdit** et que la version de l'application Citrix Workspace est prise en charge.




> **Important : reconnexion de session**
>
> - Vous devrez peut-être relancer Microsoft Teams pour obtenir une session optimisée HDX lorsque votre connectivité change. Par exemple, si vous êtes en itinérance depuis un point de terminaison non pris en charge (application Workspace pour iOS, Android ou anciennes versions de Windows/Linux/Mac) vers un point de terminaison pris en charge (application Workspace pour Windows/Linux/Mac/ChromeOS/HTML5), ou vice versa.
> - Un redémarrage de Microsoft Teams est également nécessaire si vous avez installé l'application à l'aide du programme d'installation Microsoft Teams .exe dans le VDA. Le programme d'installation .exe est recommandé pour les déploiements VDI persistants. Dans de tels cas, Microsoft Teams peut se mettre à jour automatiquement lorsque la session HDX est déconnectée. Les utilisateurs qui se reconnectent à une session HDX remarquent alors que Microsoft Teams n'est pas optimisé.
> - Lorsque vous passez d'une session locale à une session HDX, vous devez relancer Microsoft Teams pour optimiser avec HDX. Cette action est requise dans un scénario Remote PC Access.

### Configuration réseau requise

Microsoft Teams s'appuie sur les serveurs Media Processor dans Microsoft 365 pour les réunions ou les appels à plusieurs. Microsoft Teams s'appuie aussi sur les relais de transport Microsoft 365 pour les scénarios suivants :

- Deux homologues dans un appel point à point n'ont pas de connectivité directe
- Un participant n'a pas de connectivité directe avec le processeur multimédia.

Par conséquent, l'intégrité du réseau entre l'homologue et le cloud Microsoft 365 détermine les performances de l'appel. Reportez-vous aux principes de connectivité réseau Microsoft 365 pour obtenir des instructions détaillées concernant la planification du réseau.

Nous vous recommandons d'évaluer votre environnement pour identifier les risques et les exigences qui peuvent influencer votre déploiement voix et vidéo global dans le cloud.
Utilisez l'outil d'évaluation du réseau Skype Entreprise pour tester si votre réseau est prêt pour Microsoft Teams. Pour obtenir des informations sur l'assistance, consultez la section Support.

**Résumé des principales recommandations réseau pour le trafic RTP (Real Time Protocol)**

- Connectez-vous au réseau Microsoft 365 aussi directement que possible à partir de la succursale.
- Planifiez et fournissez une bande passante suffisante à la succursale.
- Vérifiez la connectivité et la qualité du réseau de chaque succursale.
- Si vous devez utiliser l'un des éléments suivants dans la succursale, assurez-vous que le trafic RTP/UDP (géré par HdxRtcEngine.exe dans l'application Citrix Workspace) n'est pas entravé.
  - Contourner les serveurs proxy
  - Interception SSL réseau
  - Dispositifs d'inspection approfondie des paquets
  - Épingles à cheveux VPN (utiliser le split tunneling si possible)

> **Important : configuration du split tunneling de VPN**
>
> Le trafic HdxRtcEngine.exe doit être détourné du tunnel VPN et autorisé à utiliser la connexion Internet locale de l'utilisateur pour se connecter directement au service. La manière dont cela est accompli dépend du produit VPN et de la plate-forme machine utilisés, mais la plupart des solutions VPN permettent une configuration simple d'une stratégie pour appliquer cette logique. Pour plus d'informations sur les instructions de split tunneling spécifiques à la plate-forme VPN, consultez cet article Microsoft.

Le moteur multimédia WebRTC dans l'application Workspace (HdxRtcEngine.exe) utilise le protocole SRTP (Secure Real-Time Transport Protocol) pour les flux multimédia qui sont déchargés sur le client. Le protocole SRTP ajoute confidentialité et authentification à RTP. Pour cette fonctionnalité, des clés symétriques (négociées avec DTLS) sont utilisées pour chiffrer les médias et les messages de contrôle à l'aide du chiffrement AES.

Les mesures suivantes sont recommandées pour garantir une expérience utilisateur positive :

| Métrique | Point de terminaison à Microsoft 365 |
|---|---|
| Latence (sens unique) | < 50 msec |
| Latence (RTT) | < 100 msec |
| Perte de paquets | < 1 % au cours d'un intervalle de 15 s |

| Métrique | Point de terminaison à Microsoft 365 |
|---|---|
| Variation inter-arrivées des paquets | < 30 ms pendant un intervalle de 15 s |

Pour plus d'informations, consultez Préparer le réseau de votre organisation pour Microsoft Teams.

En termes de bande passante requise, l'optimisation pour Microsoft Teams peut utiliser une grande variété de codecs pour l'audio (OPUS/G.722/PCM G711) et la vidéo (H264).

Les homologues négocient ces codecs pendant le processus d'établissement de l'appel à l'aide de l'offre/réponse du protocole SDP.
Les recommandations minimales Citrix par utilisateur sont les suivantes :

| Type | Bande passante | Codec |
|---|---|---|
| Audio (dans chaque sens) | ~ 90 kbps | G.722 |
| Audio (dans chaque sens) | ~ 60 Kbits/s | Opus* |
| Vidéo (dans chaque sens) | ~ 700 kbps | H264 360p @ 30 ips 16:9 |
| Partage d'écran | ~ 300 kbps | H264 1080p @ 15 ips |

* Opus prend en charge l'encodage à débit variable et constant de 6 Kbits/s à 510 Kbits/s.

Opus et H264 sont les codecs préférés pour les appels poste à poste et les conférences téléphoniques.

> **Important :**
>
> En ce qui concerne les performances, l'encodage est plus coûteux que le décodage pour l'utilisation du processeur sur la machine cliente. Vous pouvez coder en dur la résolution d'encodage maximale dans l'application Citrix Workspace pour Linux et Windows. Voir Estimation des performances au niveau du codage et Optimisation pour Microsoft Teams.

### Serveurs proxy

En fonction de l'emplacement du proxy, tenez compte de ce qui suit :

- Configuration du proxy sur le VDA :

  Si vous configurez un serveur proxy explicite dans le VDA et que vous acheminez les connexions vers localhost via un proxy, la redirection échoue. Pour configurer correctement le proxy,

vous devez sélectionner le paramètre **Ne pas utiliser de serveur proxy pour les adresses locales** dans **Options Internet > Connexions > Paramètres LAN > Serveurs proxy** et contourner `127.0.0.1:9002`.

Si vous utilisez un fichier PAC, le script de configuration du proxy VDA du fichier PAC doit renvoyer **DIRECT** pour `wss://127.0.0.1:9002`. Sinon, l'optimisation échoue. Pour vous assurer que le script renvoie **DIRECT**, utilisez `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configuration du proxy sur l'application Citrix Workspace :

  Si la succursale est configurée pour accéder à Internet via un proxy, ces versions prennent en charge les serveurs proxy :

  - Application Citrix Workspace pour Windows version 2012 (Negotiate/Kerberos, NTLM, Basic et Digest. Les fichiers `Pac` sont aussi pris en charge)
  - Application Citrix Workspace pour Windows version 1912 CU5 (Negotiate/Kerberos, NTLM, Basic et Digest. Les fichiers `Pac` sont aussi pris en charge)
  - Application Citrix Workspace pour Linux version 2101 (authentification anonyme)
  - Application Citrix Workspace pour Mac version 2104 (authentification anonyme)

Les périphériques clients dotés de versions antérieures de l'application Citrix Workspace ne peuvent pas lire les configurations de proxy. Ces périphériques envoient le trafic directement aux serveurs Microsoft 365 TURN.

> **Important :**
>
> - Vérifiez que le périphérique client peut se connecter au serveur DNS pour effectuer des résolutions DNS. Un périphérique client doit pouvoir résoudre les noms de domaine complet du serveur relais Microsoft Teams suivants :
>
>   ```
>   - worldaz.relay.teams.microsoft.com
>   - inaz.relay.teams.microsoft.com
>   - uaeaz.relay.teams.microsoft.com
>   - euaz.relay.teams.microsoft.com
>   - usaz.relay.teams.microsoft.com
>   - turn.dod.teams.microsoft.us
>   - turn.gov.teams.microsoft.us
>   ```
>
> Si les requêtes DNS échouent, les appels P2P avec des utilisateurs extérieurs et les conférences téléphoniques avec établissement de médias échouent.
>
> - L'emplacement du serveur de conférence est sélectionné en fonction de l'emplacement du bureau virtuel du premier participant (et non du client).

### Établissement des appels et chemins de circulation des médias

Autant que possible, le moteur multimédia HDX WebRTC de l'application Citrix Workspace (HdxRtcEngine.exe) tente d'établir une connexion SRTP réseau directe via UDP dans un appel de poste à poste. Si les ports à priorité élevée UDP sont bloqués, Media Engine revient à TCP/TLS 443.

HDX Media Engine prend en charge ICE, Session Traversal Utilities for NAT (STUN) et Traversal Using Relays around NAT (TURN) pour découvrir les candidats et établir les connexions. Cette prise en charge signifie que le point de terminaison doit être capable d'effectuer des résolutions DNS.

Imaginons un scénario dans lequel il n'y a pas de chemin direct entre les deux homologues ou entre un homologue et un serveur de conférence et où vous participez à un appel ou à une réunion impliquant plusieurs parties. HdxRtcEngine.exe utilise un serveur de relais de transport Microsoft Teams dans Microsoft 365 pour atteindre l'autre homologue ou le processeur multimédia, où les réunions sont hébergées. Votre machine cliente doit avoir accès à trois plages d'adresses IP de sous-réseau Microsoft 365 et à quatre ports UDP (ou TCP/TLS 443 comme solution de secours si UDP est bloqué). Pour plus d'informations, consultez le diagramme d'architecture dans Configuration d'appel et les URL et les plages d'adresses IP Office 365 pour l'ID 11.

| ID | Catégorie | Adresses | Ports de destination |
|---|---|---|---|
| 11 | Optimisation requise | 13.107.64.0/18, 52.112.0.0/14, 52.122.0.0/15 | **UDP :** 3478, 3479, 3480, 3481, **TCP :** 443 (repli) |

Ces plages incluent à la fois des relais de transport et des processeurs multimédias, avec un Azure Load Balancer en frontal.
Les relais de transport Microsoft Teams offrent des fonctionnalités STUN et TURN, mais ce ne sont pas des points de terminaison ICE. De plus, les relais de transport Microsoft Teams ne terminent pas les médias, TLS, et n'effectuent pas non plus de transcodage. Ils peuvent relier TCP (si HdxRtcEngine.exe utilise TCP) à UDP lorsqu'ils transmettent le trafic à d'autres homologues ou processeurs multimédias.

Le moteur multimédia WebRTC de l'application Workspace contacte le relais de transport Microsoft Teams le plus proche dans le cloud Microsoft 365. Le moteur multimédia utilise une adresse IP anycast et le port 3478—3481 UDP (différents ports UDP par charge de travail, bien qu'un multiplexage soit possible) ou 443 TCP/TLS pour les replis. La qualité des appels dépend du protocole réseau sous-jacent. Étant donné que UDP est toujours préférable à TCP, nous vous conseillons de concevoir vos réseaux pour prendre en charge le trafic UDP au niveau de la succursale.

Si Microsoft Teams est chargé en mode optimisé et que HdxRtcEngine.exe est en cours d'exécution sur le point de terminaison, des échecs ICE peuvent provoquer un échec de la configuration d'appel

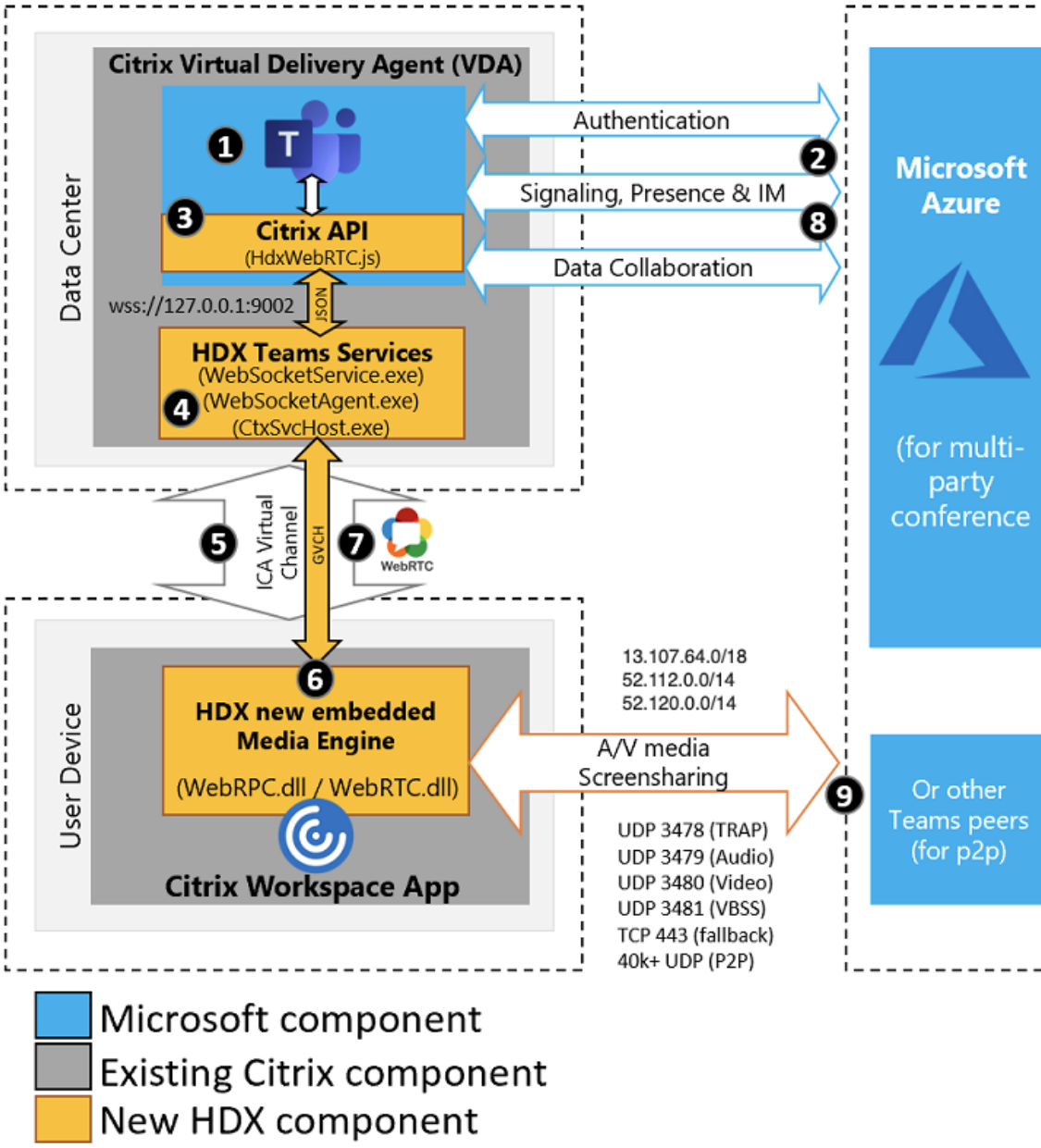
ou une lecture audio/vidéo à sens unique. Lorsqu'un appel ne peut pas être établi ou que les flux de médias ne sont pas en duplex intégral, vérifiez d'abord la **trace Wireshark** sur le point de terminaison. Pour plus d'informations sur le processus de collecte des candidats ICE, voir « Collecte des journaux » dans la section Support.

> **Remarque :**
>
> Si les points de terminaison n'ont pas accès à Internet, il peut encore être possible pour les utilisateurs d'effectuer un appel poste à poste si les participants se trouvent sur le même réseau LAN. Les réunions échouent. Dans ce cas, il y a un délai de 30 secondes avant le début de l'établissement de l'appel.

### Configuration d'appel

Utilisez ce diagramme d'architecture comme référence visuelle pour la procédure d'appel. Les étapes correspondantes sont indiquées dans le diagramme.




**Architecture**

1. Démarrez Microsoft Teams.
2. Microsoft Teams authentifie auprès d'O365. Les stratégies de locataire sont envoyées au client Microsoft Teams, et les informations TURN et de canal de signalisation pertinentes sont relayées à l'application.
3. Microsoft Teams détecte qu'il s'exécute dans un VDA et envoie des appels d'API vers l'API JavaScript Citrix.
4. Citrix JavaScript dans Microsoft Teams ouvre une connexion WebSocket sécurisée à WebSocketService.exe s'exécutant sur le VDA, ce qui génère WebSocketAgent.exe dans la session utilisateur.

5. WebSocketAgent.exe instancie un canal virtuel générique en appelant le service de redirection Microsoft Teams Citrix HDX (CtxSvcHost.exe).
6. Le wfica32.exe (moteur HDX) de l'application Citrix Workspace génère un nouveau processus appelé HdxRtcEngine.exe, qui est le nouveau moteur WebRTC utilisé pour l'optimisation pour Microsoft Teams.
7. Le moteur multimédia Citrix et Teams.exe ont un chemin de canal virtuel bidirectionnel et peuvent commencer à traiter les demandes multimédia.

   —Appels utilisateur—

8. L'**homologue A** clique sur le bouton **Appeler**. Teams.exe communique avec les services Microsoft Teams dans Microsoft 365 en établissant un chemin de signalisation de bout en bout avec l'**homologue B**. Microsoft Teams demande à HdxRtcEngine une série de paramètres d'appel pris en charge (codecs, résolutions, etc., connus sous le nom d'offre SDP (Session Description Protocol)). Ces paramètres d'appel sont ensuite relayés à l'aide du chemin de signalisation vers les services Microsoft Teams dans Microsoft 365 et à partir de là vers l'autre homologue.
9. L'offre/réponse SDP (négociation à une seule passe) est réalisée via le canal de signalisation, et les vérifications de connectivité ICE (traversée NAT et pare-feu à l'aide des requêtes de liaison STUN) sont effectuées. Ensuite, le contenu multimédia SRTP (Secure Real-Time Transport Protocol) circule directement entre HdxRtcEngine.exe et l'autre homologue (ou les serveurs de conférence Microsoft 365 s'il s'agit d'une réunion).

### Système téléphonique Microsoft

Le système téléphonique est la technologie de Microsoft qui permet le contrôle des appels et l'utilisation d'un PBX dans le cloud Microsoft 365 avec Microsoft Teams. Optimisation pour Microsoft Teams prend en charge le système téléphonique, à l'aide des forfaits d'appel ou du routage direct de Microsoft 365. Avec le routage direct, vous pouvez connecter directement votre propre contrôleur SBC (contrôleur de frontière de session) pris en charge au système téléphonique Microsoft sans logiciel local supplémentaire.
Les files d'attente d'appels, le transfert, la mise en attente, la désactivation du son et la reprise d'un appel sont pris en charge.

#### DTMF

Le code DTMF (Dual Tone Multi Frequency) est pris en charge avec les versions suivantes de l'application Citrix Workspace (et ultérieures) :

- Application Citrix Workspace pour Windows version 2102

- Application Citrix Workspace pour Windows LTSR 1912 CU5 (système d'exploitation Windows 10 uniquement)
- Application Citrix Workspace pour Linux version 2101
- Application Citrix Workspace pour Mac version 2101
- Application Citrix Workspace pour ChromeOS version 2111.1

#### Prise en charge des appels d'urgence dynamiques

À partir de la version 2112, l'application Citrix Workspace prend en charge les appels d'urgence dynamiques. Lorsque cette fonction est utilisée avec les forfaits d'appel Microsoft, Operator Connect et Direct Routing, elle vous permet d'effectuer les opérations suivantes :

- Configurer et acheminer les appels d'urgence
- Informer le personnel de sécurité.

La notification est fournie en fonction de l'emplacement actuel de l'application Citrix Workspace exécutée sur le point de terminaison, au lieu du client Microsoft Teams sur le VDA.

La loi Ray Baum exige que l'emplacement de la personne effectuant l'appel d'urgence soit transmis au centre de réception des appels d'urgence approprié. L'optimisation Microsoft Teams avec HDX est conforme à la loi Ray Baum lorsqu'elle est utilisée avec les versions suivantes de l'application Citrix Workspace :

- Application Citrix Workspace pour Windows version 2112.1 ou ultérieure
- Application Citrix Workspace pour Linux version 2112 ou ultérieure
- Application Citrix Workspace pour Mac version 2112 ou ultérieure
- Application Citrix Workspace pour ChromeOS version 2112 ou ultérieure

Pour activer les appels d'urgence dynamiques, l'administrateur doit utiliser le centre d'administration Microsoft Teams et configurer les éléments suivants pour créer un réseau ou une carte de localisation d'urgence :

- Paramètres réseau
- Service d'information d'emplacement

Pour plus d'informations sur les appels d'urgence dynamiques, consultez la documentation Microsoft.

Les informations d'emplacement que l'application Citrix Workspace transmet à Microsoft Teams sont les suivantes :

- ID de châssis/ID de port utilisant le protocole LLDP (Link Layer Discovery Protocol) pour les connexions Ethernet/Switch. Ethernet/Switch (LLDP) est pris en charge sur :
  - Versions Windows 8.1 et 10

  - macOS (exige un logiciel d'activation LLDP) Pour télécharger le logiciel d'activation LLDP, accédez à `www.microsoft.com` et recherchez le logiciel d'activation LLDP.
  - Linux (exige que la bibliothèque LLDP soit incluse dans la distribution du système d'exploitation (OS) du client léger)

- WLAN BBSID et {IPv4-IPv6; sous-réseau ; adresse MAC} du point de terminaison sur lequel l'application Citrix Workspace est installée.

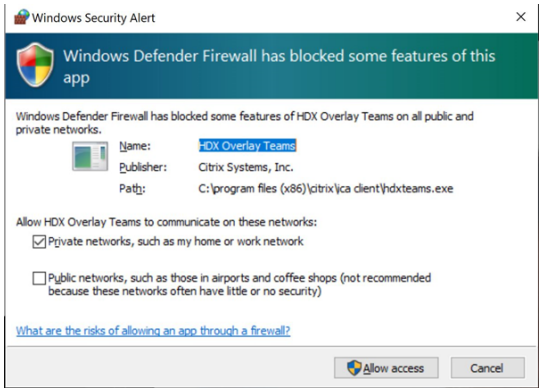
  - Les emplacements de sous-réseau et Wi-Fi sont pris en charge dans l'application Workspace pour Windows, Linux et Mac.

- Latitude et Longitude, si l'autorisation utilisateur est accordée au niveau du système d'exploitation où l'application Citrix Workspace est installée (l'autorisation est définie sur HDX RTC Engine)

  - Pris en charge sur toutes les plates-formes de l'application Toutefois, pour Citrix Workspace pour Linux, vous devez inclure la bibliothèque `libgps` dans la distribution du système d'exploitation du client léger (>sudo apt-get install libgps23 gpsd lldpd).

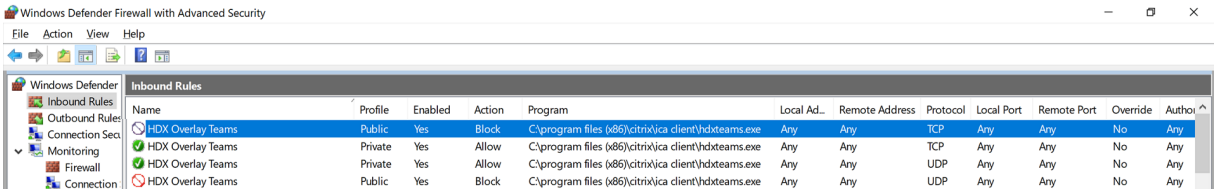
### Considérations sur les pare-feu

Lorsque les utilisateurs démarrent un appel optimisé à l'aide du client Microsoft Teams pour la première fois, ils peuvent voir un avertissement concernant les paramètres du **pare-feu Windows**. L'avertissement demande aux utilisateurs d'autoriser la communication pour HdxTeams.exe ou HdxRtcEngine.exe (HDX Overlay Microsoft Teams).




Les quatre entrées suivantes sont ajoutées sous **Règles de trafic entrant** dans la console **Pare-feu Windows Defender > Sécurité avancée**. Vous pouvez appliquer des règles plus restrictives si vous le souhaitez.

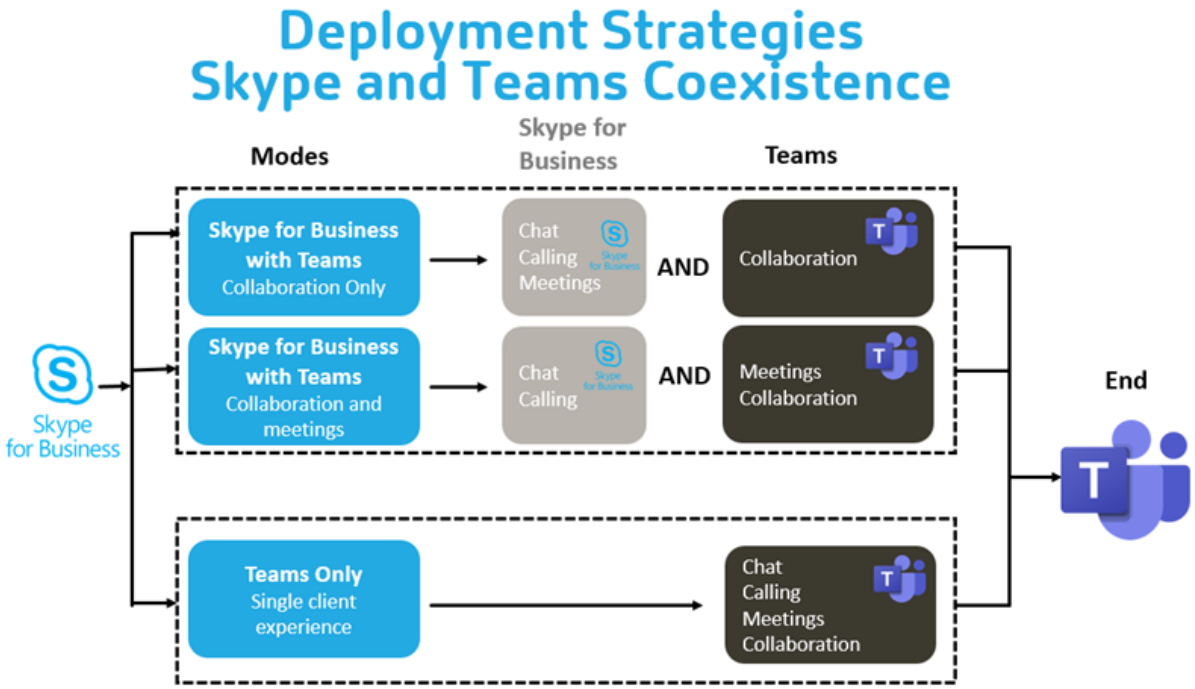



## Coexistence Microsoft Teams/Skype Entreprise

Vous pouvez déployer Microsoft Teams et Skype Entreprise côte à côte, comme deux solutions distinctes avec des fonctionnalités qui se chevauchent.
Pour plus d'informations, consultez Comprendre la coexistence et l'interopérabilité de Microsoft Teams et Skype Entreprise.

Les moteurs multimédia Pack d'optimisation Citrix HDX RealTime et Optimisation HDX pour Microsoft Teams utilisent ensuite la configuration définie dans votre environnement. Les exemples incluent les modes Îles et Skype Entreprise avec collaboration Microsoft Teams. Et aussi, Skype Entreprise avec collaboration et réunions Microsoft Teams.

L'accès aux périphériques ne peut être accordé qu'à une seule application à la fois. Par exemple, l'accès à la webcam par RealTime Media Engine pendant un appel verrouille le périphérique d'acquisition d'images pendant un appel. Lorsque le périphérique est libéré, il devient disponible pour Microsoft Teams.



### Citrix SD-WAN : connectivité réseau optimisée pour Microsoft Teams

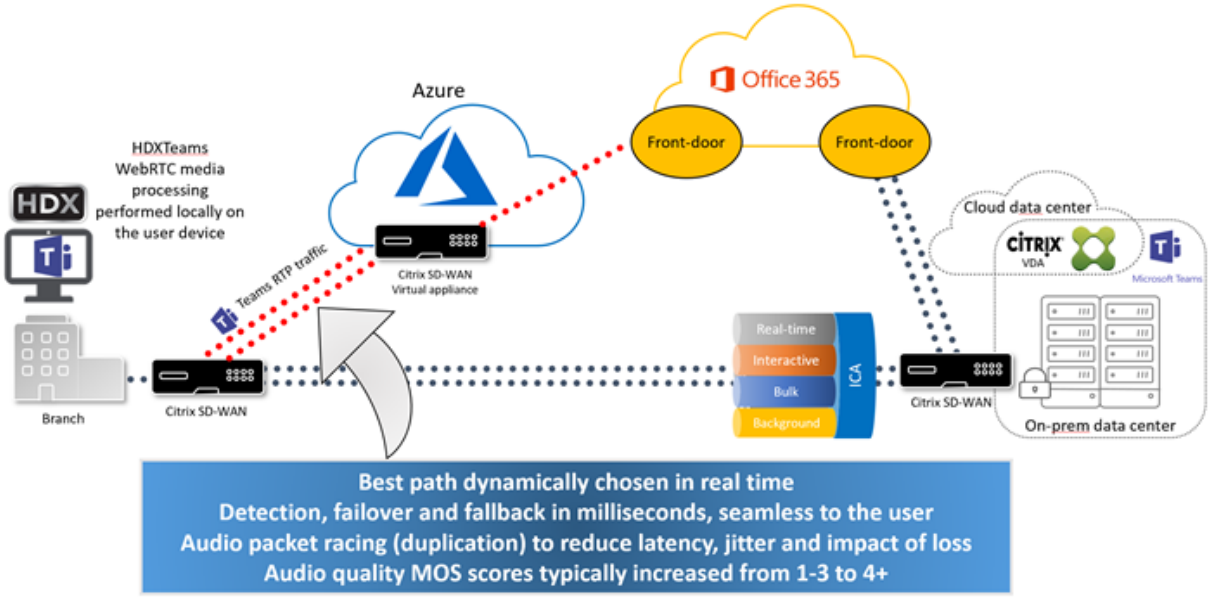
Une qualité audio et vidéo optimale nécessite une connexion réseau au cloud Microsoft 365 avec une faible latence, une faible gigue et une faible perte de paquets. Le rétroacheminement du trafic RTP audio-vidéo Microsoft Teams à partir des utilisateurs de l'application Citrix Workspace situés dans des succursales vers un centre de données avant d'accéder à Internet peut ajouter une latence excessive. Cela peut également entraîner une congestion sur les liaisons WAN. Citrix SD-WAN optimise la connectivité pour Microsoft Teams conformément aux principes de connectivité réseau Microsoft 365. Citrix SD-WAN utilise l'adresse IP et le service Web Microsoft REST Microsoft 365 et le DNS approximatif. Cette utilisation permet d'identifier, de catégoriser et de diriger le trafic Microsoft Teams.

Dans de nombreuses régions, les connexions Internet haut débit professionnelles souffrent de pertes intermittentes de paquets, de périodes de gigue excessive et de pannes.

Citrix SD-WAN propose deux solutions pour préserver la qualité audio-vidéo de Microsoft Teams lorsque l'intégrité du réseau est variable ou dégradée.

- Si vous utilisez Microsoft Azure, une appliance virtuelle Citrix SD-WAN (VPX) déployé dans le VNET Azure fournit des optimisations de connectivité avancées. Ces optimisations incluent le basculement transparent de liaison et le traçage des paquets audio.
- Les clients Citrix SD-WAN peuvent se connecter à Microsoft 365 via le service Citrix Cloud Direct. Ce service fournit une livraison fiable et sécurisée pour tout le trafic lié à Internet.

Si la qualité de la connexion Internet de la succursale n'est pas un problème, cela peut suffire à réduire la latence. Dirigez le trafic Microsoft Teams directement de l'appliance de succursale Citrix SD-WAN vers la porte d'entrée Microsoft 365 la plus proche pour réduire la latence. Pour plus d'informations, consultez Optimisation de Citrix SD-WAN Office 365.



### Réunions et chat en mode multi-fenêtres

Vous pouvez utiliser plusieurs fenêtres de réunion et de chat pour Microsoft Teams dans Windows. Pour plus d'informations sur la fonctionnalité pop-out ou multi-fenêtres, consultez Microsoft Teams Pop-Out Windows for Chats and Meetings sur le site Microsoft 365.

> **Remarque :**
>
> Cette fonctionnalité est prise en charge par l'application Citrix Workspace pour Windows 2112.1, Mac 2203, Linux 2203, ChromeOS 2303. Elle nécessite VDA 2112 ou supérieur et a été rétroportée vers 1912 CU6+ LTSR.

### Flou et effets d'arrière-plan

L'application Citrix Workspace pour Windows, Mac, Linux et ChromeOS/HTML5 prend en charge le flou et les effets d'arrière-plan dans l'optimisation Microsoft Teams avec HDX.

Vous pouvez flouter ou remplacer l'arrière-plan par une image par défaut et éviter les distractions inattendues en aidant la conversation à rester centrée sur la silhouette (corps et visage). Vous pouvez utiliser cette fonctionnalité avec des appels P2P ou des conférences téléphoniques.

> **Remarque :**
>
> Cette fonctionnalité est intégrée à l'interface utilisateur/aux boutons de Microsoft Teams. La prise en charge de fenêtres multiples est une condition préalable qui nécessite une mise à jour du VDA vers 2112 ou une version ultérieure. Pour plus d'informations, consultez Réunions et chat en mode multi-fenêtres.

Les commandes de l'interface utilisateur Microsoft Teams relatives au flou et aux effets d'arrière-plan nécessitent les versions minimales suivantes :

- Application Citrix Workspace pour Windows 2207
- Application Citrix Workspace pour Mac 2301
- Application Citrix Workspace pour Linux 2307
- Application Citrix Workspace pour ChromeOS 2303

**Limitations :**

- Le client doit être connecté à Internet lors du remplacement de l'image d'arrière-plan par une image par défaut de Microsoft Teams.
- Le remplacement des images d'arrière-plan définies par l'administrateur et l'utilisateur n'est pas pris en charge dans l'interface utilisateur de Microsoft Teams. Des images d'arrière-plan personnalisées peuvent être configurées à l'aide des paramètres de configuration du client, si l'image est également stockée sur le client.

### Configuration d'une image d'arrière-plan personnalisée

Les clés de registre suivantes ne sont requises que si vous ne prévoyez pas d'utiliser l'interface utilisateur de Microsoft Teams pour contrôler la fonctionnalité, ou si un administrateur souhaite remplacer les comportements par défaut. Par exemple, désactivez le flou d'arrière-plan car le point de terminaison n'est pas assez puissant.

**Sous Windows** Pour définir une image d'arrière-plan personnalisée, les administrateurs ou les utilisateurs finaux doivent configurer la clé de registre suivante sur le client ou point de terminaison :

Emplacement : `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nom : VideoBackgroundEffect
- Type : DWORD
- Valeur : 0 (désactivé), 1 (activé), 2 (remplacement de l'image d'arrière-plan)

La valeur 1 rend l'arrière-plan flou. L'utilisateur final ou l'administrateur peut définir cette valeur.

La valeur définie sur 2 nécessite également la présence de la clé **VideoBackgroundImage**. Seul l'administrateur peut définir cette valeur. La clé suivante n'est requise que si vous souhaitez remplacer l'image d'arrière-plan et non pour la rendre floue :

- Nom : VideoBackgroundImage
- Type : REG_SZ
- Valeur : my_image_name.jpg

L'image d'arrière-plan de la vidéo doit être présente dans le répertoire `C:\Program Files (x86)\Citrix\ICA Client`.

Cette configuration de registre peut également être utilisée pour activer le flou en arrière-plan ou le remplacement d'image dans l'application Citrix Workspace 2206 sans le sélecteur d'interface utilisateur de Microsoft Teams. En d'autres termes, si votre environnement ou VDA ne prend pas en charge le mode multi-fenêtres, vous pouvez toujours appliquer la solution du registre HKCU avec l'application Citrix Workspace 2206 ou une version ultérieure pour obtenir un résultat similaire, bien que l'utilisateur ne puisse pas contrôler la fonctionnalité au milieu de la session HDX ou de l'appel Microsoft Teams.

Les modifications apportées à la clé de registre ne prennent effet que lorsque la session HDX se connecte.

**Sous Mac** Emplacement de la photo téléchargée par l'utilisateur : */Users/username/Downloads/any_image.png*

Exécutez les commandes suivantes pour définir l'image personnalisée comme image par défaut :

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2

defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

**Sous Linux** Emplacement de la photo téléchargée par l'utilisateur : */home/username/Downloads/any_image.jpg*

Créez le fichier */var/.config/citrix/hdx_rtc_engine/config.json* et ajoutez les clés de configuration suivantes au format JSON. Par exemple,

```
{


"VideoBackgroundEffect":2,

"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"

 }
```

**Sur HTML5**

1. Accédez au fichier **configuration.js** dans le dossier **HTML5Client**.
2. Ajoutez l'attribut **backgroundEffects** et définissez-le sur **true**. Par exemple,

```
'features' : {

    'msTeamsOptimization' :
    {

        'backgroundEffects' : true
     }

 }

<!--NeedCopy-->
```

3. Enregistrez les modifications.

**Considérations relatives à la consommation du processeur**

Bien que la consommation du processeur de la fonctionnalité de floutage soit limitée, vous pouvez vous attendre à une augmentation de la consommation. Par exemple, sur un client léger doté d'une puce Intel® Pentium® Silver 4 cœurs 1,5 GHz avec TurboBoost jusqu'à 2,8 GHz, le flou d'arrière-plan augmente d'environ 2% l'utilisation du processeur. L'utilisation moyenne du processeur est inférieure à 20%.

### Vue Galerie et haut-parleurs actifs dans Microsoft Teams

Microsoft Teams prend en charge les dispositions **Galerie**, **Grande galerie** et **Mode Ensemble**.

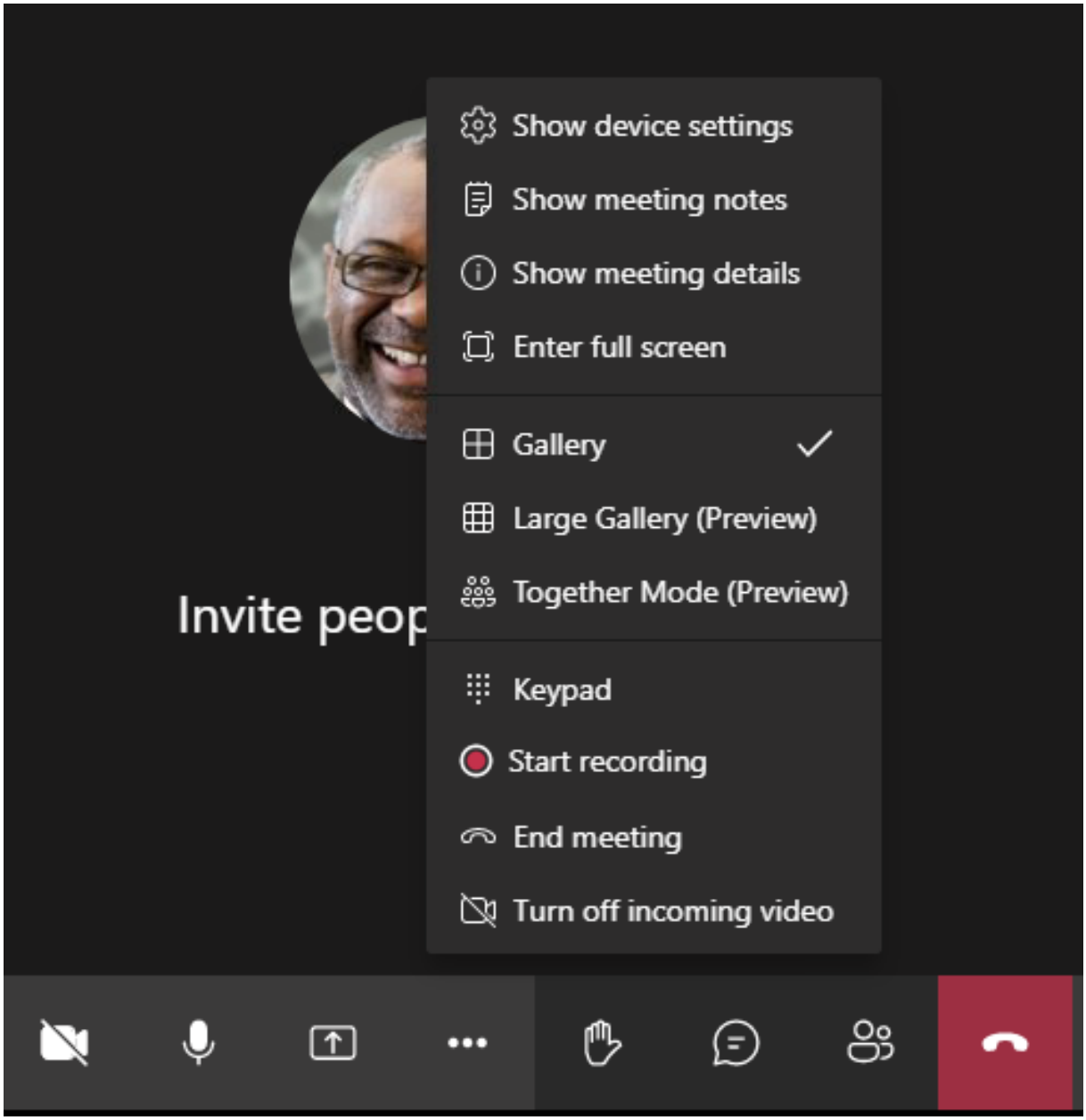
Microsoft Teams affiche une grille 2x2 avec les flux vidéo de quatre participants (aussi appelés **Galerie**). Dans ce cas, Microsoft Teams envoie 4 flux vidéo à la machine cliente pour décodage. Lorsque plus de quatre participants partagent une vidéo, seuls les quatre derniers interlocuteurs les plus actifs apparaissent à l'écran.

Microsoft Teams offre également la vue Grande galerie avec une grille pouvant aller jusqu'à 7x7. Par conséquent, le serveur de conférence Microsoft Teams compose un flux vidéo unique et l'envoie à la machine cliente pour décodage, ce qui réduit la consommation de CPU. Ce flux unique de type matriciel peut également inclure les vidéos d'auto-prévisualisation des utilisateurs.

Enfin, Microsoft Teams prend en charge le **mode Ensemble**, qui fait partie de la nouvelle expérience de réunion. Utilisant la technologie de segmentation de l'IA pour placer les participants devant un arrière-plan partagé, Microsoft Teams met tous les participants dans le même auditorium.

L'utilisateur peut contrôler ces modes lors d'une conférence téléphonique en sélectionnant **Galerie**, **Grande galerie** ou **Mode Ensemble** dans le menu des points de suspension.




Prise en charge des contraintes de rapport d'aspect vidéo (application Citrix Workspace pour Windows 2102, application Citrix Workspace pour Linux 2106, application Citrix Workspace pour MAC 2106 et versions ultérieures) :

- L'option **Remplir le cadre** est disponible en mode Galerie/Grande galerie. Cette option permet de redimensionner la taille de la vidéo pour l'ajuster à la sous-fenêtre. L'option **Ajuster à l'image** affiche quant à elle des barres noires (boîte aux lettres) sur les côtés de la vidéo afin qu'il n'y ait pas de recadrage.

Le tableau suivant présente une comparaison des dispositions Galerie et Grande galerie :

| | Vue Galerie 2x2 (par défaut) | Vue Grande galerie |
|---|---|---|
| Disposition/Grille | Affiche une grille 2x2 avec les flux vidéo de quatre participants. Seules les quatre dernières personnes les plus actives apparaissent à l'écran et les autres participants n' apparaissent pas sur la grille. | Affiche une grille 7x7 avec les flux vidéo de 49 participants. |
| Technique de mixage | Un routeur multimédia transfère les flux individuels de chaque participant vers chaque utilisateur. | Un serveur de conférence central mixe et transcode tout le contenu audio ou vidéo afin de créer une disposition composite sur mesure pour chaque participant, ce qui entraîne une latence supplémentaire. |
| Participant actif | Le nouveau participant actif remplace le participant le moins actif de la grille. | Affiche tous les participants, qu'ils soient actifs ou inactifs. |
| Codage au niveau du point de terminaison | Un ou plusieurs flux vidéo peuvent être codés au point de terminaison si la diffusion simultanée est activée. Pour plus d'informations sur la prise en charge de la diffusion simultanée, consultez Diffusion simultanée. | Un ou plusieurs flux vidéo peuvent être codés au point de terminaison si la diffusion simultanée est activée. Pour plus d'informations sur la prise en charge de la diffusion simultanée, consultez Diffusion simultanée. |
| Décodage au niveau du point de terminaison | Chaque participant reçoit jusqu'à quatre flux multimédias individuels. Par conséquent, HdxRtcEngine.exe consomme plus de processeur au niveau du point de terminaison (pour le décodage/rendu). | Chaque participant ne reçoit qu'un seul flux audio et vidéo. Cela réduit la consommation du processeur au niveau du point de terminaison. |

| | Vue Galerie 2x2 (par défaut) | Vue Grande galerie |
|---|---|---|
| Résolution maximale | 720p. Lorsque quatre participants partagent la vidéo, la résolution maximale est de 360p par flux vidéo. Si moins de quatre participants partagent la vidéo, la résolution par flux vidéo peut être supérieure. | 720p pour le mixage ou la disposition composite. Il n'est pas nécessaire de disposer d'un flux vidéo de haute qualité par participant dans une disposition composite. En raison de cette condition, chaque expéditeur réduit la résolution ou le débit binaire de téléchargement. |
| Utilisateur à réseau lent | L'expéditeur modifie la qualité de chaque modalité (audio/vidéo/partage d'écran) pour obtenir la qualité réseau commune la plus faible parmi les participants. Ce flux multimédia est ensuite transmis à tous les autres participants. Par conséquent, un participant dont le réseau n'est pas performant a un impact sur la qualité de la vidéo pour tous les autres participants à l'appel. | Moins sensible au scénario de qualité réseau commune la plus faible. Le serveur de conférence offre différentes qualités en fonction des conditions de réseau des participants individuels. |
| Auto-aperçu | Affiche votre aperçu sous forme de petite vignette en temps réel. | Affiche votre aperçu sous forme de vignette, mixé avec le reste des flux vidéo. Vous pourriez donc vous voir inclus dans la disposition vidéo principale avec un délai supplémentaire. |

### Partage d'écran dans Microsoft Teams

Microsoft Teams s'appuie sur le partage d'écran basé sur la vidéo (VBSS), codant le bureau partagé avec des codecs vidéo comme H264 et créant un flux haute définition. Avec l'optimisation HDX, le partage d'écran entrant est traité comme un flux vidéo.

À partir de l'application Citrix Workspace 2109 ou version ultérieure pour Windows, Linux, Mac et l'application Citrix Workspace 2303 pour ChromeOS, les utilisateurs peuvent partager leurs écrans et leur caméra vidéo simultanément.

Avec les versions antérieures, si vous êtes au milieu d'un appel vidéo et que l'autre participant commence à partager le bureau, le flux vidéo de la caméra d'origine est mis en pause. À la place, le flux vidéo de partage d'écran s'affiche. L'homologue doit ensuite reprendre manuellement le partage de la caméra.

> **Remarque concernant PowerPoint Live**
>
> Cette limitation ne s'applique pas si vous partagez du contenu à partir de PowerPoint Live. Dans ce cas, les autres homologues peuvent toujours voir votre webcam et votre contenu et revenir en arrière pour consulter d'autres diapositives. Dans ce scénario, les diapositives sont rendues sur le VDA. Pour accéder à une série de diapositives PowerPoint Live, cliquez sur le bouton « Bac de partage » et sélectionnez l'une des diapositives PowerPoint suggérées, ou cliquez sur « Parcourir » et recherchez un fichier PowerPoint sur votre ordinateur ou dans OneDrive.

Le partage d'écran sortant est également optimisé et déchargé vers l'application Citrix Workspace. Dans ce cas, le moteur multimédia capture et transmet uniquement la fenêtre Citrix Desktop Viewer (CDViewer.exe), entourée d'une bordure rouge. Les applications locales qui se chevauchent avec Desktop Viewer ne sont pas capturées.

> **Remarque**
>
> Définissez une autorisation spécifique dans l'application Citrix Workspace pour Mac pour activer le partage d'écran. Pour plus d'informations, veuillez consulter la section Configuration système requise.

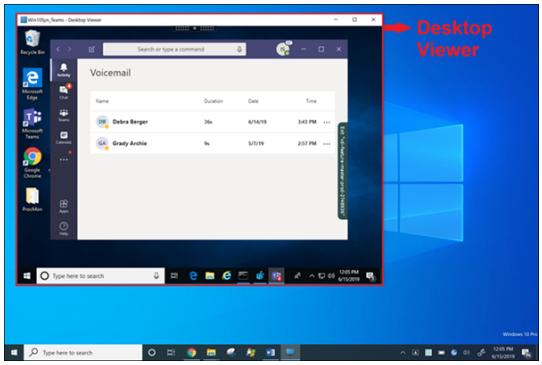
**Limitation connue :**

- Si Desktop Viewer est désactivé ou si Desktop Lock est utilisé, la sélection multi-moniteurs n'est pas disponible dans le sélecteur d'écran Microsoft Teams. Desktop Viewer peut être désactivé en modifiant le modèle de fichier `.ICA` ou `StoreFront web.config`. Le raccourci clavier MAJ+F2 n'est pas compatible avec le partage d'écran multi-moniteurs.
- Dans les versions de l'application Workspace antérieures à 2106, seul le moniteur principal est partagé. Faites glisser l'application dans le bureau virtuel vers le moniteur principal pour que les autres participants à l'appel puisse la voir.
- Le partage d'écran multi-moniteurs peut ne pas fonctionner si vous configurez l'application Citrix Workspace avec la fonctionnalité de disposition en moniteurs virtuels (partition logique d'un seul moniteur physique). Dans ce cas, tous les moniteurs virtuels sont partagés en tant qu'image composite.
- Les anciennes versions de l'application Citrix Workspace pour Windows (1907 à 2008) partagent également une application locale exécutée sur la machine cliente. Ce partage n'est possible que

si l'application locale a été superposée sur Desktop Viewer. Ce comportement a été supprimé dans 2009.6 ou supérieur, et dans 1912 CU5 ou supérieur.

- Pendant le partage d'écran, si vous passez du mode fenêtré au mode plein écran, le partage d'écran s'arrête. Vous devez arrêter et partager à nouveau pour que le partage d'écran fonctionne.
- Il n'est pas possible d'épingler les commandes de partage sur un emplacement spécifique dans Microsoft Teams optimisé.
- Lors du partage d'une application réduite, la barre de titre de l'application peut également être partagée.




**Partage d'écran à partir d'une application transparente :**

Si vous publiez Microsoft Teams en tant qu'application transparente autonome, le partage d'écran capture le bureau local de votre point de terminaison physique. L'application Citrix Workspace version minimale 1909 est requise.

### Partage d'applications

À partir de l'application Citrix Workspace pour Windows 2112.1 et VDA 2112, Microsoft Teams prend en charge le partage d'applications.

À partir de l'application Citrix Workspace pour Windows 2109, Mac 2203, Linux 2209 et VDA 2109, Microsoft Teams prend en charge le partage d'écran d'applications spécifiques exécutées dans la session virtuelle. Vous pouvez également partager des applications internes personnalisées, telles que Java, à l'aide de Microsoft Teams optimisé. Pour partager une application spécifique, procédez comme suit :

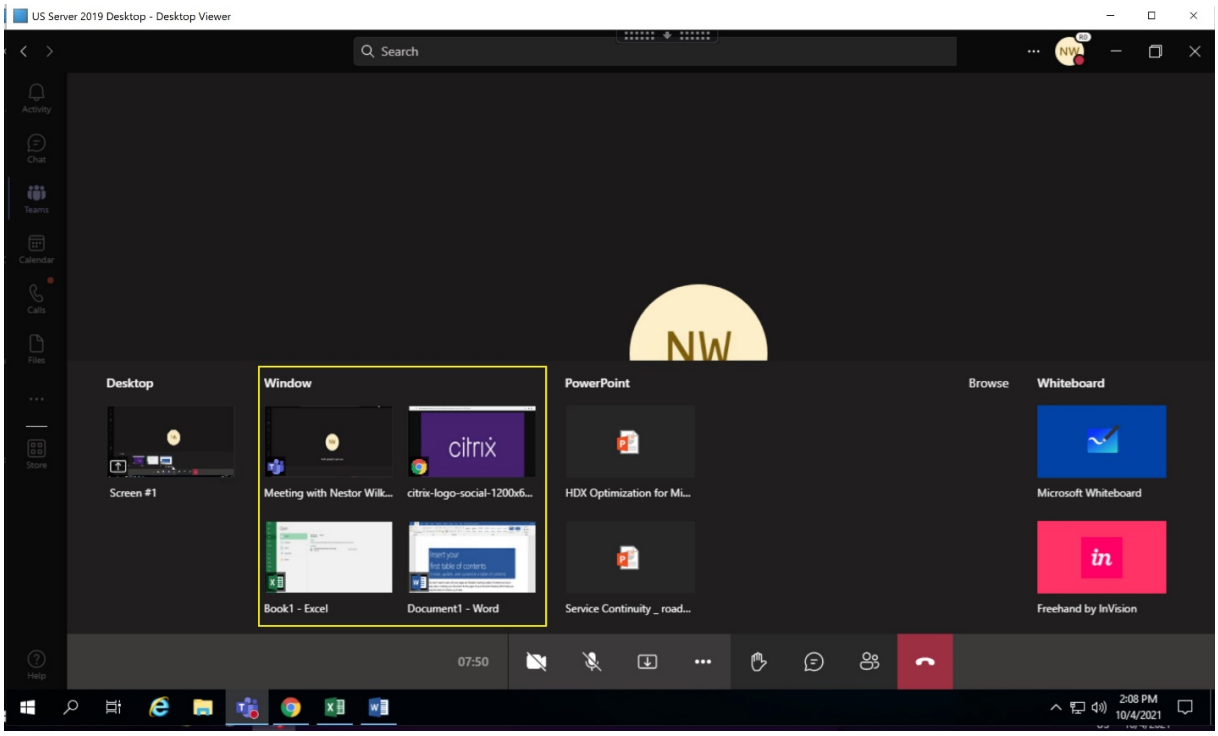
1. Accédez à l'application Microsoft Teams dans votre session à distance.
2. Cliquez sur **Partager du contenu** dans votre interface utilisateur Microsoft Teams.
3. Sélectionnez une application à partager lors de la réunion. La bordure rouge apparaît autour de l'application que vous avez sélectionnée et les participants à l'appel peuvent voir l'application partagée.

Pour partager une autre application, cliquez à nouveau sur **Partager du contenu** et sélectionnez une nouvelle application.

Si vous souhaitez désactiver le partage d'applications, créez la clé de registre suivante sur le VDA sur `HKLM\SOFTWARE\Citrix\Graphics`:
Nom : `UseWsProvider`
Type : `DWORD`
Valeur : 0

> **Remarque :**
>
> - Si vous réduisez une application, Microsoft Teams affiche la dernière image de l'application partagée. Vous pouvez agrandir la fenêtre pour reprendre le partage d'écran.
> - Le partage d'écran dépend de la capture de la fenêtre côté VDA. Le contenu est ensuite relayé à un débit maximum vers l'application Citrix Workspace. Le débit maximum est de 30 images par seconde. L'application Citrix Workspace transmet le contenu au serveur homologue ou de conférence.




**Limitations connues du partage d'écran d'une application spécifique :**

- Le pointeur de la souris n'est pas visible lorsque vous partagez l'écran d'une application.
- Si vous réduisez une application lorsque vous la partagez, seule l'icône de l'application apparaît dans le sélecteur d'écran. La vignette de l'application n'est pas prévisualisée dans le sélecteur d'écran. Vous ne pouvez pas partager le contenu et la bordure rouge n'apparaît pas tant que vous n'avez pas maximisé l'application.

- Les applications LAA affichent une liste des applications qui peuvent être partagées avec des applications de bureau dans Microsoft Teams optimisé dans le VDA. Toutefois, lorsque vous sélectionnez l'application dans la liste, le résultat peut ne pas être celui attendu.

**Compatibilité avec la protection des applications**
Le partage d'écran d'une application spécifique est compatible avec la fonction de protection des applications de Microsoft Teams optimisé pour HDX. Vous pouvez partager l'écran d'une application spécifique si vous avez lancé l'application ou le bureau à partir d'un groupe de mise à disposition pour lequel la protection des applications est activée.

Lorsque vous cliquez sur **Partager du contenu** dans l'interface utilisateur de Microsoft Teams, le sélecteur d'écran supprime l'option **Bureau**. Vous pouvez uniquement sélectionner l'option **Fenêtre** pour partager une application ouverte.

> **Remarque :**
>
> Lorsque vous lancez des applications ou des bureaux à partir d'un groupe de mise à disposition avec la protection des applications activée, vous ne pouvez pas voir la vidéo entrante ou le partage d'écran si vous utilisez l'application Citrix Workspace pour Windows 2202 ou une version antérieure.

**Donner ou demander le contrôle dans Microsoft Teams** Cette fonctionnalité est prise en charge dans les versions suivantes de l'application Citrix Workspace (elle ne dépend pas de la version du VDA ou du système d'exploitation, du mode mono-session ou multi-session) :

- Application Citrix Workspace pour Windows version 2112.1 ou ultérieure
- Application Citrix Workspace pour Mac version 2203.1 ou ultérieure
- Application Citrix Workspace pour Linux version 2203 ou ultérieure
- Application Citrix Workspace pour ChromeOS version 2303 ou ultérieure

Vous pouvez demander le contrôle lors d'un appel Microsoft Teams lorsqu'un participant partage l'écran. Une fois que vous avez le contrôle, vous pouvez effectuer des sélections, des modifications ou d'autres activités du clavier et de la souris sur l'écran partagé.

Pour prendre le contrôle lorsqu'un écran est partagé, cliquez sur le bouton **Demander le contrôle** dans l'interface utilisateur Microsoft Teams. Le participant à la réunion qui partage l'écran peut accepter ou refuser votre demande.

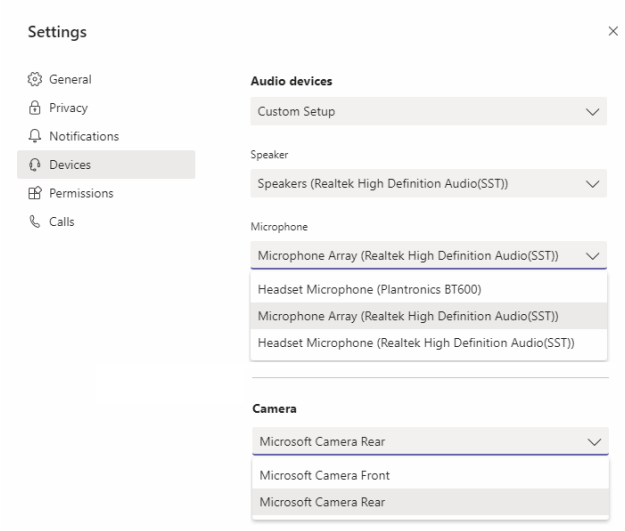
Tant que vous avez le contrôle, vous pouvez effectuer des sélections, des modifications et d'autres activités sur l'écran partagé. Pour ces actions, vous pouvez utiliser à la fois le clavier et la souris. Lorsque vous avez terminé, cliquez sur **Demander le contrôle**.

> **Limitations :**
>
> - Les contrôles Donner et Demander ne sont pas disponibles si l'utilisateur partage une seule application (également appelé partage d'applications). L'ensemble du bureau ou du moniteur doit être partagé.
> - La fonction permettant d'épingler la barre de commande à un emplacement spécifique n'est pas disponible.

## Périphériques dans Microsoft Teams

Lorsque l'optimisation pour Microsoft Teams est active, l'application Citrix Workspace accède aux périphériques (casques, microphones, caméras, haut-parleurs, etc.). Ensuite, les périphériques sont correctement répertoriés dans l'interface utilisateur Microsoft Teams (**Paramètres > Périphériques**).




Microsoft Teams n'accède pas directement aux périphériques, mais s'appuie sur le moteur multimédia WebRTC de l'application Workspace pour l'acquisition, la capture et le traitement des médias. Microsoft Teams répertorie les périphériques que l'utilisateur peut sélectionner.

Les périphériques insérés lorsque Microsoft Teams est actif ne sont pas sélectionnés par défaut. Vous devez sélectionner manuellement les périphériques à partir de l'écran **Paramètres** > **Appareils** de l'interface utilisateur Microsoft Teams. Une fois le périphérique sélectionné, Microsoft Teams met en cache les informations des périphériques. Par conséquent, les périphériques sont automatiquement sélectionnés lorsque vous vous reconnectez à une session à partir du même point de terminaison.

**Recommandations :**

- Casques certifiés Microsoft Teams avec annulation de l'écho intégrée. Un écho peut se produire dans les configurations comportant des périphériques supplémentaires, où le microphone et les haut-parleurs se trouvent sur des périphériques distincts. Par exemple, une webcam avec

un microphone intégré et un moniteur avec des haut-parleurs. Lorsque vous utilisez des haut-parleurs externes, placez-les le plus loin possible du microphone. Éloignez-les également de toute surface susceptible de réfracter le son dans le microphone. Pour plus d'informations, accédez à www.microsoft.com et recherchez des casques certifiés Microsoft Teams.

- Caméras certifiées Microsoft Teams, bien que les périphériques certifiés Skype Entreprise soient compatibles avec Microsoft Teams. Pour plus d'informations, accédez à et recherchez des caméras certifiées Microsoft Teams et des périphériques certifiés Skype Entreprise.
- Le moteur multimédia de l'application Citrix Workspace ne peut pas profiter du déchargement CPU avec des webcams qui exécutent le codage H.264 intégré -UVC 1.1 et 1.5.

> **Remarque :**
>
> L'application Workspace 2009.6 pour Windows peut désormais acquérir des périphériques avec des formats audio 24 bits ou avec des fréquences supérieures à 96 kHz.
>
> HdxTeams.exe (dans l'application Citrix Workspace pour Windows 2009 ou versions ultérieures) prend en charge uniquement ces formats de périphériques audio spécifiques (canaux, profondeur de bits et taux d'échantillonnage) :
>
> - Périphériques de lecture : jusqu'à 2 canaux, 16 bits, fréquences jusqu'à 96 000 Hz
> - Périphériques d'enregistrement : jusqu'à 4 canaux, 16 bits, fréquences jusqu'à 96 000 Hz
>
> Même si un seul haut-parleur ou un microphone ne correspond pas aux paramètres attendus, l'énumération des périphériques dans Microsoft Teams échoue et **Aucun** s'affiche sous **Paramètres > Périphériques**.
> Les journaux
> **Webrpc** dans **HDXTeams.exe** montrent ce type d'informations :
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing
> ...
> ```
>
> ```
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't
> create audio module!
> ```
>
> Pour contourner le problème, désactivez le périphérique spécifique ou :
>
> 1. Ouvrez le **Panneau de configuration Sons** (mmsys.cpl).
> 2. Sélectionnez le périphérique de lecture ou d'enregistrement.
> 3. Accédez à **Propriétés > Avancé** et réglez les paramètres sur un mode pris en charge.

#### Mode de secours

Si Microsoft Teams ne parvient pas à se charger en mode VDI optimisé (« Citrix HDX non connecté » dans Microsoft Teams/À propos de/Version), le VDA revient aux technologies HDX héritées. Les tech-

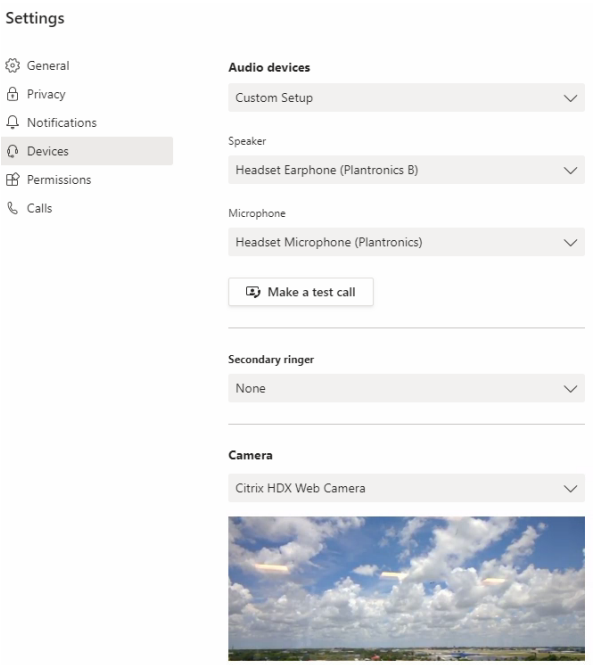
 

nologies HDX héritées peuvent être la redirection de webcam et la redirection de l'audio et du microphone client. Si vous utilisez un système d'exploitation ou une version d'application Workspace qui ne prend pas en charge l'optimisation Microsoft Teams, les clés de Registre de secours ne s'appliquent pas.
En mode de secours, les périphériques sont mappés au VDA. Les périphériques apparaissent dans l'application Microsoft Teams comme s'ils étaient connectés localement au bureau virtuel.

Vous pouvez désormais contrôler de manière précise le mécanisme de secours en définissant les clés de Registre dans le VDA. Pour plus d'informations, reportez-vous à Mode de secours Microsoft Teams dans la liste des fonctionnalités gérées via le Registre.

Cette fonctionnalité requiert l'utilisation de Microsoft Teams version 1.3.0.13565 ou ultérieure.

Pour déterminer si vous êtes en mode optimisé ou non optimisé lorsque vous affichez l'onglet **Paramètres > Périphériques** dans Microsoft Teams, la différence la plus significative est le nom de la caméra. Si Microsoft Teams s'est chargé en mode non optimisé, les technologies HDX héritées sont lancées. Le nom de la webcam a le suffixe **Citrix HDX**, comme indiqué dans le graphique suivant. Les noms des périphériques haut-parleur et microphone peuvent être légèrement différents (ou tronqués) par rapport au mode optimisé.




Lorsque les technologies HDX héritées sont utilisées, Microsoft Teams ne décharge pas le traitement audio, vidéo et partage d'écran vers le moteur multimédia WebRTC de l'application Citrix Workspace du point de terminaison. Les technologies HDX utilisent le rendu côté serveur à la place. La consommation de CPU sur le VDA est élevée lorsque vous activez la vidéo. Les performances audio en temps réel peuvent ne pas être optimales.

## Limitations connues

### Limitations Citrix

Limitations de l'application Citrix Workspace :

- Boutons HID - Réponse et fin des appels non pris en charge. Augmentation et baisse du volume sont pris en charge.
- Les paramètres QoS dans le Centre d'administration pour Microsoft Teams ne s'appliquent pas aux utilisateurs VDI.
- Les utilisateurs ne peuvent pas prendre de captures d'écran du contenu Microsoft Teams s'ils utilisent un outil de capture d'écran sur le VDA. Toutefois, si un outil de capture est utilisé côté client, le contenu peut être capturé.

Limitation du VDA :

- Lorsque vous configurez le paramètre **DPI élevé de l'application Citrix Workspace** sur `Yes`, la fenêtre vidéo redirigée n'est pas correctement positionnée. Cette limitation se produit lorsque le facteur d'échelle DPI du moniteur est défini sur une valeur supérieure à 100 %.

Limitations de l'application Citrix Workspace et du VDA :

- Vous pouvez uniquement contrôler le volume d'un appel optimisé à l'aide de la barre de volume sur la machine cliente, et non pas sur le VDA.

### Diffusion simultanée

La prise en charge de la diffusion simultanée est activée pour des visioconférences Microsoft Teams optimisées sous Windows et Mac. Pour Linux, renseignez-vous auprès de votre fournisseur de client léger.
Avec la diffusion simultanée, la qualité et l'expérience des visioconférences sur différents terminaux sont améliorées en s'adaptant à la résolution appropriée pour offrir la meilleure expérience d'appel à tous les appelants.

Grâce à cette expérience améliorée, chaque utilisateur peut diffuser plusieurs flux vidéo dans différentes résolutions (par exemple, 720p, 360p, etc.) en fonction de plusieurs facteurs, notamment la capacité du terminal, les conditions du réseau, etc. Le point de terminaison récepteur demande ensuite la résolution de qualité maximale qu'il peut gérer, offrant ainsi à tous les utilisateurs une expérience vidéo optimale.

> **Remarque :**
>
> Cette fonctionnalité est disponible uniquement après le déploiement d'une mise à jour de Microsoft Teams. Pour plus d'informations sur l'estimation de date de publication, accédez à https:

> //www.microsoft.com/ et recherchez la feuille de route de Microsoft 365. Une fois la mise à jour déployée par Microsoft, vous pourrez consulter l'article CTX253754 pour obtenir la mise à jour de la documentation et l'annonce.

#### Limitations Microsoft

- La vue Galerie 3x3 n'est pas prise en charge. Dépendance de Microsoft Teams : contactez Microsoft pour connaître la date de disponibilité de la grille 3x3.
- L'interopérabilité avec Skype Entreprise est limitée aux appels audio, la vidéo n'est pas disponible.
- La résolution maximale des flux vidéo entrants et sortants est de 720p.
- La tonalité de rappel RTC n'est pas prise en charge.
- La déviation du trafic multimédia pour le routage direct n'est pas prise en charge.
- Les rôles de producteur et de présentateur d'événements diffusés et en direct ne sont pas pris en charge. Le rôle de participant est pris en charge mais non optimisé (rendu sur le VDA).
- La fonction zoom avant et zoom arrière dans Microsoft Teams n'est pas prise en charge.
- Le routage géodépendant et la déviation du trafic multimédia ne sont pas pris en charge.
- La fusion des appels n'est pas prise en charge (option non affichée dans l'interface utilisateur).

#### Limitations Citrix et Microsoft

- Lors du partage d'écran, l'option **Inclure l'audio système** n'est pas disponible.
- La diffusion simultanée n'est pas prise en charge sur ChromeOS.

### Fin de vie prochaine pour l'interface utilisateur à fenêtre unique de Microsoft Teams

À partir du 31 janvier 2024, Microsoft ne prendra plus en charge l'interface utilisateur à fenêtre unique de Microsoft Teams lors de l'utilisation de l'optimisation VDI Microsoft Teams et ne prendra en charge que l'expérience en mode multi-fenêtres. Microsoft a annoncé cette fin de prise en charge le 8 septembre 2023 dans le centre d'administration M365s (ID de publication : MC674419).
Des informations publiques sur la fonction multi-fenêtres sont disponibles dans l'article Tech Community : New Meeting and Calling Experience in Microsoft Teams.

> **Remarque :**
>
> Citrix vous recommande de mettre à niveau votre VDA et votre application Citrix Workspace vers les versions prises en charge pour continuer à utiliser Microsoft Teams en mode optimisé pour les vidéos et le partage d'écran. Si vous ne mettez pas à niveau votre infrastructure et vos points de terminaison pour prendre en charge les fenêtres multiples, vos appels, vos appels vidéo et votre partage d'écran ne seront pas optimisés. Cela peut entraîner des problèmes de qualité

> des appels, une augmentation de la latence et une augmentation de la charge sur le serveur.

Le tableau suivant illustre les versions minimale, LTSR et recommandée du VDA et de l'application Citrix Workspace requises pour continuer à utiliser les appels optimisés dans Microsoft Teams sur Citrix VDI :

| Composant | Version minimale (1) | Version compatible LTSR (2) | Version recommandée (3) |
|---|---|---|---|
| Microsoft Teams | 1.5.00.11865 | Non applicable | Dernière version |
| VDA | 1912 CU6 LTSR, 2109 CR, 2203 LTSR | 1912 CU8+, 2203 LTSR CU2+ (4) | 2308 CR+ |
| Application Citrix Workspace pour Windows | 2112.1 CR | 2203 CU2+ (4) | 2309 CR+ |
| Application Citrix Workspace pour Mac | 2203 CR | Non applicable | 2308 CR+ |
| Application Citrix Workspace pour Linux | 2202 CR | Non applicable | 2308 CR+ |
| Application Citrix Workspace pour ChromeOS ou HTML5 | 2303 CR | Non applicable | 2309 CR+ |

> **Remarques :**
>
> 1. Version minimale : il s'agit de la version dans laquelle le mode multi-fenêtres a été introduit pour la première fois. Certaines versions minimales répertoriées ici peuvent être en fin de vie.
> 2. Version compatible LTSR : il s'agit de la version LTSR prise en charge par Citrix pour les fenêtres multiples. Les anciennes versions peuvent fonctionner, mais le support n'est plus disponible pour ces versions une fois qu'une nouvelle version LTSR CU est publiée. Pour en savoir plus sur les stratégies de support LTSR, consultez https://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr.
> 3. Version recommandée : il s'agit de la version du logiciel que Citrix recommande si l'utilisateur/le client choisit de mettre à niveau son logiciel. Ce sont toutes des versions actuelles.
> 4. La version 2203 de LTSR pour les versions de base VDA et CWA inclut la fonction multi-fenêtres. Ces versions ont été remplacées par la dernière version CU, qui est la version officiellement prise en charge. Les clients peuvent continuer à utiliser ces versions non prises en charge à leur discrétion. Citrix encourage les clients utilisant la version LTSR à passer à

> la dernière version CU.

## Annonce de fin de prise en charge du format SDP (Plan B) de WebRTC

Citrix prévoit de mettre fin à la prise en charge actuelle du format SDP (Plan B) de WebRTC dans les prochaines versions. Vous devez utiliser le format Unified Plan dans WebRTC pour prendre en charge les fonctionnalités optimisées de Microsoft Teams.

### Produits concernés

Dans l'une des versions futures de l'application Citrix Workspace, les appels entre les points de terminaison dotés de la prochaine version de l'application Citrix Workspace et les points de terminaison dotés de l'application Citrix Workspace 2108 ou de versions antérieures ne seront pas pris en charge. Cette incompatibilité d'appel inclut les clients de l'application Citrix Workspace (CWA) LTSR 1912. Les clients CWA suivants sont concernés :

- Application Citrix Workspace pour Windows
- Application Citrix Workspace pour Linux
- Application Citrix Workspace pour Mac
- Application Citrix Workspace pour Chrome

### Remplacement du format Plan B

Si vous utilisez la version de l'application Citrix Workspace antérieure à 2109, vous devez passer à une version prise en charge (de préférence la version actuelle ou CR). Dans le cas contraire, tout appel utilisant une version future ou des terminaux plus récents ne parviendra pas à se connecter. Les appels entre les versions futures et vos partenaires de communication fédérés risquent également d'échouer si le partenaire fédéré n'a pas mis à niveau son instance Citrix Workspace.

La version 2108 de l'application Citrix Workspace a atteint sa date limite de prise en charge en mars 2023 et doit être mise à niveau vers une version plus récente. Consultez la page relative à l'application Workspace pour plus d'informations sur la prise en charge des versions de l'application Citrix Workspace.

Pour plus d'informations sur la fin de la prise en charge du format Plan B, consultez la documentation de WebRTC.

## Informations supplémentaires

- Surveiller, dépanner et prendre en charge Microsoft Teams

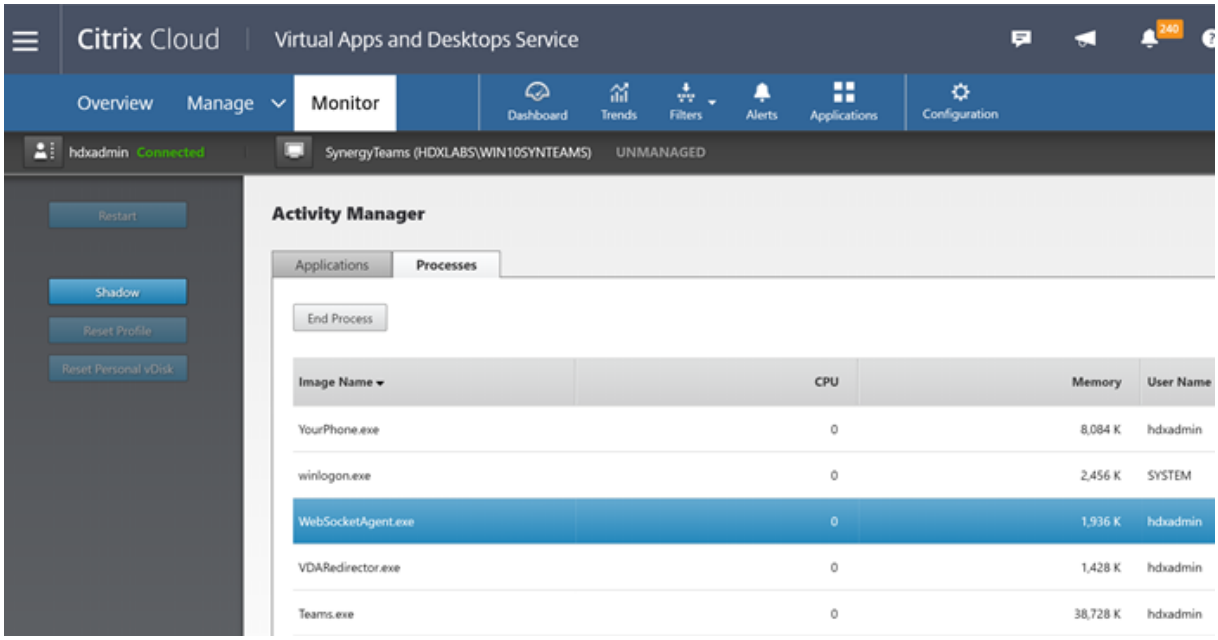
- Déployer l'application de bureau Microsoft Teams sur la machine virtuelle
- Installer Microsoft Teams à l'aide de MSI (section Installation de VDI)
- Clients légers
- Outil d'évaluation de réseau Skype Entreprise
- Comprendre la coexistence et l'interopérabilité de Microsoft Teams et Skype Entreprise

## Surveiller, dépanner et prendre en charge Microsoft Teams

June 27, 2024

### Surveillance de Teams

Cette section fournit des instructions pour la surveillance de l'optimisation Microsoft Teams avec HDX. Si vous exécutez le mode optimisé et que `HdxRtcEngine.exe` s'exécute sur la machine cliente, un processus dans le VDA appelé `WebSocketAgent.exe` s'exécute dans la session. Utilisez le **Gestionnaire d'activités** dans Director pour afficher l'application.




Le statut d'optimisation de Microsoft Teams peut être consulté dans la page Director > **Détails de l'utilisateur** > panneau **Détails de la session** > champ **Optimisation MS Teams**. L'optimisation de Microsoft Teams est essentielle pour une meilleure expérience utilisateur, notamment pour un son et une vidéo clairs. Cette fonctionnalité est disponible pour les versions 2311 et ultérieures du VDA. Les versions de l'application Citrix Workspace prises en charge sont répertoriées dans Optimisation pour Microsoft Teams. Director affiche le statut d'optimisation de Microsoft Teams uniquement si Microsoft

Teams est exécuté en tant qu'application publiée ou sur un bureau publié.
Pour en savoir plus, voir Statut d'optimisation de Microsoft Teams.

Avec la version minimale du VDA, 1912, vous pouvez surveiller les appels Teams actifs à l'aide de Citrix HDX Monitor (version minimale 3.11). L'ISO du produit Citrix Virtual Apps and Desktops contient la dernière version de `hdxmonitor.msi` dans le dossier `layout\image-full\Support\HDX Monitor`.
Avec la version minimale du VDA, 1912, vous pouvez surveiller les appels Microsoft Teams actifs à l'aide de Citrix HDX Monitor (version minimale 3.11). L'ISO du produit Citrix Virtual Apps and Desktops contient la dernière version de `hdxmonitor.msi` dans le dossier `layout\image-full\Support\HDX Monitor`.

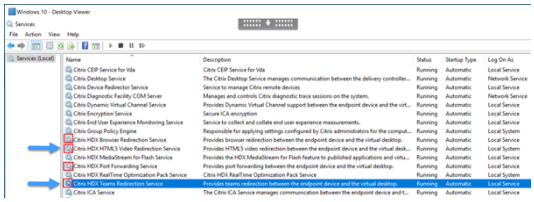
Pour plus d'informations, consultez la section *Surveillance* dans l'article CTX253754 du centre de connaissances.

## Dépannage

Cette section fournit des conseils de dépannage pour les problèmes que vous pourriez rencontrer lors de l'utilisation de l'optimisation de Microsoft Teams. Pour plus d'informations, veuillez consulter l'article CTX253754.

### Sur le VDA

Quatre services sont installés par BCR_x64.msi. Seuls deux de ces services sont responsables de la redirection Microsoft Teams dans le VDA.



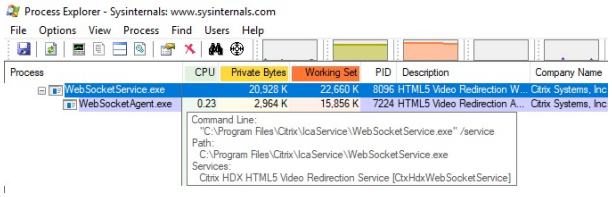
- **Citrix HDX Teams Redirection Service** établit le canal virtuel utilisé dans Microsoft Teams. Le service repose sur CtxSvcHost.exe.
- **Citrix HDX HTML5 Video Redirection Service** s'exécute en tant que WebSocketService.exe en écoute sur 127.0.0.1:9002 TCP. WebSocketService.exe exécute deux fonctions principales :

  i. La **terminaison TLS pour Secure WebSockets** reçoit une connexion WebSocket sécurisée de vdiCitrixPeerConnection.js, qui est un composant de l'application Microsoft Teams. Vous pouvez le suivre avec le moniteur de processus. Pour plus d'informations sur les certificats, consultez la section « Redirection vidéo TLS et HTML5 et redirection du contenu du navigateur » sous Communications entre le Controller et le VDA.

Certains logiciels de sécurité bureau et antivirus interfèrent avec le bon fonctionnement de `WebSocketService.exe` et de ses certificats. Bien que le service Citrix HDX HTML5 Video Redirection soit en cours d'exécution dans la console `services.msc`, le socket TCP `127.0.0.1:9002` de l'hôte local n'est jamais en mode d'écoute comme dans netstat. Lorsque vous essayez de redémarrer le service, il se bloque (« Arrêt… »). Veillez à appliquer les exclusions appropriées pour le processus `WebSocketService.exe`.

ii. **Mappage de session utilisateur.** Lorsque l'application Microsoft Teams démarre, WebSocketService.exe démarre le processus WebSocketAgent.exe dans la session de l'utilisateur dans le VDA. WebSocketService.exe s'exécute dans la session 0 en tant que compte LocalSystem.




Vous pouvez utiliser `netstat` pour vérifier si le service WebSocketService.exe est dans un état d'écoute actif dans le VDA.

Exécutez `netstat -anob -p tcp` à partir d'une fenêtre d'invite de commandes avec privilèges élevés :

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

En cas de connexion réussie, l'état passe à ESTABLISHED :

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

> **Important :**
>
> WebSocketService.exe écoute deux sockets TCP, 127.0.0.1:9001 et 127.0.0.1:9002. Le port 9001 est utilisé pour la redirection du contenu du navigateur et la redirection vidéo HTML5. Le port 9002 est utilisé pour la redirection de Microsoft Teams. Assurez-vous que vous n'avez pas dans le système d'exploitation Windows du VDA de configurations proxy qui peuvent empêcher une communication directe entre Teams.exe et WebSocketService.exe. Parfois, lorsque vous configurez un proxy explicite dans Internet Explorer 11, (**Options Internet > Connexions > Paramètres LAN > Serveur proxy**), les connexions peuvent circuler via un serveur proxy attribué. Vérifiez que l'option **Ne pas utiliser de serveur proxy pour les adresses locales** est cochée si vous utilisez

> un paramètre proxy manuel et explicite.

**Emplacements et descriptions des services**

| Service | Chemin d'accès au fichier exécutable dans le système d'exploitation Windows Server | Ouvrir une session en tant que | Description |
|---|---|---|---|
| Service de redirection vidéo Citrix HTML5 | "C:\Program Files (x86)\Citrix\System32\WebSocketService.exe" /service | Compte Système local | Fournit plusieurs services multimédia HDX avec l'infrastructure initiale requise pour effectuer la redirection de média entre le bureau virtuel et la machine de point de terminaison. |
| Service de redirection de navigateur Citrix HDX | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs | Ce compte (service local) | Permet de rediriger le contenu du navigateur entre la machine de point de terminaison et le bureau virtuel. |
| Service de transfert de port Citrix | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs | Ce compte (service local) | Permet de réacheminer le port entre la machine de point de terminaison et le bureau virtuel pour la redirection de contenu du navigateur. |
| Service de redirection de Teams Citrix HDX | "C:\Program Files (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs | Compte Système local | Offre une redirection de Microsoft Teams entre la machine de point de terminaison et le bureau virtuel. |

#### Application Citrix Workspace

Sur le point de terminaison de l'utilisateur, l'application Citrix Workspace pour Windows instancie un nouveau service appelé HdxTeams.exe ou HdxRtcEngine.exe. Elle le fait lorsque Microsoft Teams s'ouvre dans le VDA et que l'utilisateur tente d'appeler ou d'accéder à des périphériques en mode auto-aperçu. Si ce service ne s'affiche pas, vérifiez les points suivants :

1. Assurez-vous que vous avez installé au minimum la version 1905 de l'application Workspace pour Windows. Voyez-vous HdxTeams.exe ou HdxRtcEngine.exe et les binaires webrpc.dll dans le chemin d'installation de l'application Workspace ?
2. Si vous avez validé l'étape 1, procédez comme suit pour vérifier si HdxTeams.exe ou HdxRtcEngine.exe est lancé.
    a) Quittez Microsoft Teams sur le VDA.
    b) Démarrez services.msc sur le VDA.
    c) Arrêtez le service de Teams Citrix HDX.
    d) Déconnectez la session ICA.
    e) Connectez la session ICA.
    f) Démarrez le service de redirection de Teams Citrix HDX.
    g) Redémarrez le service de redirection vidéo Citrix HDX HTML5.
    h) Lancez Microsoft Teams sur le VDA.
3. Si HdxTeams.exe ou HdxRtcEngine.exe n'est toujours pas lancé sur le point de terminaison client, procédez comme suit :
    a) Redémarrez le VDA.
    b) Redémarrez le point de terminaison client.

### Assistance

Citrix et Microsoft prennent conjointement en charge la mise à disposition de Microsoft Teams à partir de Citrix Virtual Apps and Desktops à l'aide de l'optimisation pour Microsoft Teams. Cette prise en charge conjointe est le résultat d'une étroite collaboration entre les deux entreprises. Si vous avez des contrats de support valides et que vous rencontrez un problème avec cette solution, ouvrez un ticket de support avec le fournisseur dont le code semble être à l'origine du problème. Autrement dit, Microsoft pour Teams ou Citrix pour les composants d'optimisation.
Citrix ou Microsoft reçoivent le ticket, trient le problème et escaladent le problème le cas échéant. Vous n'avez pas besoin de contacter l'équipe de support de chaque entreprise.

Lorsque vous rencontrez un problème, nous vous recommandons de cliquer sur **Aide > Signaler un problème** dans l'interface utilisateur de Teams. Les journaux côté VDA sont automatiquement partagés entre Citrix et Microsoft pour résoudre les problèmes techniques plus rapidement.

**Collecte des journaux**

Les journaux HDX Media Engine se trouvent sur la machine de l'utilisateur (pas sur le VDA). En cas de problème, assurez-vous de joindre des journaux à votre ticket d'assistance.

**Journaux Windows :**

Les journaux Windows se trouvent dans %TEMP% dans le dossier **HDXTeams** (AppData/Local/Temp/HDXTeams ou AppData/Local/Temp/HdxRtcEngine). Recherchez un fichier .txt appelé webrpc_Day_Month_timestamp_Year.txt. Si vous utilisez des versions plus récentes de l'application Citrix Workspace, par exemple l'application Citrix Workspace 2009.5 ou une version ultérieure, stockez les journaux dans AppData\Local\Temp\HdxRtcEngine.

Chaque session crée un dossier distinct pour les journaux.

**Journaux Mac :**

1. Journal VDWEBRTC - enregistre l'exécution du canal virtuel.

   Emplacement : /Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt

2. Journal HdxRtcEngine - enregistre l'exécution des processus sur HdxRtcEngine.

   Emplacement : $TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log

   Le journal HdxRtcEngine est activé par défaut.

3. Journaux Webrpc - journaux les plus importants qui enregistrent l'exécution de la synthèse de la bibliothèque webrtc.

   Emplacement : /Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log

**Journaux Linux :**

Les journaux Linux se trouvent dans les dossiers /tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/.
Journal Webrtc : journal /tmp/webrpc/<current date>/webrtc.log
du noyau : /var/log/syslog

**ICE/STUN/TURN/ logs:**

Lors de l'établissement d'un appel, ces quatre phases de l'ICE sont requises :

- Récupération des candidats
- échange de candidats
- Vérifications de connectivité (demandes de liaison STUN)
- Promotion des candidats

Dans les journaux HdxRtcEngine.exe, les entrées suivantes sont les entrées ICE (Interactive Connectivity Establishment) pertinentes. Ces entrées doivent être là pour qu'un appel réussisse. Consultez l'exemple d'extrait suivant pour l'étape de collecte :

```
RPCStubs Info: -> device id = \?\display#int3470#4&1835d135&0&uid13424
    #{
 65e8773d-8f56-11d0-a3b9-00a0c9223196 }
 {
 bf89b5a5-61f7-4127-a279-e187013d7caf }
  label = Microsoft Camera Front groupId =

webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
webrtcapi.RTCPeerConnection Info: setLocalDescription.
>>> begin:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveLocalOffer

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Gathering

[...]
>>> begin:sdp
candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
    generation 0 ufrag oVk6 network-id 1
<<< end:sdp
[...]
>>> begin:sdp
candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
    raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
    network-cost 10
<<< end:sdp
[...]
>>> begin:sdp
candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx
    raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id
    1
<<< end:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
>>> begin:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveRemotelOffer

<!--NeedCopy-->
```

S'il y a plusieurs candidats ICE, l'ordre de préférence est :

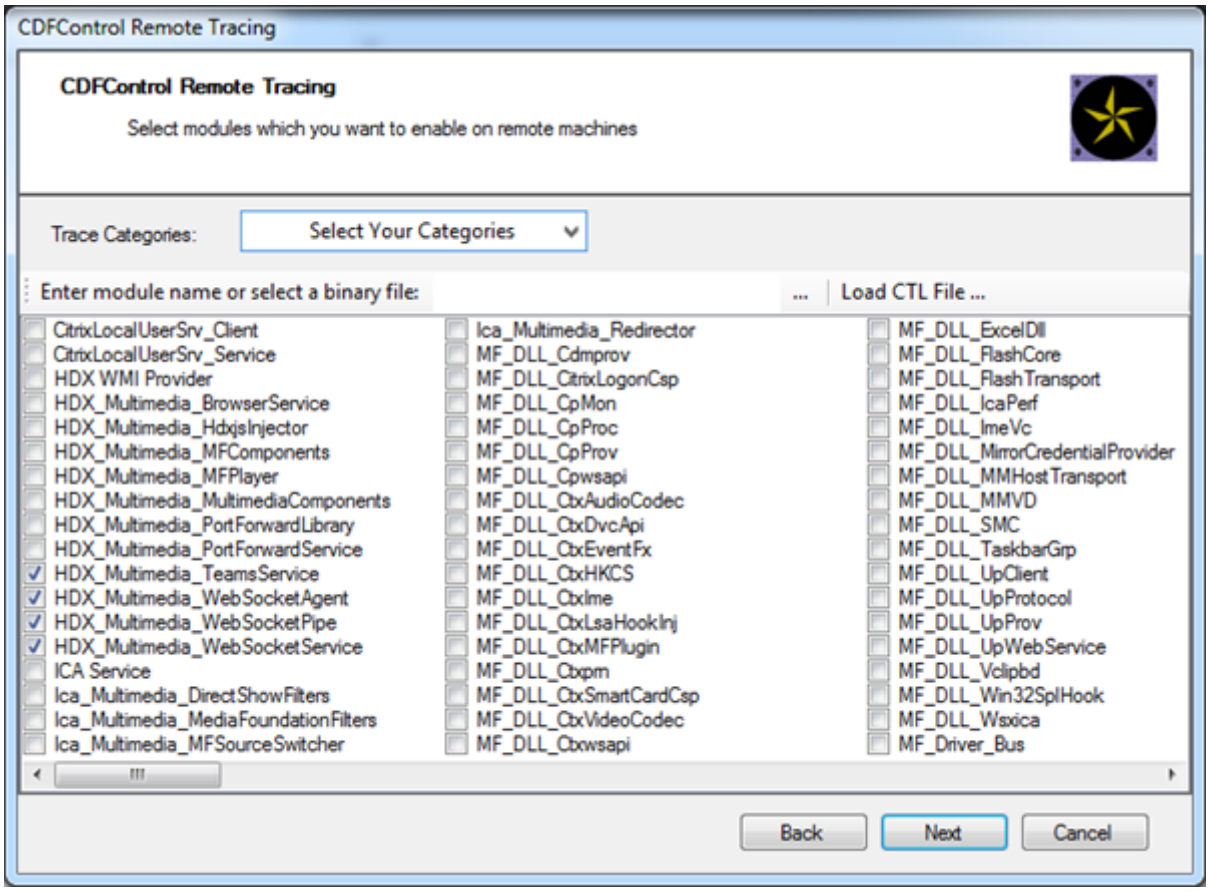
 

1. hôte
2. réflexion homologue
3. réflexion serveur
4. relais de transport

Si vous rencontrez un problème et que vous pouvez le reproduire, nous vous recommandons de cliquer sur **Aide > Signaler un problème** dans Microsoft Teams. Les journaux sont partagés entre Citrix et Microsoft pour résoudre les problèmes techniques si vous avez ouvert un dossier avec Microsoft. La capture de traces CDF avant de contacter le support Citrix est également recommandée. Pour plus d'informations, consultez l'article CDFcontrol du centre de connaissances.

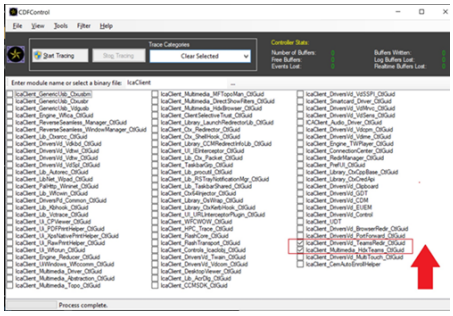
Pour obtenir des recommandations sur la collecte des traces CDF, consultez l'article du centre de connaissances Recommandations pour la collecte des traces CDF.

**Traces CDF côté VDA - Activez les fournisseurs de traces CDF suivants :**




**Traces CDF côté application Workspace - Activez les fournisseurs de traces CDF suivants :**



- IcaClient_DriversVd_TeamsRedir (facultatif)
- IcaClient_Multimedia_HdxTeams (nécessite l'application Citrix Workspace 2012 ou ultérieure)

## Redirection Windows Media

June 27, 2024

La redirection Windows Media permet de contrôler et d'optimiser le mode de livraison en streaming des données audio et vidéo par les serveurs vers les utilisateurs. Par la lecture des fichiers d'exécution multimédia sur la machine utilisateur plutôt que sur le serveur, la redirection Windows Media réduit les besoins en bande passante pour la lecture de fichiers multimédia. La redirection Windows Media améliore les performances du lecteur Windows Media et les lecteurs compatibles exécutés sur des bureaux virtuels Windows.

Si la configuration requise pour la récupération de contenu Windows Media côté client n'est pas présente, la mise à disposition utilise automatiquement la récupération côté serveur. Cette méthode est transparente pour les utilisateurs. Vous pouvez utiliser Citrix Scout pour effectuer une trace Citrix diagnostic Facility (CDF) depuis HostMMTransport.dll pour déterminer la méthode utilisée. Pour plus d'informations, voir Citrix Scout.

La redirection Windows Media intercepte le pipeline multimédia au niveau du serveur hôte, capture les données multimédia dans leur format compressé natif et redirige le contenu vers la machine cliente. La machine cliente recrée ensuite le pipeline multimédia pour décompresser et restituer les données multimédia reçues depuis le serveur hôte. La redirection Windows Media fonctionne correctement sur les machines clientes exécutant un système d'exploitation Windows. Ces machines disposent de l'infrastructure multimédia requise pour reconditionner le pipeline multimédia tel qu'il était sur le serveur hôte. Les clients Linux utilisent des infrastructures open-source similaires pour reconditionner le pipeline multimédia.

Le paramètre de stratégie **Redirection Windows Media** contrôle cette fonctionnalité et est **Autorisé** par défaut. En général, ce paramètre améliore la qualité des données audio et vidéo restituées par le serveur à un niveau comparable à celui obtenu avec des applications exécutées localement sur les

machines clientes. Dans de rares cas, la qualité obtenue avec la redirection Windows Media semble inférieure à celle obtenue à l'aide de la compression ICA de base et des réglages audio standard. Vous pouvez désactiver cette fonctionnalité en ajoutant le paramètre **Redirection Windows Media** à une stratégie et en définissant sa valeur sur **Interdit**.

Pour de plus amples informations sur les paramètres de stratégie, consultez Paramètres de stratégie multimédia.

**Limitation :**

Lorsque vous utilisez le lecteur Windows Media avec RAVE activé dans une session, un écran noir peut s'afficher. Cet écran noir peut apparaître si vous cliquez avec le bouton droit sur le contenu vidéo et que vous sélectionnez **Lecture en cours toujours visible**.

## Redirection de contenu générale

June 27, 2024

La redirection de contenu vous permet de contrôler si les utilisateurs accèdent aux informations à l'aide d'applications publiées sur des serveurs ou d'applications exécutées localement sur les machines utilisateur.

### Redirection de dossiers clients

La redirection de dossiers clients modifie la manière dont les fichiers côté client sont accessibles sur la session côté hôte.

- Lorsque vous activez uniquement le mappage de lecteur client sur le serveur, les volumes complets côté client sont automatiquement mappés sur les sessions en tant que liens UNC (Universal Naming Convention).
- Lorsque vous activez la redirection de dossiers clients sur le serveur et que l'utilisateur la configure sur la machine de bureau Windows, la partie du volume local spécifié par l'utilisateur est redirigée.

### Redirection hôte vers client

La redirection hôte vers client peut être utilisée dans certains scénarios d'utilisation peu courants. En général, les autres méthodes de redirection de contenu peuvent être préférables. Ce type de redirection est pris en charge uniquement sur les VDA avec OS multi-session (et non pas les VDA avec OS mono-session).

### Local App Access et redirection d'adresse URL

Local App Access s'intègre en toute transparence aux applications Windows installées localement dans un environnement de bureau hébergé sans passer d'un ordinateur à l'autre.

La technologie HDX offre la **redirection USB générique** pour les périphériques spécialisés dont la prise en charge n'est pas optimisée ou n'est pas adaptée.

## Redirection de dossiers clients

June 27, 2024

La redirection de dossiers clients modifie la manière dont les fichiers côté client sont accessibles sur la session côté hôte. Si vous activez uniquement le mappage de lecteur client sur le serveur, les volumes complets côté client sont automatiquement mappés en tant que liens UNC (Universal Naming Convention) vers les sessions. Lorsque vous activez la redirection de dossiers clients sur le serveur et que l'utilisateur la configure sur la machine utilisateur, la partie du volume local spécifié par l'utilisateur est redirigée.

Seuls les dossiers spécifiés par l'utilisateur apparaissent en tant que liens UNC à l'intérieur des sessions, autrement dit, au lieu du système de fichiers complet sur la machine utilisateur. Si vous désactivez les liens UNC via le registre, des dossiers clients apparaissent comme des lecteurs mappés au sein de la session.

La redirection de dossiers clients est prise en charge sur les machines avec OS mono-session Windows uniquement.

La redirection de dossiers clients d'un lecteur USB externe ne sera pas enregistrée suite à la déconnexion puis reconnexion de l'appareil.

Activez la redirection de dossiers clients sur le serveur. Ensuite, sur la machine cliente, spécifiez les dossiers à rediriger. L'application utilisée pour spécifier les options du dossier client est incluse avec l'application Citrix Workspace fournie avec cette version.

**Exigences :**

Pour les serveurs :

- Windows Server 2022
- Windows Server 2019, éditions Standard et Datacenter
- Windows Server 2016, édition Standard et Datacenter
- Windows Server 2012 R2, édition Standard et Datacenter.

Pour les clients :

- Windows 10, éditions 32 bits et 64 bits (minimum version 1607)
- Windows 8.1, éditions 32 bits et 64 bits (y compris l'édition Embedded)
- Windows 7, éditions 32 bits et 64 bits (y compris l'édition Embedded)

Pour activer la redirection de dossier client sur le serveur, reportez-vous à Redirection de dossiers clients dans la liste des fonctionnalités gérées via le Registre.

Sur la machine utilisateur, spécifiez les dossiers à rediriger :

1. Vérifiez que la dernière version de l'application Citrix Workspace est installée.
2. À partir du répertoire d'installation de l'application Citrix Workspace, démarrez CtxCFRUI.exe.
3. Sélectionnez le bouton radio **Personnaliser** et ajoutez, modifiez ou supprimez des dossiers.
4. Déconnectez-vous et reconnectez-vous à vos sessions pour que le paramètre prenne effet.

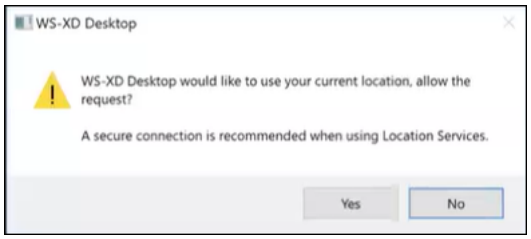
## Redirection de la localisation du client

June 27, 2024

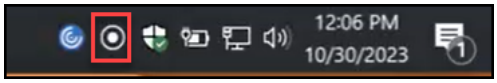
Lorsqu'elle est activée, la redirection de localisation du client permet aux applications et aux sessions de bureau hébergées sur VDA d'accéder facilement à la position actuelle du client. Sur un système d'exploitation multisession (TS VDA ou Multi-Session WS VDA), chaque session dispose d'une localisation unique fournie par le client connecté. Grâce à cette fonctionnalité, les applications du VDA qui dépendent de la position disposent de la localisation précise du client.

Pour de plus amples informations, consultez la documentation de Microsoft.

Une fois la redirection de localisation du client activée et l'accès à la localisation autorisé à la fois côté serveur et côté client, lorsque vous lancez une application ou un poste de travail accédant à la localisation, le client vous invite à partager sa position actuelle à l'aide de la boîte de dialogue suivante :




Lorsque vous activez la redirection de localisation du client, l'icône suivante apparaît dans la barre des tâches du client si/lorsque l'application ou le bureau hébergé par un VDA interroge les informations de localisation actuelles.




### Configuration système requise

Pour les serveurs :

- OS VDA session unique (Win10/11) ou multi-sessions (Win 11 22H2 et Server 2022 23H2 ou version ultérieure)
- Application Citrix Workspace pour Windows, iOS ou Android

### Configuration

La redirection de la localisation du client doit être activée à l'aide de la stratégie Citrix pour que la fonctionnalité fonctionne. La redirection de la localisation du client est désactivée par défaut.

Pour activer la redirection de la localisation du client, procédez comme suit :

Côté Windows VDA et côté client :

1. Depuis les **Paramètres > Confidentialité > Localisation**, activez les options suivantes :
   - **Autoriser l'accès à la localisation sur cet appareil**
   - **Autoriser les applications à accéder à votre position**
   - **Autoriser les applications de bureau à accéder à votre localisation**
2. Pour les systèmes d'exploitation multi-sessions, activez le paramètre **Remplacer la localisation**.

Pour Controller/DDC :

Activez la stratégie **Studio > Stratégies > Localisation > Paramètres > Autoriser l'application à utiliser l'emplacement physique de l'appareil client**.
Pour en savoir plus, consultez la section Paramètres de stratégie des capteurs clients.

## Redirection bidirectionnelle du contenu

June 27, 2024

La redirection bidirectionnelle du contenu permet de transférer des URL HTTP ou HTTPS dans les navigateurs Web, ou intégrées aux applications, entre la session VDA Citrix et le point de terminaison client dans les deux sens. Une URL saisie dans un navigateur exécuté dans la session Citrix peut être ouverte à l'aide du navigateur par défaut du client. Inversement, une URL saisie dans un navigateur exécuté sur le client peut être ouverte dans une session Citrix, avec une application ou un bureau publié. Exemples de cas d'utilisation courants pour la redirection bidirectionnelle du contenu :

- Redirection des URL Web dans les cas où le navigateur de départ n'a pas d'accès réseau à la source.
- Redirection des URL Web pour des raisons de compatibilité et de sécurité du navigateur.
- La redirection des URL Web intégrées aux applications lors de l'exécution d'un navigateur Web sur la session Citrix où le client n'est pas souhaitée.

### Configuration système requise

- VDA avec OS mono-session ou multi-session
- Application Citrix Workspace pour Windows

Navigateurs :

- Google Chrome avec extension de redirection Citrix Browser (disponible sur le Google Chrome Web Store)
- Microsoft Edge (Chromium) avec extension de redirection Citrix Browser (disponible sur le Google Chrome Web Store)

### Configuration

À partir de Citrix Virtual Apps and Desktops 2311, la redirection bidirectionnelle du contenu est configurée via Citrix Studio uniquement. Les paramètres de stratégie des versions précédentes étaient configurés à la fois sur le terminal client et sur Studio. La redirection bidirectionnelle du contenu est désactivée par défaut.

Pour la configuration du VDA, consultez la section Redirection bidirectionnelle du contenu dans les paramètres de **stratégie ICA**.

Pour que la redirection du navigateur fonctionne, les extensions de navigateur doivent être enregistrées sur le navigateur d'origine (d'où l'URL est redirigée) à l'aide des commandes affichées. Exécutez les commandes selon vos besoins sur le VDA et le client en fonction du navigateur utilisé.

| Navigateur | VDA | Client |
|---|---|---|
| Google Chrome | %ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /regChrome | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome |
| Microsoft Edge | %ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /regEdge | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regEdge |
| Tous les navigateurs disponibles | %ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /regall | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regall |

Pour annuler l'enregistrement d'une extension de navigateur :

| Navigateur | VDA | Client |
|---|---|---|
| Google Chrome | %ProgramFiles(x86)%\Citrix\HDX\bin\ogamedirect.exe /unregChrome | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome |
| Microsoft Edge | %ProgramFiles(x86)%\Citrix\HDX\bin\ogamedirect.exe /unregEdge | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregEdge |
| Tous les navigateurs disponibles | %ProgramFiles(x86)%\Citrix\HDX\bin\ogamedirect.exe /unregall | %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregall |

> **Remarque :**
>
> Avec la commande register, les navigateurs Chrome et Edge invitent les utilisateurs à activer l'extension de redirection du navigateur Citrix lors du premier lancement. L'extension de navigateur peut également être installée manuellement à partir du Google Chrome Web Store. Pour Microsoft Edge, voir également Ajouter une extension à Microsoft Edge depuis le Chrome Web Store.

### Redirection générique depuis le VDA Citrix vers le client

La redirection bidirectionnelle du contenu prend en charge l'utilisation de caractères génériques lors de la définition des URL à rediriger. Pour configurer la redirection bidirectionnelle du contenu, consultez les instructions de configuration.

### Redirection de protocole personnalisé depuis le VDA vers le client

La redirection bidirectionnelle du contenu prend en charge la redirection de protocoles personnalisés depuis le VDA Citrix vers le client. Les protocoles autres que HTTP ou HTTPS sont pris en charge. Pour configurer la redirection bidirectionnelle du contenu, consultez les instructions de configuration.

Dans Web Studio, définissez le protocole personnalisé dans **Redirection bidirectionnelle du contenu**.

> **Remarque :**
>
> - Vous devez disposer de privilèges d'administrateur pour exécuter ces commandes.
> - Le client doit disposer d'une application enregistrée pour gérer le protocole. Dans le cas contraire, l'URL est redirigée vers le client et ne se lance pas.

> - Les URL de protocole personnalisé que vous saisissez ou lancez dans les navigateurs Chrome et Edge ne sont pas prises en charge et ne sont pas redirigées.
> - Les protocoles suivants ne sont pas pris en charge : `rtsp://`, `rtspu://`, `pnm://`, `mms://`.

### Autres considérations

- Les exigences et les configurations du navigateur ne s'appliquent qu'au navigateur qui démarre la redirection. Le navigateur de destination, dans lequel l'URL s'ouvre une fois la redirection réussie, n'a pas besoin d'être pris en charge. Lorsque vous redirigez des URL du VDA vers un client, une configuration de navigateur prise en charge est uniquement requise sur le VDA. À l'inverse, lorsque vous redirigez des URL du client vers un VDA, une configuration de navigateur prise en charge est uniquement requise sur le client. Les URL redirigées sont transférées au navigateur par défaut configuré sur la machine de destination, soit le client, soit le VDA, selon la direction. Il n'est pas nécessaire d'utiliser le même type de navigateur sur le VDA et le client.
- Vérifiez que les règles de redirection n'entraînent pas une configuration en boucle. Par exemple, une stratégie VDA est définie pour rediriger `https://www.citrix.com` et la stratégie client est définie pour rediriger la même URL, ce qui entraîne une boucle infinie.
- Les raccourcis d'URL ne sont pas pris en charge.
- La redirection client vers VDA requiert l'installation du client Windows avec des droits d'administrateur.
- Si le navigateur de destination est déjà ouvert, l'URL redirigée s'ouvre dans un nouvel onglet. Sinon, l'URL s'ouvre dans une nouvelle fenêtre de navigateur.
- La redirection bidirectionnelle du contenu ne fonctionne pas lorsque l'accès local aux applications (LAA) est activé.

## Redirection hôte vers client

June 27, 2024

La redirection de l'hôte vers le client permet aux URL intégrées sous forme de liens hypertexte dans des applications exécutées sur une session Citrix, de s'ouvrir à l'aide de l'application correspondante sur la machine de point de terminaison utilisateur. Voici quelques cas d'utilisation courants pour la redirection de l'hôte vers le client :

- Redirection de sites Web dans les cas où le serveur Citrix n'a pas d'accès Internet ou réseau à la source.

- La redirection de sites Web lors de l'exécution d'un navigateur Web dans la session Citrix n'est pas souhaitée pour des raisons de sécurité, de performances, de compatibilité ou de scalabilité.
- Redirection de types d'URL spécifiques dans les cas où les applications requises pour ouvrir l'URL ne sont pas installées sur le serveur Citrix.

La redirection de l'hôte vers le client n'est pas destinée aux URL auxquelles vous accédez sur une page Web ou que vous saisissez dans la barre d'adresse du navigateur Web exécuté dans la session Citrix. Pour la redirection des URL dans les navigateurs Web, consultez Redirection d'URL bidirectionnelle ou Redirection du contenu de navigateur.

### Configuration système requise

- VDA avec OS multi-session
- Clients pris en charge :
  - Application Citrix Workspace pour Windows
  - Application Citrix Workspace pour Mac
  - Application Citrix Workspace pour Linux
  - Application Citrix Workspace pour HTML5
  - Application Citrix Workspace pour Chrome

Une application doit être installée et configurée sur la machine cliente pour gérer la redirection des types d'URL.

### Configuration

Utilisez la stratégie Citrix Redirection hôte vers client pour activer cette fonctionnalité. La **redirection hôte vers client** est désactivée par défaut. Une fois que vous avez activé la stratégie de redirection de l'hôte vers le client, l'application Citrix Launcher s'enregistre auprès du serveur Windows pour s'assurer qu'elle peut intercepter des URL et les envoyer à la machine cliente.

Vous devez ensuite configurer la stratégie de groupe Windows pour utiliser Citrix Launcher comme application par défaut pour les types d'URL requis. Sur le VDA du serveur Citrix, créez le fichier ServerFTAdefaultPolicy.xml et insérez le code XML suivant.

```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />

<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
    "ServerFTA" />
```

```
8
9  </DefaultAssociations>
10 <!--NeedCopy-->
```

Dans la Console de gestion des stratégies de groupe, accédez à **Configuration ordinateur > Modèles d'administration > Composants Windows > Explorateur de fichiers > Définir un fichier de configuration des associations par défaut**, puis enregistrez votre fichier ServerFTAdefaultPolicy.xml.

> **Remarque :**
>
> Si un serveur Citrix ne dispose pas des paramètres de stratégie de groupe, Windows invite les utilisateurs à sélectionner une application pour ouvrir des URL.

Par défaut, nous prenons en charge la redirection des types d'URL suivants :

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

Pour inclure des types d'URL standard ou personnalisés supplémentaires dans la liste de redirection, créez une nouvelle ligne d'**identifiant d'association** (Association Identifier) dans le fichier ServerFTAdefaultPolicy.xml référencé précédemment. Par exemple :

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>

<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>

<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

L'ajout de types d'URL à la liste nécessite également une configuration client. Créez la clé et les valeurs de registre suivantes sur le client Windows.

> **Remarque :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie

> de sauvegarde de votre registre avant de le modifier.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Nom de la valeur : ExtraURLProtocols
- Type de valeur : REG_SZ
- Données de valeur : spécifiez les types d'URL requis séparés par un point-virgule. Incluez tout ce qui se trouve avant la partie autorité de l'URL. Par exemple : `ftp://;mailto:;customtype1:///;custometype2://`

Vous pouvez ajouter des types d'URL uniquement pour les clients Windows. Les clients qui ne disposent pas des paramètres de registre ci-dessus rejettent la redirection vers la session Citrix. Une application doit être installée et configurée chez le client pour gérer les types d'URL spécifiés.

Pour supprimer des types d'URL de la liste de redirection par défaut, créez la clé de registre et les valeurs suivantes sur le VDA du serveur.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nom de la valeur : DisableServerFTA
- Type de valeur : DWORD
- Données de valeur : 1
- Nom de la valeur : NoRedirectClasses
- Type de valeur : REG_MULTI_SZ
- Données de valeur : spécifiez n'importe quelle combinaison de valeurs : `http`, `https`, `rtsp`, `rtspu`, `pnm` ou `mms`. Tapez les valeurs multiples sur des lignes distinctes. Par exemple :

```
http
https
rtsp
```

Pour activer la redirection de l'hôte vers le client pour un ensemble spécifique de sites Web, créez une clé de registre et des valeurs sur le VDA de serveur.

- Clé : HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nom de la valeur : ValidSites
- Type de valeur : REG_MULTI_SZ
- Données de valeur : spécifiez toute combinaison de noms de domaine complet (FQDN). Tapez les noms de domaine complet sur des lignes distinctes. N'incluez que le nom de domaine complet, sans protocoles (`http://` ou `https://`). Un nom de domaine complet peut inclure un astérisque (*) en tant que caractère générique dans la position la plus à gauche uniquement. Ce caractère générique correspond à un seul niveau de domaine, ce qui est compatible avec les règles définies dans RFC 6125. Par exemple :

`www.exmaple.com`

`*.example.com`

> **Remarque :**
>
> Vous ne pouvez pas utiliser la clé **ValidSites** en combinaison avec les clés **DisableServerFTA** et **NoRedirectClasses**.

### Configuration du navigateur par défaut du VDA serveur

L'activation de la redirection de l'hôte vers le client comme indiqué dans cette section remplace toute configuration de navigateur par défaut précédente sur le VDA de serveur. Si une URL Web n'est pas redirigée, Citrix Launcher transmet l'URL au navigateur configuré dans la clé de registre `command_backup`. La clé pointe vers Internet Explorer par défaut, mais vous pouvez la modifier pour inclure le chemin d'accès à un autre navigateur. Pour plus d'informations, reportez-vous à Configuration du navigateur par défaut du VDA serveur dans la liste des fonctionnalités gérées via le Registre.

## Local App Access et redirection d'adresse URL

June 27, 2024

### Introduction

Local App Access s'intègre en toute transparence aux applications Windows installées localement dans un environnement de bureau hébergé sans passer d'un bureau à l'autre. Avec Local App Access, vous pouvez :

- Accédez aux applications installées localement sur un ordinateur portable, un PC ou tout autre périphérique physique directement à partir de votre bureau virtuel.
- Fournir une solution de mise à disposition d'applications flexible. Si les utilisateurs possèdent des applications locales que vous ne pouvez pas virtualiser ou qui ne sont pas gérées par le département informatique, ces applications se comporteront toujours comme si elles étaient installées sur un bureau virtuel.
- Éliminez la latence double-hop lorsque les applications sont hébergées séparément du bureau virtuel. Pour ce faire, placez le raccourci vers l'application publiée sur la machine Windows de l'utilisateur.
- Utiliser des applications telles que :

  - Logiciels de conférence vidéo tels que GoToMeeting.
  - Applications de niche ou spécialisées qui ne sont pas encore virtualisées.
  - Applications et périphériques qui transfèrent des quantités très importantes de données depuis une machine utilisateur vers un serveur et à nouveau vers la machine utilisateur, comme par exemple, les graveurs de DVD et les tuners TV.

Dans Citrix Virtual Apps and Desktops, les sessions de bureau hébergées utilisent la redirection d'URL pour démarrer les applications Local Access App. La redirection d'URL met l'application à disposition sous plusieurs adresses URL. Elle lance un navigateur local (en fonction de la liste de blocage d'adresses URL de votre navigateur) en cliquant sur des liens intégrés dans un navigateur dans une session de bureau. Si vous accédez à une URL qui n'est pas présente dans la liste de blocage, l'adresse URL est ouverte dans la session de bureau.

La redirection d'adresse URL ne fonctionne que pour les sessions de bureau, pas les sessions d'application. La seule fonctionnalité de redirection que vous pouvez utiliser pour des sessions d'application est la redirection de contenu hôte vers client, qui est un type de redirection de FTA (Association de type de fichier) serveur. Cette FTA redirige certains protocoles vers le client, tels que HTTP, HTTPS, RTSP ou MMS. Par exemple, si vous voulez ouvrir uniquement des liens avec HTTP, les liens s'ouvrent directement avec l'application cliente. Il n'y a pas de liste de blocage ou d'autorisation d'URL.

Lorsque Local App Access est activé pour les bureaux hébergés, les adresses URL qui sont affichées pour les utilisateurs en tant que liens depuis des applications exécutées localement, depuis les applications hébergées par l'utilisateur ou en tant que raccourcis sur le bureau sont redirigées de l'une des manières suivantes :

- À partir de l'ordinateur de l'utilisateur vers le bureau hébergé
- À partir du serveur Citrix Virtual Apps and Desktops vers l'ordinateur de l'utilisateur
- Restitué dans l'environnement dans lequel ils sont démarrés (et non pas redirigés)

Pour spécifier le chemin d'accès de redirection du contenu de sites Web spécifiques, configurez la liste d'autorisation et la liste de blocage d'adresses URL sur Virtual Delivery Agent. Ces listes contiennent des clés de Registre de chaînes multiples qui spécifient les paramètres de stratégie de redirection d'URL. Pour de plus amples informations, consultez la section Paramètres de stratégie Local App Access.

Les adresses URL peuvent être restituées sur le VDA avec les exceptions suivantes :

- Informations géographiques et relatives aux paramètres régionaux : sites Web qui requièrent des informations sur les paramètres régionaux, telles que msn.com ou news.google.com (ouvre une page spécifique au pays en fonction de l'emplacement géographique). À titre d'exemple, si le VDA est provisionné à partir d'un centre de données situé au Royaume-Uni et que le client se connecte depuis l'Inde, l'utilisateur s'attend à voir in.msn.com. Au lieu de cela, l'utilisateur voit uk.msn.com.

- Contenu multimédia : les sites Web contenant du contenu multimédia riche, lorsqu'ils sont restitués sur la machine cliente, offrent aux utilisateurs une expérience native et permettent d'économiser la bande passante même dans les réseaux à latence élevée. Cette fonctionnalité redirige les sites avec d'autres types de contenu multimédia tels que Silverlight. Ce processus est dans un environnement sécurisé. En effet, les URL qui sont approuvées par l'administrateur sont exécutées sur la machine cliente tandis que le reste des URL sont redirigées vers le VDA.

En plus de la redirection d'URL, vous pouvez également utiliser la redirection FTA. L'association de types de fichier démarre des applications locales lorsqu'un fichier est détecté dans la session. Si l'application locale est démarrée, elle doit avoir accès au fichier pour l'ouvrir. Par conséquent, vous pouvez uniquement ouvrir des fichiers qui résident sur des partages réseau ou sur des lecteurs clients (avec CDM) à l'aide d'applications locales. Par exemple, lors de l'ouverture d'un fichier PDF, si un lecteur PDF est une application locale, le fichier s'ouvre à l'aide de ce lecteur PDF. Étant donné que l'application locale peut accéder au fichier directement, il n'y a pas de transfert réseau du fichier via ICA pour ouvrir ce dernier.

### Configuration requise, considérations et limitations à prendre en compte

Local App Access est pris en charge sur des systèmes d'exploitation valides pour les VDA pour OS multi-session Windows et VDA pour OS mono-session Windows. Local App Access nécessite l'application Citrix Workspace pour Windows version 4.1 (minimum). Les navigateurs Web pris en charge sont les suivants :

- Edge, dernière version
- Firefox, dernière version et version de prise en charge étendue
- Chrome, dernière version

Vérifiez les informations et les limitations suivantes lors de l'utilisation de Local App Access et de la redirection d'adresse URL.

- Local App Access est uniquement conçu pour les bureaux virtuels en mode plein écran couvrant tous les moniteurs comme suit :
  - L'expérience utilisateur pourrait prêter à confusion si vous utilisez Local App Access avec un bureau virtuel qui s'exécute en mode fenêtre ou ne couvre pas tous les moniteurs.
  - Plusieurs moniteurs : si un moniteur est agrandi, il devient le bureau par défaut pour toutes les applications démarrées dans cette session. Ce comportement par défaut se produit même si les applications suivantes sont démarrées généralement sur l'autre moniteur.
  - La fonctionnalité prend en charge un seul VDA. Il n'y a pas d'intégration avec plusieurs VDA simultanés.

- Certaines applications peuvent se comporter de manière inattendue et affecter les utilisateurs :
  - Les utilisateurs risquent d'être déroutés par les lettres de lecteur, telles que C: local plutôt que le lecteur C: du bureau virtuel.
  - Les imprimantes disponibles dans le bureau virtuel ne sont pas disponibles pour les applications locales.
  - Les applications qui nécessitent des autorisations élevées ne peuvent pas être démarrées en tant qu'applications hébergées sur le client.
  - Aucun traitement spécial pour les applications à instance unique (telles que le Lecteur Windows Media).
  - Les applications locales s'affichent avec le thème Windows de la machine locale.
  - Les applications en plein écran ne sont pas prises en charge. Ces applications incluent les applications qui s'ouvrent en plein écran, telles que des diaporamas PowerPoint, ou les visionneuses de photos couvrant la totalité du bureau.
  - Local App Access copie les propriétés de l'application locale (telles que les raccourcis sur le bureau et le menu Démarrer du client) sur le VDA. Cependant, il ne copie pas les autres propriétés, telles que les touches de raccourci et les attributs en lecture seule.
  - Les applications qui permettent de personnaliser la manière dont est géré le chevauchement des fenêtres peuvent avoir des résultats imprévisibles. Par exemple, certaines fenêtres peuvent être masquées.
  - Les raccourcis ne sont pas pris en charge, y compris Ordinateur, Corbeille, Panneau de configuration, les raccourcis du lecteur réseau et les raccourcis de dossiers.
  - Les types de fichiers et fichiers suivants ne sont pas pris en charge : types de fichiers personnalisés, fichiers sans programmes associés, fichiers zippés et fichiers masqués.
  - Le regroupement de la barre des tâches n'est pas pris en charge pour les applications mixtes 32 bits et 64 bits hébergées sur le client ou le VDA, telles que le regroupement d'applications locales 32 bits avec des applications VDA 64 bits.
  - Les applications ne peuvent pas être démarrées en utilisant COM. Par exemple, si vous cliquez sur un document Office incorporé à une application Office, le démarrage du processus ne peut pas être détecté et l'intégration de l'application locale échoue.
- Les scénarios double-hop, dans lesquels un utilisateur démarre un bureau virtuel à partir d'une autre session de bureau virtuel, ne sont pas pris en charge.
- La redirection d'URL prend uniquement en charge les adresses URL explicites (c'est-à-dire, celles qui apparaissant dans la barre d'adresse du navigateur ou celles détectées à l'aide de la barre de navigation du navigateur, selon le navigateur spécifique).
- La redirection d'adresses URL fonctionne uniquement avec les sessions de bureau, et non pas avec les sessions d'application.
- Le dossier du bureau local dans une session VDA n'autorise pas les utilisateurs à créer de fichiers.

- Plusieurs instances d'une application exécutée localement se comportent conformément aux paramètres de barre des tâches établis pour le bureau virtuel. Les raccourcis vers des applications exécutées localement ne sont pas regroupés avec les instances en cours d'exécution de ces applications. Ils sont également non groupés avec les instances en cours d'exécution des applications hébergées ou les raccourcis épinglés pour les applications hébergées. Les utilisateurs ne peuvent fermer les fenêtres des applications exécutées localement qu'à partir de la barre des tâches. Bien que les utilisateurs puissent épingler les fenêtres d'applications locales à la barre des tâches et au menu Démarrer, les applications risquent de ne pas fonctionner de manière cohérente lors de l'utilisation de ces raccourcis.
- Si vous définissez le paramètre de stratégie **Autoriser Local App Access** sur **Activé**, la redirection de contenu du navigateur n'est pas prise en charge. Par défaut, l'accès à l'application locale est interdit.

### Interaction avec Windows

L'interaction de Local App Access avec Windows comprend les comportements suivants.

- Comportement des raccourcis de Windows 8 et Windows Server 2012
  - Les applications Windows Store installées sur le client ne sont pas énumérées comme faisant partie des raccourcis Local App Access.
  - Les fichiers image et vidéo sont ouverts par défaut à l'aide des applications du Windows Store. Toutefois, Local App Access énumère les applications du Windows Store et ouvre les raccourcis avec les applications du bureau.
- Programmes locaux
  - Pour Windows 7, le dossier est disponible dans le menu Démarrer.
  - Pour Windows 8, Programmes locaux est disponible uniquement lorsque l'utilisateur choisit **Toutes les applications** comme catégorie dans l'écran de démarrage. Les sous-dossiers ne sont pas tous affichés dans Programmes locaux.
- Fonctionnalités graphiques Windows 8 pour les applications
  - Les applications de bureau sont limitées à la zone de bureau et sont couvertes par l'écran d'accueil et les applications de style Windows 8.
  - Les applications Local App Access ne se comportent pas comme des applications de bureau en mode multi-écrans. En mode multi-écrans, l'écran d'accueil et le bureau s'affichent sur des moniteurs différents.
- Windows 8 et la redirection d'URL Local App Access
  - Étant donné que Windows 8 n'a aucun module complémentaire Internet Explorer activé, utilisez Internet Explorer sur le bureau pour activer la redirection d'adresse URL.

- Dans Windows Server 2012, Internet Explorer désactive les modules complémentaires par défaut. Pour implémenter la redirection d'adresse URL, désactivez la configuration renforcée d'Internet Explorer. Réinitialisez ensuite les options d'Internet Explorer et redémarrez pour vous assurer que les modules complémentaires sont activés pour les utilisateurs standards.

## Configurer Local App Access et la redirection d'adresse URL

Pour utiliser Local App Access et la redirection d'adresse URL à l'aide de l'application Citrix Workspace :

- Installez l'application Citrix Workspace sur la machine cliente locale. Vous pouvez activer les fonctionnalités lors de l'installation de l'application Citrix Workspace ou vous pouvez activer le modèle Local App Access à l'aide de l'éditeur de stratégie de groupe.
- Définissez le paramètre de stratégie **Autoriser Local App Access** sur **Activé**. Vous pouvez également configurer les paramètres de stratégie de la liste d'autorisation et la liste de blocage d'adresses URL pour la redirection d'adresses URL. Pour de plus amples informations, consultez la section Paramètres de stratégie Local App Access.

### Activer Local App Access et la redirection d'adresse URL

Pour activer Local App Access pour toutes les applications locales, procédez comme suit :

1. Connectez-vous à Web Studio et cliquez sur **Stratégies** dans le volet de gauche.
2. Dans la barre d'actions, cliquez sur **Créer une stratégie**.
3. Dans la fenêtre Créer une stratégie, tapez « Autoriser Local App Access » dans la zone de recherche, puis cliquez sur **Sélectionner**.
4. Dans la fenêtre Modifier le paramètre, sélectionnez **Autorisé**. Par défaut, la stratégie **Autoriser Local App Access** est interdite. Lorsque ce paramètre est autorisé, le VDA permet à l'utilisateur de décider si les applications publiées et les raccourcis Local App Access sont activés dans la session. (Lorsque ce paramètre est interdit, les applications publiées et les raccourcis Local App Access ne fonctionnent pas pour le VDA.) Ce paramètre de stratégie, ainsi que la stratégie de redirection d'URL, s'appliquent à la totalité de la machine.
5. Dans la fenêtre Créer une stratégie, tapez « Liste d'autorisation de redirection d'adresse URL » dans la zone de recherche, puis cliquez sur **Sélectionner**. La liste d'autorisation de redirection d'adresse URL spécifie les adresses URL à ouvrir dans le navigateur par défaut de la session distante.
6. Dans la fenêtre Modifier les paramètres, cliquez sur **Ajouter** pour ajouter les adresses URL, puis cliquez sur **OK**.

7. Dans la fenêtre Créer une stratégie, tapez « Liste de blocage de redirection d'adresse URL » dans la zone de recherche, puis cliquez sur **Sélectionner**. La liste de blocage de redirection d'adresse URL spécifie les adresses URL redirigées vers le navigateur par défaut s'exécutant sur le point de terminaison.
8. Dans la fenêtre Modifier les paramètres, cliquez sur **Ajouter** pour ajouter les adresses URL, puis cliquez sur **OK**.
9. Sur la page Paramètres, cliquez sur **Suivant**.
10. Sur la page Utilisateurs et machines, attribuez la stratégie aux groupes de mise à disposition applicables, puis cliquez sur **Suivant**.
11. Dans la page Résumé, vérifiez les paramètres et cliquez sur **Terminer**.

Pour activer la redirection d'adresse URL pour toutes les applications locales lors de l'installation de l'application Citrix Workspace, procédez comme suit :

1. Activez la redirection d'adresses URL lors de l'installation de l'application Citrix Workspace pour tous les utilisateurs d'une machine. Cette action enregistre également les modules complémentaires du navigateur requis pour la redirection d'adresses URL.
2. À partir de l'invite de commandes, exécutez la commande appropriée pour installer l'application Citrix Workspace avec l'une des options suivantes :
   - Pour CitrixReceiver.exe, utilisez `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
   - Pour CitrixReceiverWeb.exe, utilisez `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

#### Pour activer le modèle Local App Access à l'aide de l'éditeur de stratégie de groupe

> **Remarque :**
>
> - Avant d'activer le modèle Local App Access à l'aide de l'éditeur de stratégie de groupe, ajoutez les fichiers de modèle receiver.admx/adml à l'objet de stratégie de groupe local.
> - Les fichiers de modèle de l'application Citrix Workspace pour Windows sont disponibles sur l'objet de stratégie de groupe local dans le dossier **Modèles d'administration > Composants Citrix > Citrix Workspace** uniquement lorsque le fichier CitrixBase.admx/CitrixBase.adml est ajouté au dossier %systemroot%\policyDefinitions.

Pour activer le modèle Local App Access à l'aide de l'éditeur de stratégie de groupe, procédez comme suit :

1. Exécutez **gpedit.msc**.
2. Accédez à **Configuration ordinateur > Modèles d'administration > Modèles d'administration classiques (ADM) > Composants Citrix > Citrix Workspace > Expérience utilisateur**.
3. Cliquez sur **Paramètres Local App Access**.

4. Sélectionnez **Activé** puis sélectionnez **Autoriser la redirection d'URL**. Pour la redirection d'URL, enregistrez les modules complémentaires du navigateur à l'aide de la ligne de commande décrite dans la section *Enregistrer les modules complémentaires du navigateur* plus loin dans cet article.

#### Fournir uniquement l'accès aux applications publiées

Vous pouvez donner accès aux applications publiées à l'aide de l'Éditeur du Registre ou du Kit de développement logiciel (SDK) PowerShell.

Pour accéder à l'Éditeur du Registre, consultez La section Local App Access pour les applications publiées dans la liste des fonctionnalités gérées via le registre.

Pour utiliser le SDK PowerShell :

1. Ouvrez PowerShell sur la machine sur laquelle le Delivery Controller est en cours d'exécution.
2. Entrez la commande suivante : `set-configsitemetadata -name "studio_clientHostedApps"-value "true"`.

Pour accéder à **Ajouter l'application Local App Access** dans un déploiement de service de cloud, utilisez le kit SDK PowerShell à distance Citrix DaaS. Pour plus d'informations, consultez kit SDK PowerShell à distance Citrix DaaS.

1. Téléchargez le programme d'installation :

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. Exécutez ces commandes :

   a) `asnp citrix.*`
   b) `Get-XdAuthentication`

3. Entrez la commande suivante : `set-configsitemetadata -name "studio_clientHostedApps"-value "true"`.

Après avoir terminé les étapes précédentes applicables, procédez comme suit pour continuer.

1. Connectez-vous à Web Studio et sélectionnez **Applications** dans le volet de gauche.
2. Dans le volet central supérieur, cliquez avec le bouton droit de la souris sur la zone vide et sélectionnez **Ajouter l'application Local App Access** dans le menu contextuel. Vous pouvez également cliquer sur **Ajouter l'application Local App Access** dans la barre d'actions. Pour afficher l'option Ajouter l'application Local App Access dans la barre d'actions, cliquez sur **Actualiser**.
3. Publiez l'application Local App Access.

- L'assistant Local Application Access s'ouvre avec une page Introduction, que vous pouvez supprimer des lancements ultérieurs de l'assistant.
- L'assistant vous guide à travers les pages Groupes, Emplacement, Identification, Mise à disposition et Résumé décrites ci-dessous. Lorsque vous avez terminé chaque page, cliquez sur **Suivant** jusqu'à la page Résumé.
- Dans la page Groupes, sélectionnez un ou plusieurs groupes de mise à disposition dans lesquels les nouvelles applications seront ajoutées, puis cliquez sur **Suivant**.
- Sur la page Emplacement, tapez le chemin d'exécution complet de l'application sur la machine locale de l'utilisateur et tapez le chemin d'accès au dossier dans lequel se trouve l'application. Citrix recommande d'utiliser le chemin de variable de l'environnement système ; par exemple, %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.
- Sur la page Identification, acceptez les valeurs par défaut ou tapez les informations souhaitées, puis cliquez sur **Suivant**.
- Sur la page Mise à disposition, configurez comment cette application est mise à disposition des utilisateurs, puis cliquez sur **Suivant**. Vous pouvez spécifier l'icône de l'application sélectionnée. Vous pouvez également spécifier si le raccourci vers l'application locale sur le bureau virtuel est visible dans le menu Démarrer, le bureau ou les deux.
- Dans la page Résumé, vérifiez les paramètres et cliquez sur **Terminer** pour quitter l'assistant Local Application Access.

#### Enregistrer les modules complémentaires du navigateur

> **Remarque :**
>
> Les modules complémentaires du navigateur requis pour la redirection d'adresse URL ne sont pas enregistrés automatiquement lorsque vous installez application Citrix Workspace à partir de la ligne de commande avec l'option /ALLOW_CLIENTHOSTEDAPPSURL=1.

Vous pouvez utiliser les commandes suivantes pour enregistrer et annuler l'enregistrement d'un ou de plusieurs modules complémentaires :

- Pour enregistrer les composants sur une machine cliente : <*dossier-installation-client*>\redirector.exe /reg<*navigateur*>.
- Pour annuler l'enregistrement des composants sur une machine cliente : <*dossier-installation-client*>\redirector.exe /unreg<*navigateur*>.
- Pour enregistrer les composants sur un VDA :<*dossier-VDAinstallation*> \VDARedirector.exe /reg<*navigateur*>
- Pour annuler l'enregistrement des composants sur un VDA :<*dossier-VDAinstallation*> \VDARedirector.exe /unreg<*navigateur*>

Où <*navigateur*> est Internet Explorer, Firefox, Chrome ou Tous.

Par exemple, la commande suivante enregistre les composants Internet Explorer sur une machine exécutant l'application Citrix Workspace.

C:\Program Files\Citrix\ICA Client\redirector.exe/regIE

La commande suivante enregistre tous les composants d'un VDA avec OS multi-session Windows.

C:\Program Files (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

#### Interception d'adresses URL dans les navigateurs

- Par défaut, Internet Explorer redirige l'adresse URL spécifiée. Si l'adresse URL ne figure pas dans la liste de blocage mais est redirigée vers une autre adresse URL par le navigateur ou un site Web, l'adresse URL finale n'est pas redirigée. Elle n'est pas redirigée même si elle est sur la liste de blocage.

Pour que la redirection d'adresse URL fonctionne correctement, activez le module complémentaire lorsque vous y êtes invité par le navigateur. Si les modules complémentaires utilisant les options Internet ou les modules complémentaires dans l'invite de commande sont désactivés, la redirection d'adresse URL ne fonctionne pas correctement.

- Les modules complémentaires Firefox redirigent toujours les adresses URL.

Lorsqu'un module complémentaire est installé, Firefox vous invite à autoriser/empêcher l'installation du module complémentaire dans un nouvel onglet. Autorisez le module complémentaire pour que la fonctionnalité fonctionne.

- Le module complémentaire Chrome redirige toujours l'adresse URL finale qui est ouverte et non pas les adresses URL saisies.

Les extensions ont été installées en externe. Si vous désactivez l'extension, la fonctionnalité de redirection d'adresse URL ne fonctionne pas dans Chrome. Si la redirection d'adresse URL est requise en mode Incognito, autorisez l'exécution de l'extension dans ce mode dans la page de paramètres du navigateur.

#### Configurer le comportement de l'application locale lors de la fermeture de session et de la déconnexion

> **Remarque :**
>
> Si vous ne suivez pas ces étapes pour configurer les paramètres, par défaut, les applications locales continuent à s'exécuter lorsqu'un utilisateur ferme sa session ou se déconnecte du bureau virtuel. Après la reconnexion, les applications locales sont réintégrées si elles sont disponibles

> dans le bureau virtuel.

Pour configurer le comportement de l'application locale lors de la fermeture de session et de la déconnexion, reportez-vous à Comportement de l'application locale lors de la fermeture de session et de la déconnexion dans la liste des fonctionnalités gérées via le Registre.

## Considérations de redirection USB générique et de lecteur client

June 27, 2024

La technologie HDX offre une **prise en charge optimisée** pour la plupart des périphériques USB populaires, La prise en charge optimisée offre une meilleure expérience utilisateur avec de meilleures performances et une bande passante plus efficace via un réseau étendu. La prise en charge optimisée est généralement la meilleure option, notamment dans les environnements à latence élevée ou avec des exigences de sécurité strictes.

La technologie HDX offre la **redirection USB générique** pour les périphériques spécialisés dont la prise en charge n'est pas optimisée ou n'est pas adaptée, par exemple :

- Le périphérique USB est doté d'autres fonctionnalités avancées ne faisant pas partie de la prise en charge optimisée, telles qu'une souris ou une webcam avec des boutons supplémentaires.
- Les utilisateurs ont besoin de fonctionnalités qui ne font pas partie de la prise en charge optimisée.
- Le périphérique USB est un périphérique spécialisé, tel qu'un équipement de test et de mesure ou un contrôleur industriel.
- Une application requiert un accès direct au périphérique USB.
- Un seul pilote Windows est disponible pour le périphérique USB. Par exemple, un lecteur de carte à puce peut ne pas avoir de pilote pour l'application Citrix Workspace pour Android.
- La version de l'application Citrix Workspace n'offre pas de prise en charge optimisée pour ce type de périphérique USB.

Avec la redirection USB générique :

- Il n'est pas nécessaire pour les utilisateurs d'installer des pilotes de périphériques sur la machine utilisateur.
- Les pilotes clients USB sont installés sur la machine VDA.

> **Important :**
>
> - La redirection USB générique peut être utilisée conjointement avec la prise en charge optimisée. Si vous activez la redirection USB générique, configurez les paramètres de stratégie

> des périphériques USB Citrix pour la redirection USB générique et la prise en charge optimisée.
> - Le paramètre de stratégie Citrix Règles d'optimisation de périphérique USB client est un paramètre spécifique pour la redirection USB générique, pour un périphérique USB spécifique. Il ne s'applique pas à la prise en charge optimisée comme indiqué ici.

### Considérations sur les performances pour les périphériques USB

Lors de l'utilisation de la redirection USB générique avec certains types de périphériques USB, la latence et la bande passante réseau peuvent affecter l'expérience utilisateur et le fonctionnement du périphérique USB. Par exemple, les périphériques soumis à des contraintes de temps risquent de ne pas fonctionner correctement avec des liens à faible bande passante et latence élevée. Utilisez la prise en charge optimisée autant que possible.

Certains périphériques USB requièrent une bande passante élevée pour être utilisables, par exemple une souris 3D (utilisée avec des applications 3D qui requièrent également une bande passante élevée en général). Si la bande passante ne peut pas être augmentée, vous pouvez peut-être limiter le problème en optimisant l'utilisation de la bande passante des autres composants à l'aide des paramètres de stratégie de bande passante. Pour de plus amples informations, consultez la section Paramètres de stratégie de bande passante pour la redirection de périphérique USB client et Paramètres de stratégie Connexions Multi-Stream.

### Considérations sur la sécurité pour les périphériques USB

Certains périphériques USB sont sécurisés par nature, par exemple, les lecteurs de carte à puce, les lecteurs d'empreintes digitales et les dispositifs de signature numérique. D'autres périphériques USB tels que les périphériques de stockage USB peuvent être utilisés pour transmettre des données qui peuvent être confidentielles.

Les périphériques USB sont souvent utilisés pour distribuer des logiciels malveillants. La configuration de l'application Citrix Workspace et de Citrix Virtual Apps and Desktops peut réduire, mais pas éliminer, le risque lié à ces périphériques USB, que vous utilisiez la redirection USB générique ou la prise en charge optimisée.

> **Important :**
>
> Pour les périphériques et les données sensibles, sécurisez toujours la connexion HDX à l'aide de TLS ou d'IPsec.
>
> Activez uniquement la prise en charge pour les périphériques USB dont vous avez besoin. Configurez à la fois la redirection USB générique et la prise en charge optimisée pour répondre à ce besoin.

> Fournir des conseils aux utilisateurs pour une utilisation sûre des périphériques USB :
>
> - Utiliser uniquement des périphériques USB provenant d'une source fiable.
> - Ne pas laisser les périphériques USB sans surveillance dans des environnements ouverts - par exemple, un lecteur flash dans un cybercafé.
> - Expliquer les risques liés à l'utilisation d'un périphérique USB sur plusieurs ordinateurs.

### Compatibilité avec la redirection USB générique

La redirection USB générique est prise en charge pour les périphériques USB 2.0 et versions antérieures. La redirection USB générique est également prise en charge pour les périphériques USB 3.0 connectés à un port USB 2.0 ou USB 3.0. La redirection USB générique ne prend pas en charge les fonctionnalités USB introduites dans USB 3.0, telles que la vitesse.

Ces applications Citrix Workspace prennent en charge la redirection USB générique :

- Application Citrix Workspace pour Windows, consultez la section Configuration de la mise à disposition d'applications
- Application Citrix Workspace pour Mac, consultez la section Application Citrix Workspace pour Mac
- Application Citrix Workspace pour Linux, consultez la section Optimiser
- Application Citrix Workspace pour Chrome OS, consultez la section Application Citrix Workspace pour Chrome

Pour les versions de l'application Citrix Workspace, reportez-vous au tableau des fonctionnalités de l'application Citrix Workspace.

Si vous utilisez des versions antérieures de l'application Citrix Workspace, reportez-vous à la documentation relative à l'application Citrix Workspace afin de vérifier que la redirection USB générique est prise en charge. Reportez-vous à la documentation de l'application Citrix Workspace pour connaître les restrictions sur les types de périphériques USB qui sont pris en charge.

La redirection USB générique est prise en charge pour les sessions de bureau à compter de VDA pour OS mono-session version 7.6 jusqu'à la version actuelle.

La redirection USB générique est prise en charge pour les sessions de bureau à compter de VDA pour OS multi-session version 7.6 jusqu'à la version actuelle, avec les restrictions suivantes :

- Le VDA doit exécuter Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 ou Windows Server 2022.
- Les pilotes de périphérique USB doivent être entièrement compatibles avec Remote Desktop Session Host (RDSH) pour l'OS de VDA (Windows 2012 R2), y compris la prise en charge complète de la virtualisation.

Certains types de périphériques USB ne sont pas pris en charge pour la redirection USB générique, car il n'est pas nécessaire de les rediriger :

- Modems USB.
- Cartes réseau USB.
- Concentrateurs USB. Les périphériques USB connectés à des concentrateurs USB sont gérés individuellement.
- Ports COM virtuels USB. Utilisez la redirection du port COM, plutôt que la redirection USB générique.

Pour de plus amples informations sur les périphériques USB qui ont été testés avec la redirection USB générique, veuillez consulter l'article Citrix Ready Marketplace.. Certains périphériques USB ne fonctionnent pas correctement avec la redirection USB générique.

### Configurer la redirection USB générique

Vous pouvez contrôler, et configurer séparément, les types de périphériques USB qui utilisent la redirection USB générique :

- Sur le VDA, à l'aide des paramètres de stratégie Citrix. Pour de plus amples informations, consultez la section Redirection des lecteurs clients et de machines utilisateur et Paramètres de stratégie Périphériques USB dans la section Référence des paramètres de stratégie
- Dans l'application Citrix Workspace, à l'aide de mécanismes liés à l'application Citrix Workspace. À titre d'exemple, un modèle d'administration peut contrôler les paramètres de registre qui configurent l'application Citrix Workspace pour Windows. Par défaut, la redirection USB est autorisée pour certaines classes de périphériques USB et refusée pour d'autres. Pour plus d'informations, consultez la section Configurer dans la documentation de l'application Citrix Workspace pour Windows.

Cette configuration séparée fournit une plus grande flexibilité. Par exemple :

- Si deux organisations ou services distincts sont responsables de l'application Citrix Workspace et du VDA, elles peuvent appliquer le contrôle séparément. Cette configuration s'applique lorsqu'un utilisateur d'une organisation accède à une application située dans une autre organisation.
- Les paramètres de stratégie Citrix peuvent contrôler les périphériques USB qui sont autorisés pour certains utilisateurs ou pour les utilisateurs se connectant uniquement via un réseau local (plutôt qu'avec Citrix Gateway).

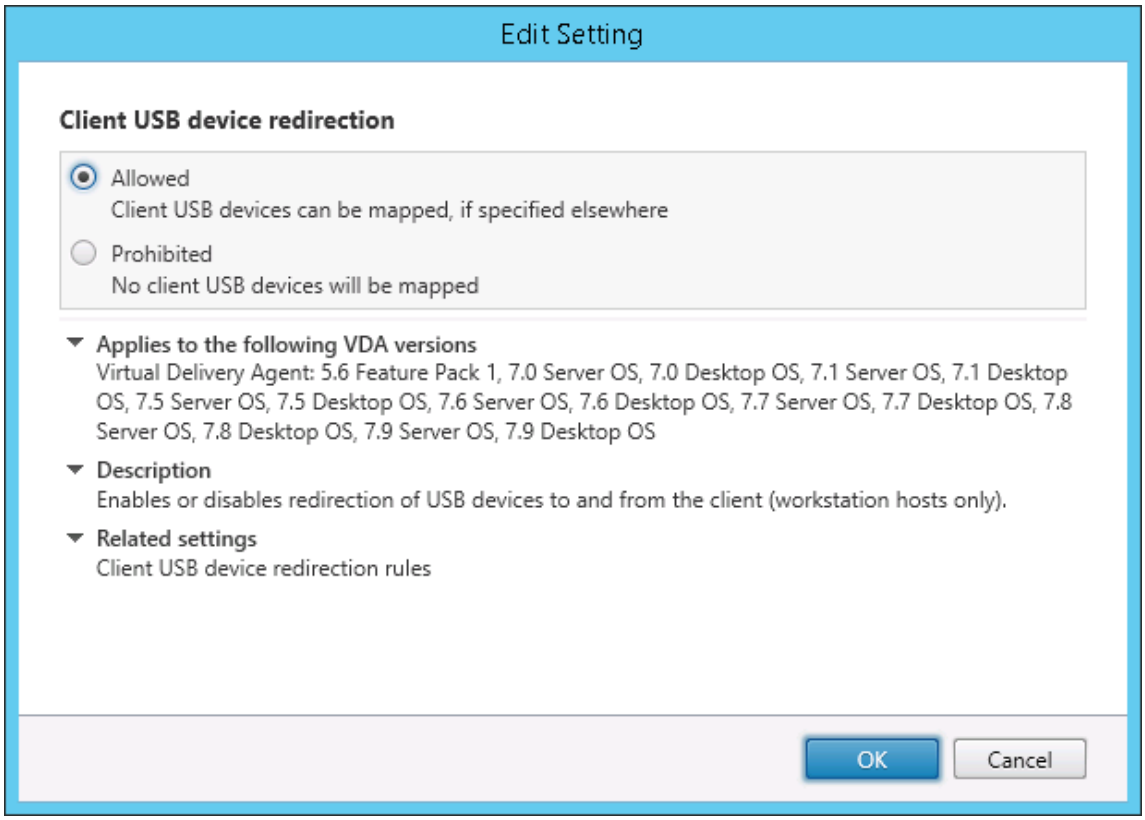
 

### Activer la redirection USB générique

Pour activer la redirection USB générique et ne pas nécessiter de redirection manuelle par l'utilisateur, configurez les paramètres de stratégie Citrix et les préférences de connexion de l'application Citrix Workspace.

Dans les paramètres de stratégie Citrix :

1. Ajoutez Redirection de périphérique USB client à une stratégie et définissez sa valeur sur **Autorisé**.

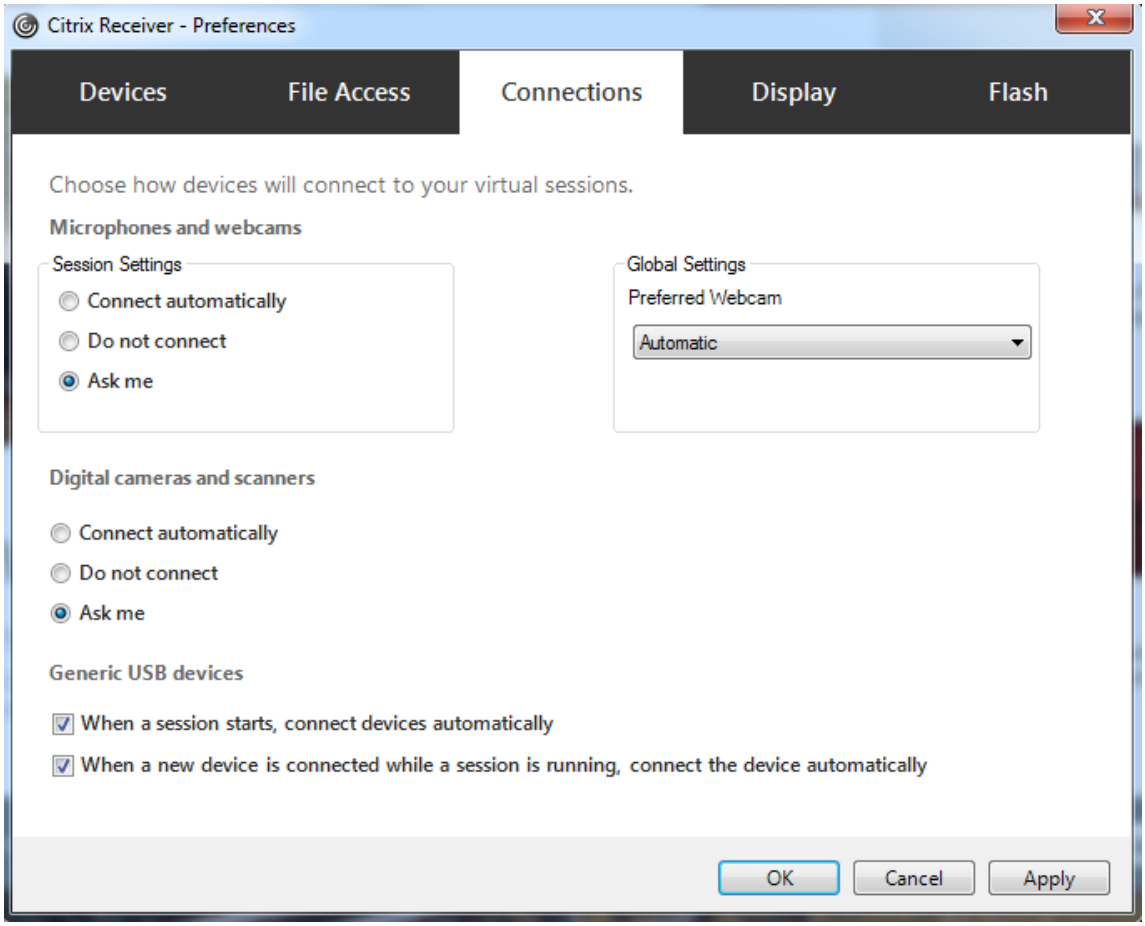



2. (Facultatif). Pour mettre à jour la liste des périphériques USB disponibles pour la redirection, ajoutez le paramètre Règles de redirection de périphérique USB client à une stratégie et spécifiez les règles de stratégie USB.

   Une fois les paramètres de stratégie définis, dans l'application Citrix Workspace :

3. Spécifiez que les périphériques sont connectés automatiquement sans redirection manuelle. Vous pouvez effectuer cette opération à l'aide d'un modèle d'administration ou dans Application Citrix Workspace pour **Windows > Préférences > Connexions**.




Si vous avez spécifié des règles de stratégie USB pour le VDA à l'étape précédente, spécifiez les mêmes règles de stratégie pour l'application Citrix Workspace.

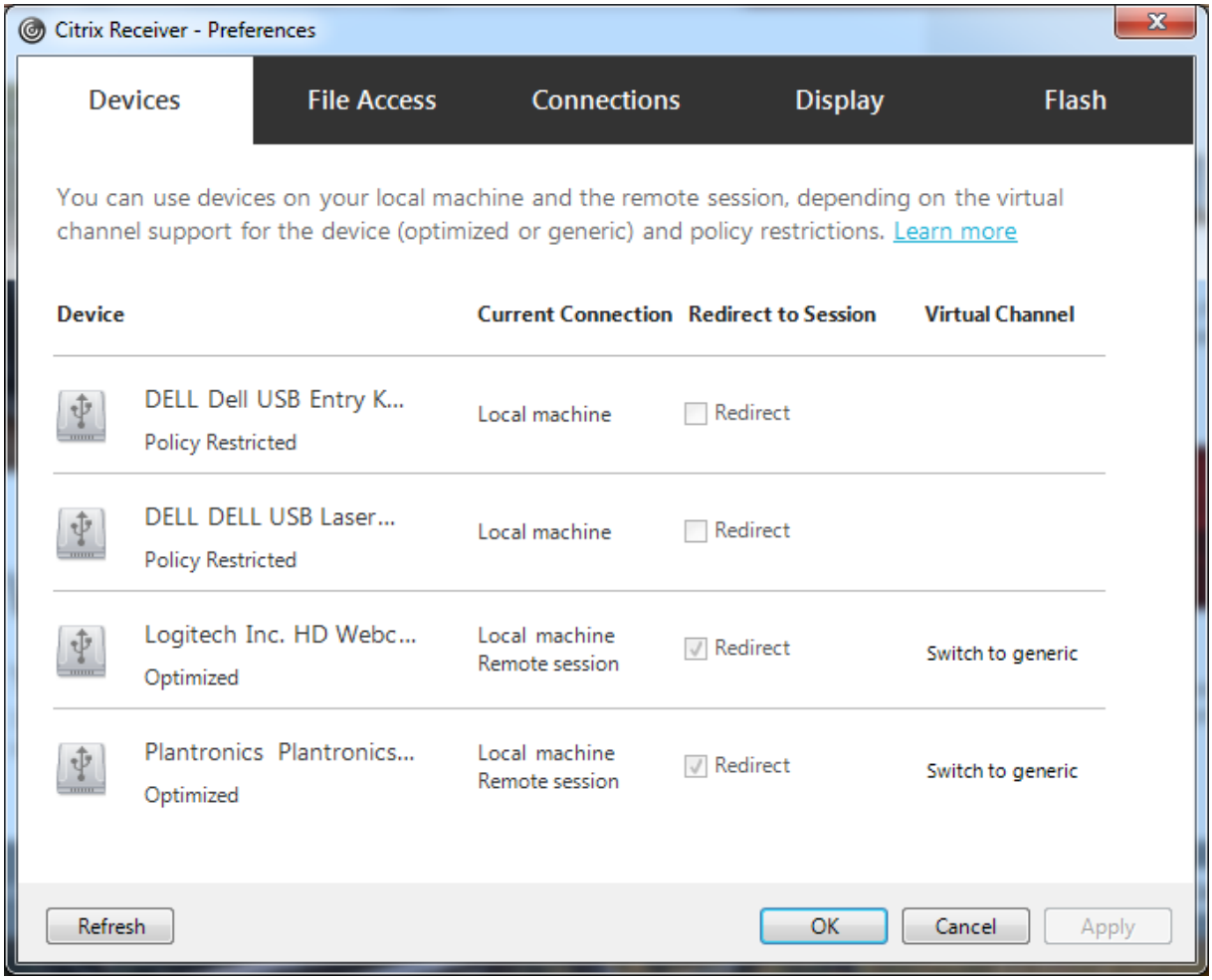
pour les clients légers, consultez le fabricant pour obtenir des détails sur la prise en charge USB et sur la configuration requise.

### Configuration des types de périphériques USB disponibles pour la redirection USB générique

Les périphériques USB sont automatiquement redirigés lorsque la prise en charge USB est activée et que les paramètres de préférences de l'utilisateur USB sont définis pour la connexion automatique aux périphériques USB. Les périphériques USB sont également automatiquement redirigés lorsque la barre de connexion est absente.

Les utilisateurs peuvent rediriger explicitement les périphériques qui ne sont pas automatiquement redirigés en les sélectionnant dans la liste des périphériques USB. Pour plus d'informations, consultez l'article de l'application Citrix Workspace pour Windows, Afficher vos périphériques dans Desktop Viewer.




Pour utiliser la redirection USB générique plutôt que la prise en charge optimisée, vous pouvez :

- Dans l'application Citrix Workspace, sélectionnez manuellement le périphérique USB qui devra utiliser la redirection USB générique et choisissez **Basculer en mode générique** dans l'onglet Périphériques de la boîte de dialogue Préférences.
- Sélectionnez automatiquement le périphérique USB qui devra utiliser la redirection USB générique en configurant la redirection automatique pour le type de périphérique USB (par exemple, AutoRedirectStorage=1), et définissez les paramètres de préférences de l'utilisateur sur la connexion automatique aux périphériques USB. Pour de plus amples informations, consultez la section Configurer la redirection automatique des périphériques USB sur le site de support de Citrix.

> **Remarque :**
>
> Configurez la redirection USB générique pour une utilisation avec une webcam uniquement si la webcam n'est pas compatible avec la redirection multimédia HDX.

Pour empêcher les périphériques USB d'être répertoriés ou redirigés, vous pouvez spécifier des règles

de périphérique pour l'application Citrix Workspace et le VDA.

Pour la redirection USB générique, vous devez connaître au moins la classe et la sous-classe du périphérique USB. Tous les périphériques USB n'utilisent pas nécessairement une classe et une sous-classe de périphérique USB logiques. Par exemple :

- Les stylets utilisent la classe de périphérique de la souris.
- Les lecteurs de carte à puce peuvent utiliser la classe de périphérique définie par le fournisseur ou HID.

Pour un contrôle plus précis, vous avez également besoin de connaître l'ID du fournisseur, l'ID du produit et l'ID de version. Vous pouvez obtenir ces informations auprès du fabricant du périphérique.

> **Important :**
>
> Les périphériques USB malveillants peuvent présenter des caractéristiques de périphérique USB qui ne correspondent pas à l'utilisation prévue. Les règles de périphérique ne permettent pas d'empêcher ce comportement.

Vous pouvez contrôler les périphériques USB disponibles pour la redirection USB générique en spécifiant des règles de redirection de périphérique USB qui remplaceront les règles de stratégie USB par défaut.

Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) :

- Dans la plupart des cas, téléchargez le MSI de la console de gestion des stratégies de groupe Citrix (`CitrixGroupPolicyManagement_x64.msi`) et installez-le dans votre système Active Directory, puis gérez les stratégies de groupe AD. (N'installez pas le MSI sur un VDA.)
- Pour l'application Citrix Workspace pour Windows, modifiez le registre de la machine utilisateur. Un modèle administratif (fichier ADM) est inclus dans le support d'installation pour vous permettre d'effectuer des modifications sur la machine utilisateur via une stratégie de groupe Active Directory : dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

Citrix Virtual Apps and Desktops sur site :

- Pour le VDA, modifiez les règles de remplacement de l'administrateur pour les machines avec OS multi-session à l'aide de règles de stratégie de groupe. La console de gestion des stratégies de groupe est incluse sur le support d'installation :
  - x64 : dvd root `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86 : dvd root `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`

- Pour l'application Citrix Workspace pour Windows, modifiez le registre de la machine utilisateur. Un modèle administratif (fichier ADM) est inclus dans le support d'installation pour vous permettre d'effectuer des modifications sur la machine utilisateur via une stratégie de groupe Active Directory : dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Les règles par défaut du produit sont stockées dans HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\GenericUSB. ne modifiez pas les règles par défaut du produit. Au lieu de cela, utilisez-les pour créer des règles de remplacement de l'administrateur comme expliqué plus loin dans cet article. Les règles de remplacement d'objets de stratégie de groupe de substitution sont évaluées avant les règles par défaut du produit.

Les règles de remplacement de l'administrateur sont stockées dans HKEY_LOCAL_MACHINE\SOFTWARE\Policies\C Les règles de stratégies GPO sont au format **{Allow: | Deny:}** et sont suivies d'un ensemble d'expressions *tag=value* (balise=valeur) séparées par des espaces.

Les balises suivantes sont prises en charge :

| Balise | Description |
|---|---|
| VID | ID fournisseur du descripteur de périphérique |
| PID | ID de produit du descripteur de périphérique |
| REL | ID de version du descripteur de périphérique |
| Classe | Classe du descripteur de périphérique ou d'un descripteur d'interface ; veuillez consulter le site Web USB sur http://www.usb.org/ pour les codes de classe USB disponibles |
| Sous-classe | Sous-classe du descripteur de périphérique ou d'un descripteur d'interface |
| Prot | Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface |

Lors de la création de règles de stratégies, tenez compte de ce qui suit.

- Les règles ne sont pas sensibles à la casse.

- Les règles peuvent éventuellement comporter un commentaire, introduit par #, à la fin. Aucun délimiteur n'est requis et le commentaire est ignoré en cas de correspondance.
- Les espaces vides et les lignes de commentaires pures sont ignorés.
- L'espace est utilisé comme séparateur, mais il ne peut pas apparaître au milieu d'un nombre ou d'un identificateur. Par exemple, Deny: Class = 08 SubClass=05 est une règle valide, mais Deny: Class=0 Sub Class=05 ne l'est pas.
- Les balises doivent utiliser l'opérateur de correspondance =. Par exemple, VID=1230.
- Chaque règle doit commencer sur une nouvelle ligne ou faire partie d'une liste séparée par des points-virgules.

> **Remarque :**
>
> - À partir de la version 2212 de Citrix Virtual Apps and Desktops, certains périphériques USB ne peuvent plus utiliser la fonctionnalité de redirection USB générique. Vous devez ajouter ces périphériques de manière explicite à l'aide de leur ID de fournisseur (VID) et leur ID de produit (PID) respectifs.
> - Si vous utilisez le fichier modèle ADM, vous devez créer des règles sur une seule ligne sous forme de liste séparée par des points-virgules.

Exemples :

- Cet exemple illustre une règle de stratégie USB définie par l'administrateur pour des identificateurs de fabricant et de produit :

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
 Deny: VID=046D # Deny all Logitech products
```

- Cet exemple illustre une règle de stratégie USB définie par l'administrateur pour une classe, une sous-classe et un protocole définis :

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF
# Allow all USB-Miscellaneous devices
```

### Utiliser et supprimer des périphériques USB

Les utilisateurs peuvent se connecter un périphérique USB avant ou après le démarrage d'une session virtuelle.

Lors de l'utilisation de l'application Citrix Workspace pour Windows, ce qui suit s'applique :

- Les périphériques connectés après démarrage d'une session apparaissent immédiatement dans le menu USB de Desktop Viewer.

- Si un périphérique USB n'est pas correctement redirigé, vous pouvez essayer de résoudre le problème en attendant que la session virtuelle ait démarré avant de connecter le périphérique.
- Pour éviter la perte de données, utilisez l'icône « Retirer le périphérique en toute sécurité » Windows avant de supprimer le périphérique USB.

### Contrôles de sécurité pour les périphériques de stockage de masse USB

Une prise en charge optimisée est fournie pour les périphériques de stockage de masse USB. Elle fait partie du mappage des lecteurs clients Citrix Virtual Apps and Desktops. Les lecteurs de la machine utilisateur sont automatiquement mappés vers les lettres de lecteur sur le bureau virtuel lorsque les utilisateurs ouvrent une session. Les lecteurs sont affichés sous la forme de dossiers partagés associés à des lettres de lecteur mappé. Pour configurer le mappage de lecteur client, utilisez le paramètre **Lecteurs amovibles clients**. Ce paramètre se trouve dans la section Paramètres de stratégie de la redirection de fichier des paramètres de stratégie ICA.

Avec les périphériques de stockage de masse USB, vous pouvez utiliser le mappage de lecteurs clients ou la redirection USB générique, ou les deux. Vous pourrez contrôler ces fonctions à l'aide de stratégies Citrix. Les principales différences sont les suivantes :

| Fonctionnalité | Mappage des lecteurs clients | Redirection USB générique |
|---|---|---|
| Activée par défaut | Oui | Non |
| Accès en lecture seule configurable | Oui | Non |
| Accès chiffré au périphérique | Oui, si le cryptage est déverrouillé avant l'accès au périphérique | Oui |
| Appareils BitLocker To Go | Non | Non |
| Le périphérique peut être retiré en toute sécurité au cours d'une session | Non | Oui, étant donné que les utilisateurs suivent les recommandations du système d'exploitation pour un retrait en toute sécurité. |

Si la redirection USB générique et les stratégies de mappage de lecteurs clients sont activées, alors lorsqu'un périphérique de stockage de masse est inséré avant ou après le démarrage d'une session, il est redirigé à l'aide du mappage de lecteur client. Lorsque la redirection USB générique et les stratégies de mappage de lecteurs clients sont activées et qu'un périphérique est configuré pour une redirection automatique et un périphérique de stockage de masse est inséré avant ou après le démarrage

d'une session, il sera redirigé à l'aide d'USB générique. Pour plus d'informations, consultez l'article CTX123015 du centre de connaissances.

> **Remarque :**
>
> La redirection USB est prise en charge sur les connexions de bande passante faible, par exemple de 50 Kbps. Toutefois, la copie de fichiers volumineux ne fonctionnera pas

## Imprimer

June 27, 2024

La gestion des imprimantes dans votre environnement est un processus à plusieurs étapes :

1. Familiarisation avec les concepts d'impression, si ce n'est pas déjà le cas.
2. Planifiez votre architecture d'impression. Cela comprend l'analyse des besoins de votre entreprise, votre infrastructure d'impression existante, la façon dont vos utilisateurs et applications interagissent avec l'impression aujourd'hui et le modèle de gestion de l'impression qui s'applique le mieux à votre environnement.
3. Configurez votre environnement d'impression en sélectionnant une méthode de provisioning de l'imprimante et en créant des stratégies pour déployer votre solution d'impression. Mettez à jour des stratégies lorsque de nouveaux employés ou serveurs sont ajoutés.
4. Testez la configuration du pilote d'impression avant de le déployer auprès des utilisateurs.
5. Gérez votre environnement d'impression Citrix en gérant des pilotes d'imprimante et en optimisant les performances d'impression.
6. Résolvez les problèmes qui peuvent se produire.

### Concepts d'impression

Avant de commencer à planifier votre déploiement, assurez-vous que vous comprenez ces concepts majeurs pour l'impression :

- Les types suivants de provisioning de l'imprimante sont disponibles
- comment les tâches sont routées ;
- les bases de la gestion de pilotes d'impression.

Concepts d'impression créés sur les concepts d'impression Windows. Pour configurer et gérer l'impression correctement dans votre environnement, vous devez comprendre le fonctionnement de l'impression réseau et cliente Windows et ce que cela signifie en comportement d'impression dans cet environnement.

### Processus d'impression

Dans cet environnement, toutes les impressions sont lancées (par l'utilisateur) sur les machines hébergeant les applications. Les tâches d'impression sont redirigées via le serveur d'impression réseau ou la machine utilisateur vers le périphérique d'impression.

Il n'existe aucun espace de travail permanent pour les utilisateurs de bureaux et d'applications virtuels. Lorsqu'une session se termine, l'espace de travail de l'utilisateur est supprimé, et tous les paramètres doivent être recréés au début de chaque session. Par conséquent, chaque fois qu'un utilisateur démarre une nouvelle session, le système doit recréer l'espace de travail de l'utilisateur.

Lorsqu'un utilisateur effectue l'impression :

- Détermine les imprimantes à fournir à l'utilisateur. Ceci est appelé provisioning de l'impression ;
- restaure les préférences d'impression de l'utilisateur ;
- détermine la nature de l'imprimante par défaut pour la session.

Vous pouvez personnaliser la manière dont vous souhaitez réaliser ces tâches en configurant des options pour le provisioning de l'impression, le routage des tâches d'impression, la rétention des propriétés d'imprimante et la gestion de pilotes. Veillez à évaluer la manière dont les paramètres des options peuvent modifier les performances d'impression dans votre environnement, ainsi que l'expérience de l'utilisateur.

### Provisioning de l'impression

Le processus par lequel les imprimantes sont mises à disposition dans une session est appelé provisioning. Le provisioning de l'imprimante est généralement traité de manière dynamique. En d'autres termes, les imprimantes qui s'affichent dans une session ne sont pas prédéterminées et stockés. Au lieu de cela, les imprimantes sont assemblées et basées sur les stratégies, au fur et à mesure que la session est créée lors de l'ouverture de session et la reconnexion. Par conséquent, les imprimantes peuvent changer selon la stratégie, l'emplacement de l'utilisateur, et les modifications de réseau, s'ils sont reflétés dans les stratégies. Par conséquent, les utilisateurs itinérants vers un autre emplacement peuvent voir les modifications apportées à leur espace de travail.

Le système surveille également les imprimantes côté client et ajuste dynamiquement les imprimantes créées automatiquement dans les sessions en fonction des ajouts, suppressions et modifications apportées aux imprimantes côté client. Cette découverte dynamique des imprimantes présente un avantage pour les utilisateurs itinérants lorsqu'ils se connectent à partir de divers périphériques.

Les méthodes les plus courantes de provisioning de l'imprimante sont :

- **Serveur d'impression universelle** : le serveur d'impression universelle Citrix fournit la prise en charge de l'impression universelle pour les imprimantes réseau. Le serveur d'impression

universelle utilise le pilote d'impression universelle. Cette solution vous permet d'utiliser un pilote unique sur une machine avec OS multi-session pour permettre l'impression réseau à partir de n'importe quel périphérique.

Citrix recommande d'utiliser le serveur d'impression universelle Citrix pour les scénarios de serveur d'impression distants. Le serveur d'impression universelle transfère la tâche d'impression sur le réseau selon un format optimisé et compressé, réduisant ainsi l'utilisation du réseau et améliorant l'expérience utilisateur.

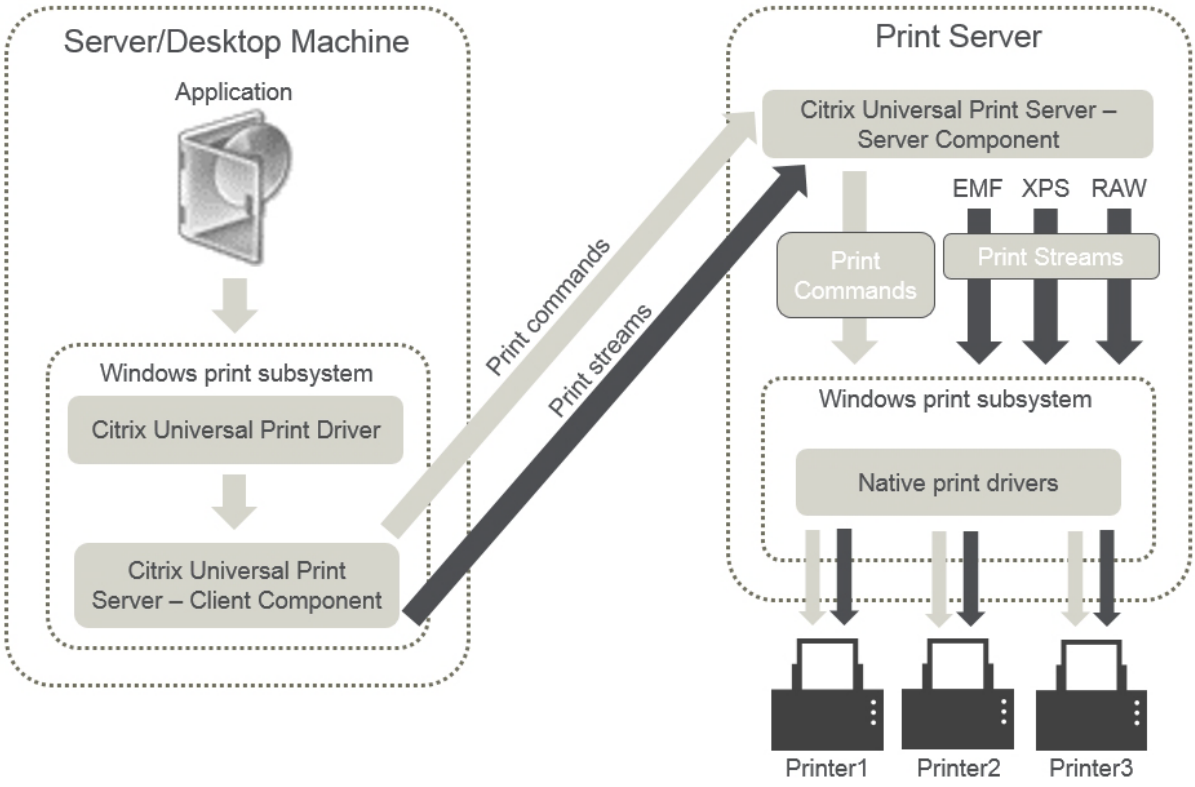
La fonctionnalité Serveur d'impression universelle comprend :

Un composant client, **UPClient** : activez UPClient sur chaque machine d'OS multi-session qui fournit des imprimantes réseau de session et utilise le pilote d'imprimante universel.

Un composant serveur, **UPServer** : installez UPServer sur chaque serveur d'impression qui fournit des imprimantes réseau de session et utilise le pilote d'impression universel pour les imprimantes de session (que les imprimantes de session soient approvisionnées de manière centralisée ou non).

Pour la configuration requise du serveur d'impression universelle et les détails d'installation, reportez-vous aux articles Configuration système requise et Installation.

L'illustration suivante affiche le flux de travail classique pour un réseau en fonction de l'imprimante réseau dans un environnement qui utilise le serveur d'impression universelle.




Lorsque vous activez le Serveur d'impression universelle Citrix, toutes les imprimantes réseau con-

nectées en tirent parti automatiquement via la découverte automatique.

- **Création automatique** : le terme *Création automatique* fait référence aux imprimantes crées automatiquement au début de chaque session. À la fois les imprimantes réseaux distantes et les imprimantes clientes locales peuvent être créées automatiquement. Envisagez la création automatique uniquement de l'imprimante cliente par défaut pour les environnements possédant un grand nombre d'imprimantes par utilisateur. La création automatique d'un plus petit nombre d'imprimantes utilise moins de traitement de mémoire et de processeur sur les machines avec OS multi-session. La réduction des imprimantes créées automatiquement permet également de réduire les durées d'ouverture de session de l'utilisateur.

  Les imprimantes créées automatiquement sont basées sur :

  - les imprimantes installées sur la machine utilisateur ;
  - toutes les stratégies qui s'appliquent à la session.

    Les paramètres de stratégie de création automatique vous permettent de limiter le nombre ou le type d'imprimantes créées automatiquement. Par défaut, les imprimantes mises à disposition dans les sessions lors de la configuration automatique de toutes les imprimantes sur la machine cliente, y compris celles connectées localement et les imprimantes réseau.

  Après que l'utilisateur ait mis fin à la session, les imprimantes de cette session sont supprimées.

  La création automatique de l'imprimante cliente et réseau possède une maintenance associée. Par exemple, l'ajout d'une imprimante requiert que vous effectuiez les opérations suivantes :

  - Mettre à jour le paramètre de stratégie Imprimantes de session.
  - Ajouter le pilote à toutes les machines avec OS multi-session utilisant le paramètre de stratégie Mappage et compatibilité du pilote d'imprimante.

### Routage des tâches d'impression

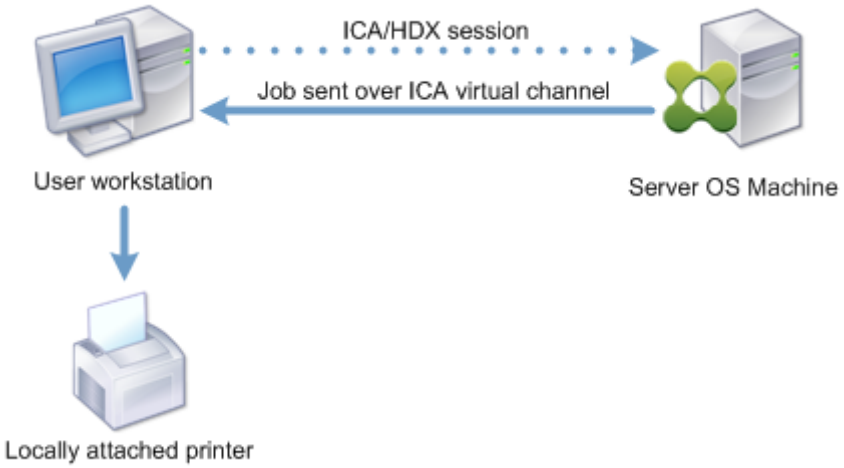
Le terme piste d'impression regroupe à la fois le chemin suivant lequel les tâches d'impression sont routées et l'emplacement dans lequel les tâches d'impression sont spoulées. Les deux aspects de ce concept sont importants. Le routage affecte le trafic réseau. La mise en file d'attente affecte l'utilisation des ressources locales sur la machine qui traite la tâche d'impression.

Dans cet environnement, les tâches d'impression peuvent prendre deux chemins d'accès vers un périphérique d'impression : via le client ou via un serveur d'impression réseau. Ces chemins d'accès sont appelées piste d'impression cliente et piste d'impression réseau. Le chemin d'accès sélectionné par défaut dépend du type d'imprimante utilisé.

### Imprimantes connectées localement

Le système route les tâches vers des imprimantes connectées localement à partir de la machine avec OS multi-session, au travers du client, puis vers le périphérique d'impression. Le protocole ICA optimise et compresse le trafic de la tâche d'impression. Lorsqu'un périphérique d'impression est connecté localement à la machine utilisateur, les tâches d'impression sont routées via le canal virtuel ICA.




### Imprimantes réseau

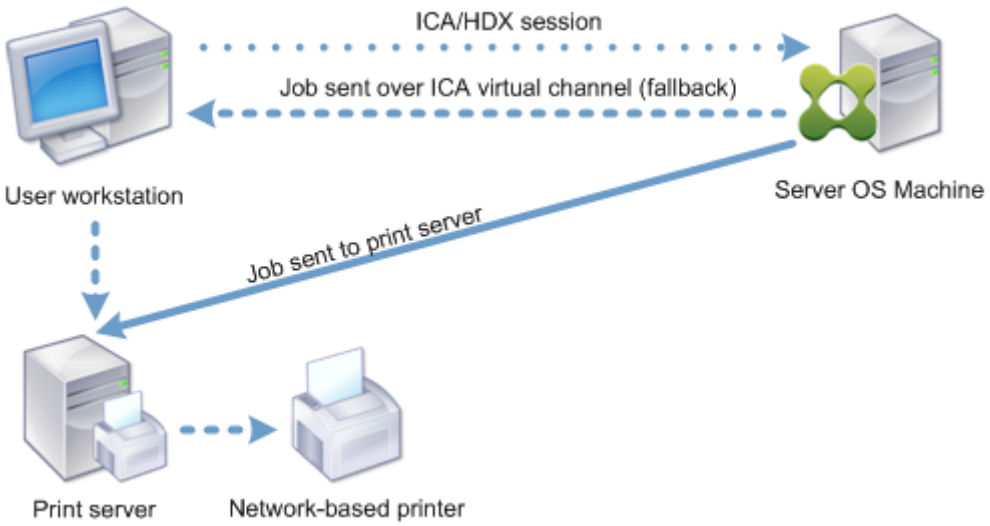
Par défaut, toutes les tâches d'impression sont destinées à la route d'imprimantes réseau à partir de la machine avec OS multi-session, au travers du réseau, et directement vers le serveur d'impression. Cependant, les tâches d'impression sont routées automatiquement via la connexion ICA dans les cas suivants :

- Si le bureau virtuel ou l'application ne peuvent pas contacter le serveur d'impression.
- Si le pilote d'imprimante natif n'est pas disponible sur la machine avec OS multi-session.

Si le serveur d'impression universelle n'est pas activé, la configuration de la piste d'impression cliente pour l'impression réseau est utile pour les connexions à faible bande passante, telles que les réseaux étendus, qui peuvent bénéficier de l'optimisation et de la compression du trafic résultant en l'envoi de tâches via la connexion ICA.

La piste d'impression cliente vous permet également de limiter le trafic ou de restreindre la bande passante allouée aux tâches d'impression. Si le routage de tâches via la machine utilisateur n'est pas possible, tel que pour les clients légers sans les fonctionnalités d'impression, la qualité de service doit être configurée pour favoriser le trafic ICA/HDX et assurer une bonne expérience de l'utilisateur dans les sessions.




### Gestion des pilotes d'impression

Le pilote d'imprimante universelle Citrix (UPD) est un pilote d'imprimante indépendant du périphérique, qui est compatible avec la plupart des imprimantes. Le pilote UPD Citrix est constitué de deux composants :

**Composant serveur**. Le pilote d'imprimante universelle Citrix est installé dans le cadre de l'installation de VDA Citrix Virtual Apps and Desktops. Le VDA installe les pilotes suivants avec le pilote UPD Citrix : « Citrix Universal Printer » (pilote EMF) et « Citrix XPS Universal Printer » (pilote XPS).

| Name | Processor | Type |
|---|---|---|
| Citrix Universal Printer | x64 | Type 3 - User Mode |
| Citrix XPS Universal Printer | x64 | Type 3 - User Mode |

Les programmes d'installation de VDA n'offrent plus d'options permettant de contrôler l'installation du pilote d'impression universel PDF Citrix. Le pilote d'imprimante PDF est maintenant installé automatiquement. Lorsque vous effectuez une mise à niveau vers le VDA 7.17 (ou une version ultérieure prise en charge), tout pilote d'imprimante Citrix PDF précédemment installé est automatiquement supprimé et remplacé par la dernière version.

Lorsqu'une tâche d'impression est initiée, le pilote enregistre la sortie de l'application et l'envoie, sans qu'aucune modification ne soit apportée au périphérique de destination.

**Composant client**. Le pilote d'imprimante universelle Citrix est installé dans le cadre de l'installation de l'application Citrix Workspace. Il récupère le flux d'impression entrant pour la session Citrix Virtual Apps and Desktops. Il transmet ensuite le flux d'impression au sous-système d'impression locale où la tâche d'impression est restituée à l'aide des pilotes d'imprimante spécifiques au périphérique.

Le pilote d'imprimante universelle Citrix prend en charge les formats d'impression suivants :

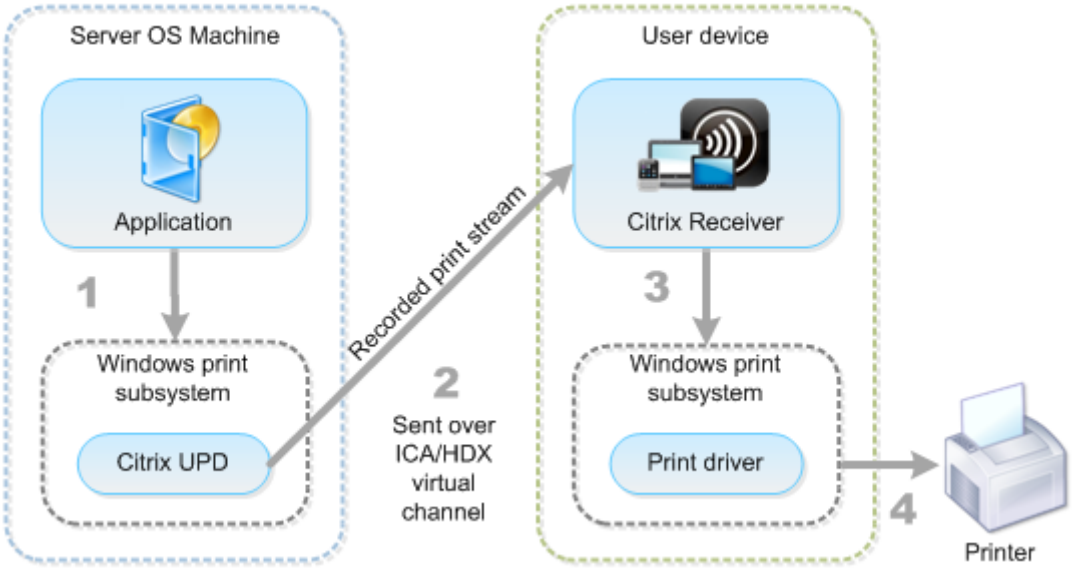
 

- Enhanced Metafile Format (**EMF**), valeur par défaut. EMF est la version 32 bits de Windows Metafile Format (WMF). Le pilote EMF peut uniquement être utilisé par les clients Windows.
- XML Paper Specification (**XPS**). Le pilote XPS utilise XML pour créer un « papier électronique » indépendant de la plate-forme utilisée similaire au format PDF d'Adobe.
- Printer Command Language (**PCL5c** et **PCL4**). PCL est un protocole d'impression développé par Hewlett-Packard pour les imprimantes à jet d'encre. Il est utilisé pour l'impression de texte et de graphiques de base et est largement pris en charge sur les périphériques HP LaserJet et multifonctions.
- PostScript (**PS**). PostScript est un langage informatique qui peut être utilisé pour l'impression de texte et de graphiques vectoriels. Ce pilote est largement utilisé avec les imprimantes et multifonctions de base.

Les pilotes PS et PCL sont plus adaptés lors de l'utilisation de machines non Windows, avec un client Mac ou UNIX par exemple. L'ordre dans lequel le pilote d'imprimante universelle Citrix tente d'utiliser les pilotes peut être modifié à l'aide du paramètre de stratégie Préférence de pilote universel.

Le pilote d'imprimante universelle Citrix (pilotes EMF et XPS) prend en charge les fonctionnalités d'impression avancées, telles que l'agrafage et la sélection de l'alimentation papier. Ces fonctionnalités sont disponibles si le pilote natif les rend disponibles à l'aide de la technologie d'impression de Microsoft. Le pilote natif doit utiliser les mots clés du schéma d'impression standard dans le fichier XML des fonctionnalités d'impression. Si des mots-clés non standard sont utilisés, les fonctionnalités d'impression avancées ne sont pas disponibles à l'aide du pilote d'imprimante universelle Citrix.

L'illustration suivante affiche les composants du pilote d'impression universelle et un flux de travail typique pour une imprimante connectée localement sur un périphérique.



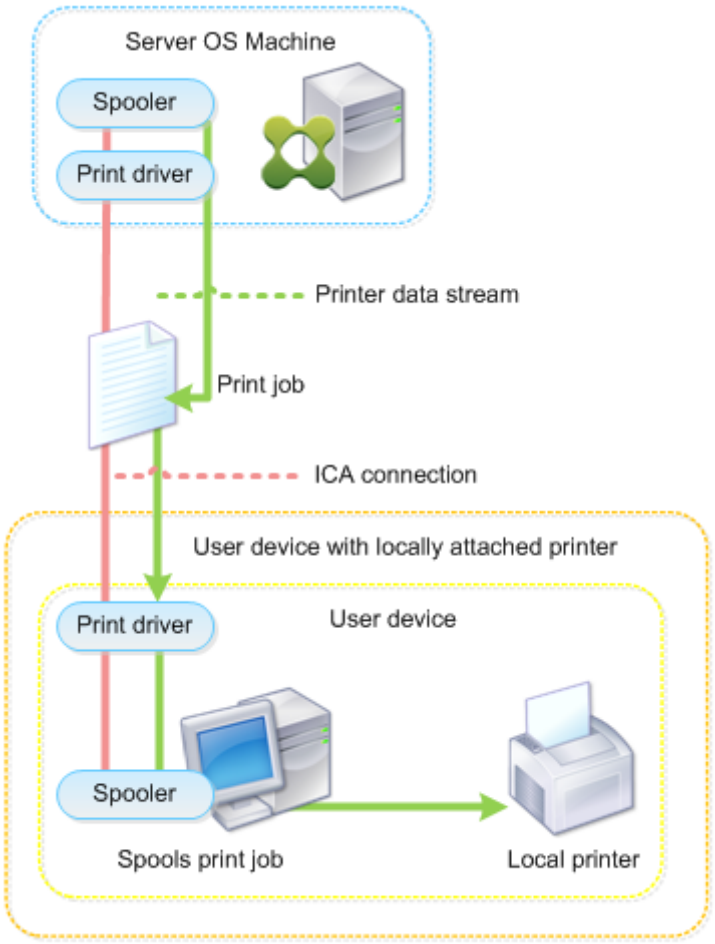

Lors de la planification de votre stratégie de gestion de pilote, déterminez si vous allez prendre en charge le pilote d'impression universelle, le pilote spécifique à la machine, ou les deux. Si vous prenez

en charge les pilotes standards, vous devrez également déterminer :

Lors de la création automatique des imprimantes, si le système détecte une nouvelle imprimante locale connectée à une machine utilisateur, il vérifie la présence du pilote d'imprimante requis sur la machine avec OS multi-session. Par défaut, si un pilote natif Windows n'est pas disponible, le système utilise le pilote d'impression universelle.

Le pilote d'imprimante de la machine avec OS multi-session et le pilote de la machine utilisateur doivent correspondre pour que l'impression réussisse. Le diagramme qui suit démontre comment le pilote d'imprimante est utilisé à deux endroits pour l'impression cliente.




- Les types de pilotes à prendre en charge.
- Indiquez si vous devez installer les pilotes d'imprimante automatiquement lorsqu'ils sont manquants sur les machines avec OS multi-session.
- Indiquer s'il faut créer des listes de compatibilité du pilote.

### Contenu associé

- Exemple de configuration d'impression
- Meilleures pratiques, considérations de sécurité et opérations par défaut
- Stratégies et préférences d'impression
- Provisionner les imprimantes
- Gestion de l'environnement d'impression

## Exemple de configuration d'impression

June 27, 2024

Le choix d'options de configuration d'impression les plus appropriées à vos besoins et à l'environnement peut simplifier l'administration. Bien que la configuration d'impression par défaut permet aux utilisateurs d'imprimer dans la plupart des environnements, les valeurs par défaut peuvent ne pas fournir la meilleure expérience utilisateur attendue ou l'utilisation du réseau et de surcharge de gestion pour votre environnement.

Votre configuration d'impression dépend des facteurs suivants :

- Les besoins de votre entreprise et votre infrastructure d'impression existante.

  Concevez votre configuration d'impression selon les besoins de votre organisation. Votre implémentation d'impression existante (capacité des utilisateurs à ajouter des imprimantes, quels utilisateurs ont accès à quelles imprimantes, etc) peut être un guide utile lors de la définition de la configuration de l'impression.

- Si votre entreprise possède des stratégies de sécurité qui réservent des imprimantes pour certains utilisateurs (par exemple, des imprimantes pour le département des ressources humaines ou finance).

- Si les utilisateurs doivent imprimer alors qu'ils sont éloignés de leur emplacement de travail principal ; par exemple, les travailleurs qui se déplacent entre stations de travail ou sont en voyage d'affaire.

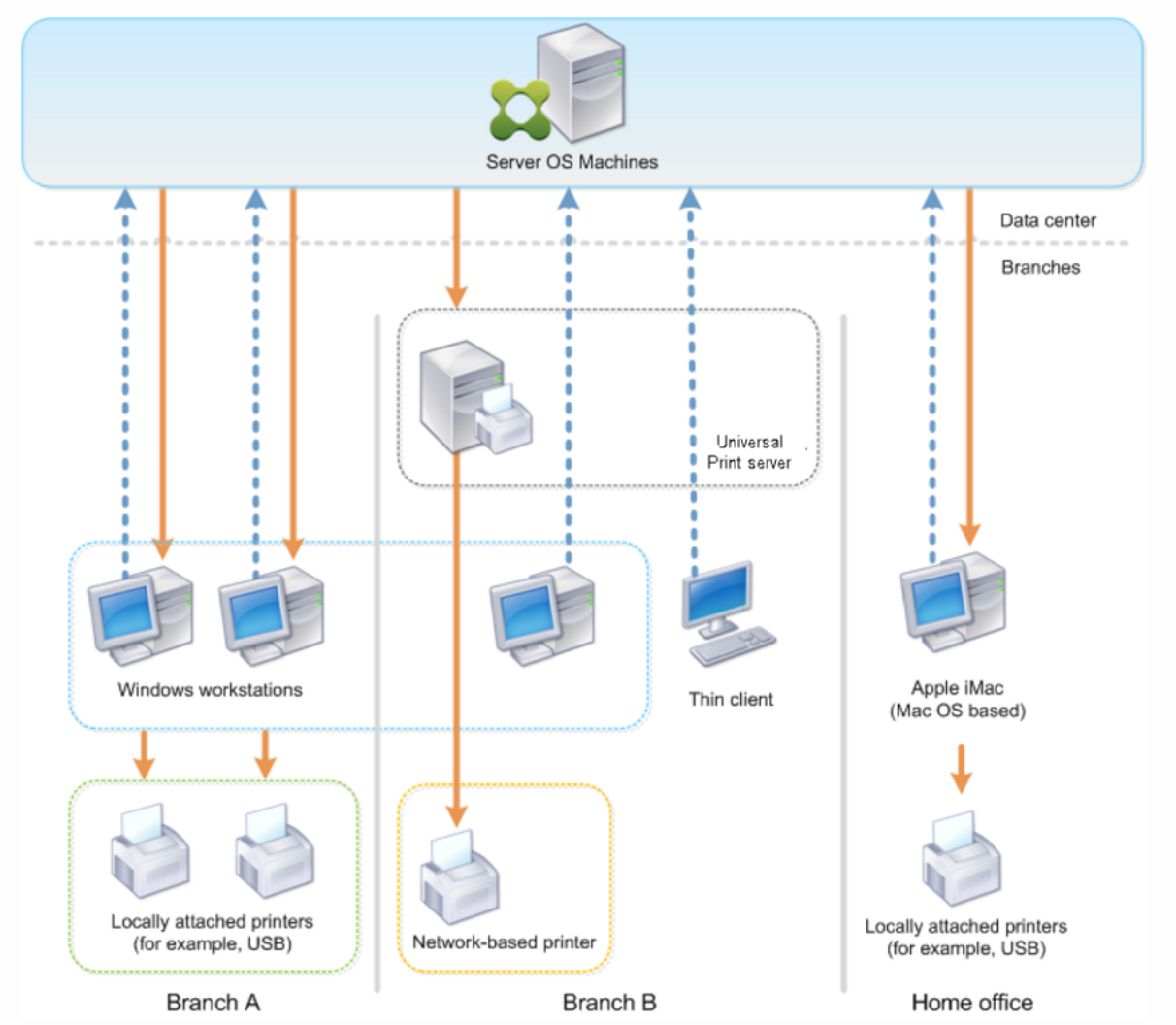
Lors de la conception de votre configuration d'impression, essayez de fournir aux utilisateurs la même expérience en session qu'ils rencontrent lorsqu'ils impriment depuis leurs machines utilisateur locales.

### Exemple de déploiement d'impression

L'illustration suivante affiche le déploiement pour ces cas d'utilisation :

- **Succursale A :** une petite succursale à l'étranger avec quelques stations de travail Windows. Chaque utilisateur station de travail possède une imprimante privée, connectée localement.
- **Succursale B :** une succursale importante avec des clients légers et des stations de travail Windows. Pour une meilleure efficacité, les utilisateurs de cette succursale partagent des imprimantes réseau (une par étage). Des serveurs d'impression Windows situés dans la succursale gèrent les files d'attente d'impression.
- **Bureau à domicile :** un bureau à domicile avec une machine utilisateur Mac OS qui accède à l'infrastructure Citrix de l'entreprise. La machine utilisateur dispose d'une imprimante connectée localement.




Les sections suivantes décrivent les configurations qui réduisent la complexité de l'environnement et simplifient sa gestion.

### Imprimantes créées automatiquement et pilote d'imprimante universelle Citrix

Dans la succursale A, tous les utilisateurs travaillent sur des stations de travail Windows, par conséquent, les imprimantes clientes créées automatiquement et le pilote d'imprimante universelle sont utilisés. Ces technologies fournissent ces avantages :

- Performances : les tâches d'impression sont fournies via le canal ICA d'impression et les données d'impression peuvent être compressées pour économiser la bande passante.

  Pour vous assurer qu'un seul utilisateur imprimant un document important ne peut dégrader les performances de session des autres utilisateurs, une stratégie Citrix est configurée pour spécifier la bande passante d'impression maximale.

  Une autre solution consiste à tirer parti d'une connexion multi-stream ICA, dans laquelle le trafic d'impression est transféré vers une autre connexion TCP à basse priorité. Multi-stream ICA est une option lorsque la qualité de service (QoS) n'est pas implémentée sur la connexion de réseau étendu.
- Flexibilité : l'utilisation du pilote d'imprimante universelle Citrix assure que toutes les imprimantes connectées à un client peuvent également être utilisées à partir d'un bureau virtuel ou la session d'application sans intégrer un nouveau pilote d'imprimante dans le centre de données.

### Serveur d'impression universelle Citrix

Dans la succursale B, toutes les imprimantes sont basées sur le réseau et leurs files d'attente sont gérées sur un serveur d'impression Windows, et le Serveur d'impression universelle Citrix est ainsi le plus efficace de la configuration.

Tous les pilotes d'imprimante requis sont installés et gérés sur le serveur d'impression par les administrateurs locaux. Le mappage des imprimantes dans le bureau virtuel ou la session d'application fonctionne comme suit :

- Pour les stations de travail Windows : l'équipe informatique locale permet aux utilisateurs de connecter l'imprimante réseau à leurs stations de travail Windows. Cela permet aux utilisateurs d'imprimer à partir des applications installées localement.

  Lors d'une session application ou de bureau virtuel, les imprimantes de session configurées localement sont énumérées via la création automatique. Le bureau virtuel ou l'application se connectent au serveur d'impression en tant que connexion réseau directe si possible.

  Les composants du serveur d'impression universelle Citrix sont installés et activés, ainsi les pilotes d'imprimante natifs ne sont pas requis. Si un pilote est mis à jour ou une file d'attente d'imprimante est modifiée, aucune configuration supplémentaire n'est requise dans le centre de données.

- Pour les clients fins : pour les utilisateurs des clients légers, les imprimantes doivent être connectées au sein de la session de bureau virtuel ou d'application. Pour fournir aux utilisateurs l'expérience d'impression la plus simple, les administrateurs configurent une stratégie Citrix Imprimante de session unique par étage pour connecter une imprimante par étage en tant qu'imprimante par défaut.

  Pour vous assurer que l'imprimante appropriée est connectée, même si les utilisateurs itinèrent entre les étages, les stratégies sont filtrées en fonction du sous-réseau ou du nom du client léger. Cette configuration, appelée impression de proximité, permet la maintenance du pilote d'imprimante locale (en fonction du modèle d'administration déléguée).

  Si une file d'attente d'imprimante doit être modifiée ou ajoutée, les administrateurs Citrix doivent modifier la stratégie Imprimante de session correspondante au sein de l'environnement.

Étant donné que le trafic d'impression réseau sera envoyé en dehors du canal virtuel ICA, la qualité de service (QoS) est implémentée. Le trafic réseau entrant et sortant sur les ports utilisés par le trafic ICA/HDX sont prioritaires sur tous les autres trafics réseau. Cette configuration permet d'assurer que les sessions utilisateur ne sont pas affectées par les tâches d'impression importantes.

### Imprimantes créées automatiquement et pilote d'imprimante universelle Citrix

Pour les bureaux à domicile sur lesquels les utilisateurs travaillent sur des stations de travail non standard et utilisent des périphériques d'impression non gérés, l'approche la plus simple consiste à utiliser les imprimantes clientes créées automatiquement et le pilote d'imprimante universelle.

### Récapitulatif du déploiement

Dans le récapitulatif, l'exemple de déploiement est configuré comme suit :

- Aucun des pilotes d'imprimante n'est installé sur les machines avec OS multi-session. Seul le pilote d'imprimante universelle Citrix est utilisé. Le retour à l'impression native et l'installation automatique des pilotes d'imprimantes est désactivé.
- Une stratégie est configurée pour créer automatiquement toutes les imprimantes clientes pour tous les utilisateurs. Les machines avec OS multi-session se connecteront directement aux serveurs d'impression par défaut. La seule configuration requise est l'activation des composants du serveur d'impression universelle.
- Une stratégie d'imprimante de session est configurée pour chaque étage de la succursale B et appliquée à tous les clients légers de l'étage respectif.
- QoS est implémentée pour la succursale B afin d'assurer une excellente expérience utilisateur.

# Meilleures pratiques, considérations de sécurité et opérations par défaut

June 27, 2024

## Recommandations

De nombreux facteurs déterminent la meilleure solution d'impression pour un environnement particulier. Certaines de ces recommandations risquent de ne pas s'appliquer à votre site.

- Utilisez le Serveur d'impression universelle Citrix.
- Utilisez le pilote d'imprimante universelle ou les pilotes natifs Windows.
- Réduisez le nombre de pilotes d'imprimante installés sur les machines avec OS multi-session.
- Utilisez le mappage de pilote pour les pilotes natifs.
- Ne jamais installer de pilotes d'imprimante non testés sur un site de production.
- Évitez de la mise à jour de pilote. Essayez toujours de désinstaller un pilote, redémarrer le serveur d'impression, puis installer le pilote de remplacement.
- Désinstallez les pilotes non utilisées ou utilisez la stratégie Mappage et compatibilité du pilote d'imprimante pour empêcher la création d'imprimantes avec le pilote.
- Essayez d'éviter d'utiliser la version 2 des pilotes en mode noyau.
- Pour savoir si un modèle d'imprimante est pris en charge, contactez le fabricant ou consultez le guide du produit Citrix Ready sur www.citrix.com/ready.

  En général, les pilotes d'imprimante fourni par Microsoft sont testées avec les services Terminal Server et sont garantis de fonctionner avec Citrix. Toutefois, avant d'utiliser un pilote d'impression tiers, consultez votre fournisseur de pilote d'imprimante pour que le pilote soit certifié pour les services Terminal Server par le programme Windows Hardware Quality Labs (WHQL). Citrix ne certifie pas les pilotes d'imprimante.

## Considérations de sécurité

Les solutions d'impression Citrix sont sécurisées dès leur conception.

- Le service du Gestionnaire d'impression Citrix surveille en permanence et répond aux événements de session, tels que l'ouverture et la fermeture de session, la déconnexion, la reconnexion et la terminaison d'une session. Il gère les demandes de service en imitant la session utilisateur courante.

- L'impression Citrix affecte un espace de noms unique à chaque imprimante dans une session.
- L'impression Citrix définit le descripteur de sécurité par défaut pour les imprimantes créées automatiquement pour vous assurer que les imprimantes clientes créées automatiquement dans une session ne sont pas accessibles aux utilisateurs exécutés dans d'autres sessions. Par défaut, les utilisateurs administratifs ne peuvent pas accidentellement d'imprimer vers une autre session d'imprimante cliente, même s'ils peuvent afficher et ajuster manuellement les permissions des imprimantes clientes.

### Opérations d'impression par défaut

Par défaut, si vous ne configurez aucune règle de stratégie, le comportement d'impression est le suivant :

- La fonctionnalité Serveur d'impression universelle est désactivée.
- Toutes les imprimantes configurées sur la machine utilisateur sont automatiquement créées au début de chaque session.

  Ce comportement est équivalent à la configuration du paramètre de stratégie Citrix Créer automatiquement les imprimantes clientes avec l'option Créer automatiquement toutes les imprimantes clientes.
- Le système route toutes les tâches d'impression mises en file d'attente sur les imprimantes connectées localement vers les machines clientes en tant que tâches d'impression clientes (c'est-à-dire, via le canal ICA et au travers de la machine utilisateur).
- Le système route toutes les tâches d'impression mises en file d'attente vers les imprimantes réseau directement depuis les machines avec OS multi-session. Si le système ne peut pas router les tâches sur le réseau, il les routera au travers de la machine utilisateur sous la forme d'une tâche d'impression cliente redirigée.

  Ce comportement est équivalent à la désactivation du paramètre de stratégie Citrix Diriger les connexions vers les serveurs d'impression.
- Le système tente de stocker les propriétés d'impression, une combinaison des préférences d'impression de l'utilisateur et des paramètres d'impression spécifiques à la machine, sur la machine cliente. Si le client ne prend pas en charge cette opération, le système stocke les propriétés d'impression dans les profils utilisateur sur la machine avec OS multi-session.

  Ce comportement est équivalent à la configuration du paramètre de stratégie Citrix Rétention des propriétés de l'imprimante avec l'option Contenu dans le profil uniquement si non enregistré sur le client.
- Dans les VDA version 7.16 et ultérieures, le paramètre de stratégie Citrix « Installation automatique de pilotes d'imprimante fournis avec Windows » n'a aucun effet sur Windows 8 et les ver-

sions ultérieures des systèmes d'exploitation Windows car les pilotes d'imprimante V3 ne sont pas inclus dans le système d'exploitation.

- Dans les VDA de version antérieure à 7.16, le système utilise la version de Windows du pilote d'imprimante si elle est disponible sur la machine avec OS multi-session. Si le pilote d'imprimante n'est pas disponible, le système tente d'installer le pilote à partir du système d'exploitation Windows. Si le pilote n'est pas disponible sous Windows, il utilise un pilote d'impression universelle Citrix.

  Ce comportement est équivalent à l'activation du paramètre de stratégie Citrix « Installation automatique de pilotes d'imprimante fournis avec Windows » et à la configuration du paramètre Impression universelle avec l'option Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible.

  L'activation de l'installation automatique de pilotes d'imprimante fournis avec Windows peut entraîner l'installation de nombreux pilotes d'imprimante natifs.

> **Remarque :**
>
> Si vous n'êtes pas sûr des paramètres par défaut de livraison pour l'impression, vous pouvez les afficher en créant une nouvelle stratégie et en définissant toutes les règles de stratégie d'impression sur Activé. L'option qui s'affiche est l'option par défaut.

### Journalisation permanente

Une fonctionnalité de journalisation permanente est disponible pour le serveur d'impression et le sous-système d'impression sur le VDA.

Pour regrouper les journaux au format ZIP pour l'envoi par e-mail, ou pour charger automatiquement les journaux vers Citrix Insight Services, utilisez l'applet de commande PowerShell **Start-TelemetryUpload**.

## Stratégies et préférences d'impression

June 27, 2024

Lorsque les utilisateurs accèdent aux imprimantes à partir des applications publiées, vous pouvez configurer des stratégies Citrix pour spécifier :

- comment les imprimantes sont approvisionnées (ou ajoutées aux sessions) ;
- comment les tâches sont routées ;
- comment les pilotes d'imprimante sont gérés.

Vous pouvez posséder plusieurs configurations d'impression pour différentes machines utilisateur, utilisateurs ou tout autre objet sur lequel les stratégies sont filtrées.

La plupart des fonctions d'impression sont configurées au travers des paramètres de stratégie d'impression Citrix. Les paramètres d'impression sont conformes au comportement de stratégie Citrix standard :

XenDesktop peut écrire les paramètres de l'imprimante dans l'objet d'imprimante à la fin de la session ou sur le périphérique d'impression cliente, étant donné que le compte réseau de l'utilisateur possède les permissions suffisantes. Par défaut, l'application Citrix Workspace utilise les paramètres stockés dans l'objet d'imprimante de la session, avant de rechercher dans d'autres emplacements les paramètres et préférences.

Par défaut, le magasin store, ou conserve, des propriétés d'imprimante sur la machine utilisateur (si elle est prise en charge par la machine) ou dans le profil utilisateur de la machine avec OS multi-session. Lorsqu'un utilisateur modifie les propriétés de l'imprimante au cours d'une session, ces modifications sont mises à jour dans le profil de l'utilisateur sur la machine. La prochaine fois que l'utilisateur ouvre une session ou se reconnecte, la machine utilisateur hérite de ces paramètres conservés. En d'autres termes, les modifications apportées aux propriétés de l'imprimante sur la machine utilisateur n'affectent pas la session courante tant que l'utilisateur n'a pas fermé puis rouvert une session.

### Emplacements des préférence d'impression

Dans les environnements d'impression Windows, les modifications apportées aux préférences d'impression peuvent être stockées sur l'ordinateur local ou dans un document. Dans cet environnement, lorsque les utilisateurs modifient leurs paramètres d'impression, ils peuvent être stockés aux emplacements suivants :

- **Sur la machine utilisateur elle-même :** les utilisateurs Windows peuvent modifier les paramètres d'un périphérique sur la machine utilisateur en cliquant avec le bouton droit de la souris sur l'imprimante dans le Panneau de configuration, en sélectionnant Préférences d'impression. Par exemple, si Paysage est sélectionné en tant qu'orientation de page de l'imprimante, paysage est désormais enregistré en tant que préférence d'orientation de page par défaut pour cette imprimante.
- **Dans un document :** dans les programmes de traitement de texte et de publication assistée par ordinateur, les paramètres du document, tels que l'orientation de page, sont souvent stockés à l'intérieur des documents. Par exemple, une fois un document placé dans la file d'attente d'un document, Microsoft Word stocke généralement les préférences d'impression spécifiées, telles que l'orientation de page, et le nom de l'imprimante dans le document. Ces paramètres s'affichent par défaut la prochaine fois que vous imprimez ce document.

- **À partir des modifications effectuées par un utilisateur lors d'une session :** le système conserve uniquement les modifications apportées aux paramètres d'impression d'une imprimante créée automatiquement si la modification a été apportée dans le Panneau de configuration dans la session ; c'est-à-dire, sur la machine avec OS multi-session.
- **Sur la machine avec OS multi-session :** ce sont les paramètres par défaut associés à un pilote d'imprimante spécifique sur la machine.

Les paramètres préservés dans tout environnement Windows varient selon l'emplacement dans lequel l'utilisateur a effectué les modifications. Ceci signifie également que les paramètres d'impression qui s'affichent à un endroit, tel qu'un tableur, peuvent être différents de ceux qui s'affichent à d'autres endroits, tels que des documents. Ainsi, les paramètres d'impression appliqués à une imprimante spécifique peuvent changer dans une session.

### Hiérarchie des préférences d'impression des utilisateurs

Les préférences d'impression pouvant être stockées à plusieurs endroits, le système les traite selon une priorité spécifique. Il est également important de noter que les paramètres de la machine sont traités différemment des paramètres du document (et ont habituellement priorité sur ces derniers).

Par défaut, le système applique toujours tout paramètre d'impression modifié par un utilisateur lors d'une session, c'est-à-dire, les paramètres conservés, avant de considérer tout autre paramètre. Lorsque l'utilisateur effectue l'impression, le système fusionne et applique les paramètres de l'imprimante par défaut stockés sur la machine avec OS multi-session avec tout paramètre d'imprimante cliente ou conservé.

### Enregistrement des préférences d'impression de l'utilisateur

Citrix vous recommande de ne pas modifier l'emplacement de stockage des propriétés de l'imprimante. Le paramètre par défaut, qui enregistre les propriétés de l'imprimante sur la machine cliente, est la manière la plus facile d'assurer des propriétés d'impression cohérentes. Si le système n'a pas pu enregistrer les propriétés sur la machine utilisateur, il retourne automatiquement au profil utilisateur sur la machine avec OS multi-session.

Vérifiez le paramètre de stratégie Conservation des propriétés d'imprimante si ces scénarios s'appliquent :

- Si vous utilisez des plug-ins d'ancienne génération qui n'autorisent pas les utilisateurs à stocker des propriétés d'imprimante sur une machine utilisateur.
- Si vous utilisez des profils obligatoires sur votre réseau Windows et que vous souhaitez conserver les propriétés d'imprimante de l'utilisateur.

# Provisionner les imprimantes

June 27, 2024

## Serveur d'impression universelle Citrix

Lorsque vous déterminez la meilleure solution d'impression pour votre environnement, tenez compte de ce qui suit :

- Le serveur d'impression universelle fournit des fonctionnalités ne sont pas disponibles pour le fournisseur d'impression Windows : la mise en cache des images et des polices, la compression avancée, l'optimisation et la prise en charge de la qualité de service (QoS).
- Le pilote d'impression universelle prend en charge les paramètres indépendants de machine publics définis par Microsoft. Si les utilisateurs ont besoin d'accéder à des paramètres qui sont spécifiques au fabricant d'un pilote d'impression, le Serveur d'impression universelle associé à un pilote natif Windows peut être la meilleure solution. Avec cette configuration, vous conservez les avantages du Serveur d'impression universelle tout en offrant aux utilisateurs l'accès aux fonctionnalités d'impression spécialisées. Un compromis à prendre en compte est que les pilotes natifs Windows nécessitent une certaine maintenance.
- Le serveur d'imprimante universel Citrix fournit une prise en charge de l'impression universelle pour les imprimantes réseau. Le serveur d'impression universelle utilise le pilote d'impression universelle, un seul pilote sur la machine avec OS multi-session qui permet l'impression locale ou réseau à partir de n'importe quel périphérique, y compris des clients légers et des tablettes.

Pour utiliser le Serveur d'impression universelle avec un pilote natif Windows, activez le serveur d'impression universelle. Par défaut, si le pilote natif Windows est disponible, il est utilisé. Sinon, le pilote d'impression universelle est utilisé. Pour spécifier les modifications apportées à ce comportement, par exemple pour utiliser uniquement les pilotes natifs Windows ou le pilote d'impression universelle, mettez à jour le paramètre de stratégie Utilisation du pilote d'impression universelle.

### Installer le serveur d'impression universelle

Pour utiliser le serveur d'impression universelle, installez le composant UpsServer sur vos serveurs d'impression, comme décrit dans les documents d'installation et configurez-le. Pour de plus amples informations, consultez la section Installer les composants principaux et Installer à l'aide de la ligne de commande.

Dans les environnements dans lesquels vous voulez déployer le composant UPClient séparément, par exemple avec **XenApp 6.5** :

1. Téléchargez le package autonome Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA) pour OS mono-session ou multi-session Windows.
2. Extrayez le VDA à l'aide des instructions de ligne de commande décrites dans la section Installer à l'aide de la ligne de commande.
3. Installez les composants requis depuis \Image-Full\Support\VcRedist_2013_RTM
    - Vcredist_x64 / vcredist_x86
        - Exécutez x86 pour 32 bits uniquement, et les deux packages pour les déploiements 64 bits
4. Installez le composant requis cdf depuis \Image-Full\x64\Virtual Desktop Components ou \Image-Full\x86\Virtual Desktop Components.
    - Cdf_x64 / Cdf_x86
        - x86 pour 32 bits, x64 pour 64 bits
5. Localisez le composant UPClient dans \Image-Full\x64\Virtual Desktop Components ou \Image-Full\x86\Virtual Desktop Components.
6. Installez le composant UPClient en extrayant et en lançant le MSI du composant.
7. Un redémarrage est nécessaire après l'installation du composant UPClient.

#### Refuser de prendre part au programme CEIP pour le serveur d'impression universelle

Vous êtes automatiquement inscrit au Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) lorsque vous installez le serveur d'impression universelle. Le premier chargement de données s'effectue sept jours après la date et heure d'installation.

Pour ne plus participer au programme CEIP, modifiez la clé de registre **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled** et définissez la valeur **DWORD** sur **0**.

Pour participer à nouveau, définissez la valeur DWORD sur 1.

**Avertissement** : toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Pour de plus amples informations, consultez Citrix Insight Services.

#### Configurer le serveur d'impression universelle

Utilisez les paramètres de stratégie Citrix suivants pour configurer le serveur d'impression universelle. Pour plus d'informations, reportez-vous à l'aide des paramètres de stratégie à l'écran.

- **Serveur d'impression universelle activé**. Le serveur d'impression universelle est désactivé par défaut. Lorsque vous activez le serveur d'impression universelle, vous pouvez choisir d'utiliser le fournisseur d'impression Windows si le serveur d'impression universelle n'est pas disponible. Après avoir installé le serveur d'impression universelle, un utilisateur peut ajouter et énumérer des imprimantes réseau au travers des interfaces du fournisseur d'impression Windows et du fournisseur Citrix.
- **Port (CGP) du flux de données d'impression du serveur d'impression universelle**. Spécifie le numéro de port TCP utilisé par l'écouteur CGP (Common Gateway Protocol) du flux de données d'impression Serveur d'impression universelle. Valeurs par défaut **7229**.
- **Port (HTTP/SOAP) du service Web du serveur d'impression universelle**. Spécifie le numéro de port TCP utilisé par l'écouteur Serveur d'impression universelle pour les requêtes HTTP/-SOAP entrantes. Valeurs par défaut **8080**.

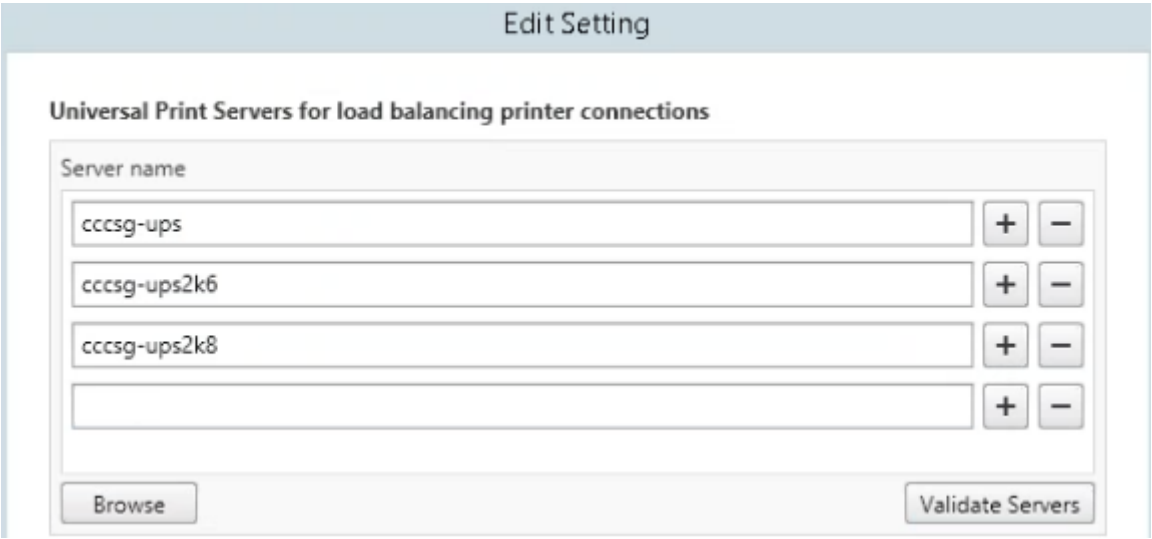
Pour modifier le port par défaut HTTP 8080 pour les communications du serveur d'impression universelle vers des VDA Citrix Virtual Apps and Desktops, le registre suivant doit également être créé et la valeur du numéro de port doit être modifiée sur l'ordinateur du serveur d'impression universelle :

HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Citrix\\PrintingPolicies
"UpsHttpPort"=DWORD:<portnumber>

Ce numéro de port doit correspondre à la stratégie HDX, le port du service Web du serveur d'impression universelle (HTTP/SOAP), dans Studio.

- **Limite de bande passante d'entrée du flux d'impression du serveur d'impression universelle (kbps)**. Spécifie la limite supérieure (en kilobits par seconde) pour le transfert des données d'impression mises à disposition depuis chaque tâche d'impression vers le Serveur d'impression universelle à l'aide de CGP. La valeur par défaut est 0 (illimitée).
- **Serveurs d'impression universelle d'équilibrage de la charge**. Ce paramètre dresse la liste des serveurs d'impression universelle à utiliser pour répartir la charge des connexions aux imprimantes établies lors du lancement de la session, après l'évaluation d'autres paramètres de stratégie d'impression Citrix. Pour optimiser la durée de création des imprimantes, Citrix recommande que les mêmes imprimantes partagées soient installées sur tous les serveurs d'impression.




- **Seuil au-delà duquel les serveurs d'impression universelle sont hors service**. Indique la durée pendant laquelle l'équilibrage de charge attend le rétablissement de la connexion à un serveur d'impression universelle avant de considérer que le serveur est hors connexion et de répartir sa charge sur d'autres serveurs d'impression disponibles. Le délai par défaut est de 180 secondes.

Une fois les stratégies d'impression modifiées sur le Delivery Controller, l'application des modifications de stratégie aux VDA peut prendre quelques minutes.

**Interactions avec d'autres paramètres de stratégie** : le serveur d'impression universelle respecte les autres paramètres de stratégie d'impression Citrix et interagit avec eux comme indiqué dans le tableau suivant. Les informations fournies supposent que si le paramètre de stratégie Serveur d'impression universelle est activé, les composants Serveur d'impression universelle sont installés, et les paramètres de stratégie sont appliqués.

| Paramètre de stratégie | Interaction |
| --- | --- |
| Redirection d'imprimante cliente, Créer automatiquement les imprimantes clientes | Si le Serveur d'impression réseau est activé, les imprimantes réseau clientes peuvent être créées à l'aide du pilote d'imprimante universelle, au lieu des pilotes natifs. Les utilisateurs aperçoivent le même nom d'imprimante qu'avant. |
| Imprimantes de session | Lors de l'utilisation de la solution du serveur d'impression universelle Citrix, les paramètres de stratégie du pilote d'imprimante universelle sont appliqués. |

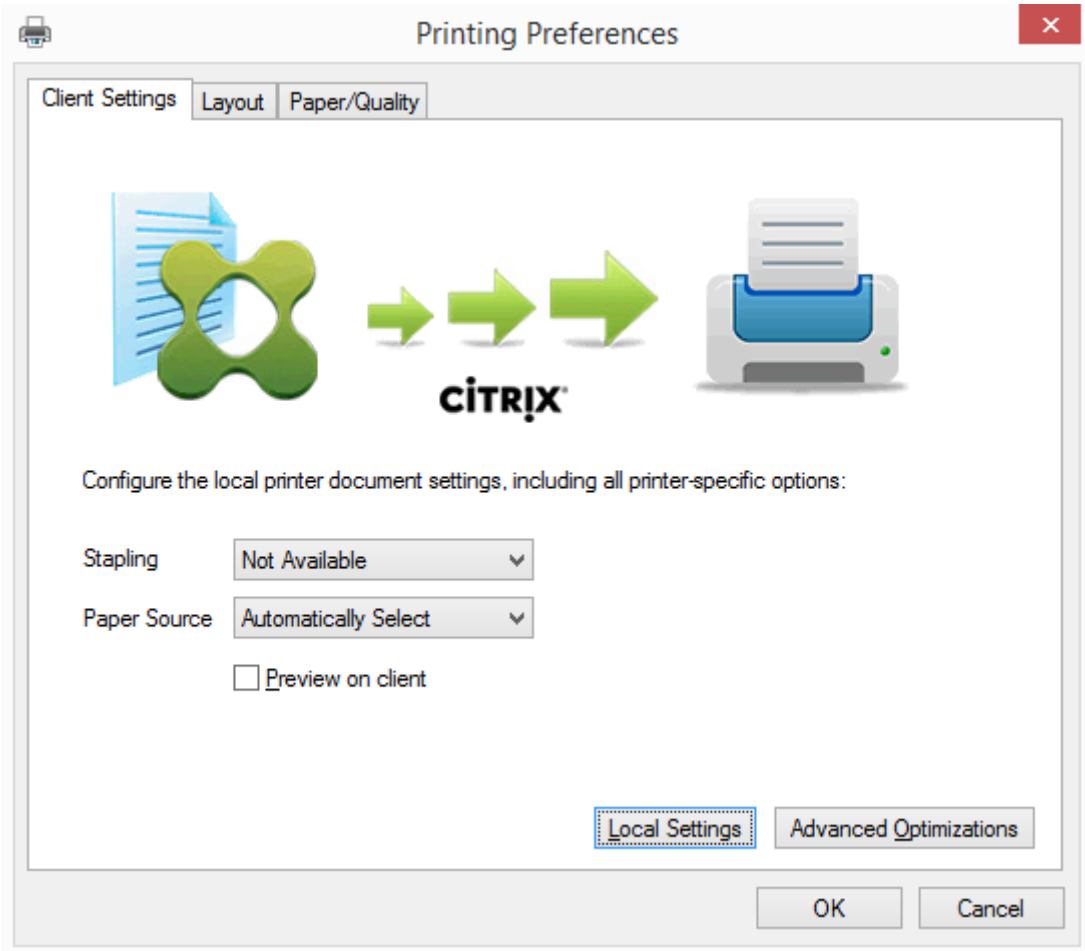
| | |
|---|---|
| Connexions directes au serveur d'impression | Lorsque le serveur d'impression réseau est activé et que le paramètre de stratégie d'utilisation des pilotes d'imprimante universelle est configuré pour utiliser l'impression universelle uniquement, une connexion d'imprimante réseau directe peut être créée sur le serveur d'impression, à l'aide du pilote d'impression universelle. |
| Préférence UPD | Prend en charge les pilotes EMF et XPS. |

**Effets sur les interfaces utilisateur** : le pilote d'impression universelle Citrix utilisé par le serveur d'impression universelle désactive les contrôles d'interface utilisateur suivants :

- dans la boîte de dialogue Propriétés d'imprimante, le bouton Paramètres d'imprimante local ;
- dans la boîte de dialogue Propriétés du document, les boutons Paramètres d'imprimante locale et Aperçu sur le client.

Le pilote d'imprimante universelle Citrix (pilotes EMF et XPS) prend en charge les fonctionnalités d'impression avancées, telles que l'agrafage et l'alimentation papier. L'utilisateur peut sélectionner les options Agrafage ou Alimentation papier dans la boîte de dialogue d'impression UDP personnalisée si le client ou les imprimantes réseau qui sont mappés sur le pilote d'imprimante universelle (UDP) dans la session prennent en charge ces fonctionnalités.




Pour configurer les paramètres d'imprimante non standard, tels que l'agrafage et le code PIN, sélectionnez **Paramètres locaux** dans la boîte de dialogue d'impression du pilote d'imprimante universelle pour les imprimantes mappées par le client qui utilisent le pilote Citrix EMF ou XPS. La boîte de dialogue **Préférences d'impression** de l'imprimante mappée est affichée en dehors de la session sur la machine cliente, ce qui permet à l'utilisateur de modifier les options d'imprimante, et les paramètres modifiés sont utilisés dans la session active lors de l'impression de ce document.

Ces fonctionnalités sont disponibles si le pilote natif les rend disponibles à l'aide de la technologie d'impression de Microsoft. Le pilote natif doit utiliser les mots clés du schéma d'impression standard dans le fichier XML des fonctionnalités d'impression. Si des mots-clés non standard sont utilisés, les fonctionnalités d'impression avancées ne seront pas disponibles à l'aide du pilote d'imprimante universelle Citrix.

Lors de l'utilisation du serveur d'impression universelle, l'assistant d'ajout d'imprimante du fournisseur d'impression Citrix est le même que l'assistant d'ajout d'imprimante du fournisseur d'impression Windows, avec les exceptions suivantes :

- Lors de l'ajout d'une imprimante par nom ou adresse, vous pouvez fournir un numéro de port HTTP/SOAP pour le serveur d'impression. Ce numéro de port devient une partie du nom d'

imprimante et apparaît dans les affichages.
- Si le paramètre de stratégie d'utilisation du pilote d'impression universelle Citrix spécifie que l'impression universelle doit être utilisée, le nom du pilote d'imprimante universelle s'affiche lors de la sélection d'une imprimante. Le fournisseur d'impression Windows ne peut utiliser le pilote d'impression universelle.

Le fournisseur d'impression Citrix ne prend pas en charge la restitution côté client.

Pour de plus amples informations sur le serveur d'impression universelle, consultez l'article CTX200328.

### Imprimantes clientes créées automatiquement

Ces solutions d'impression universelle sont fournies pour les imprimantes clientes :

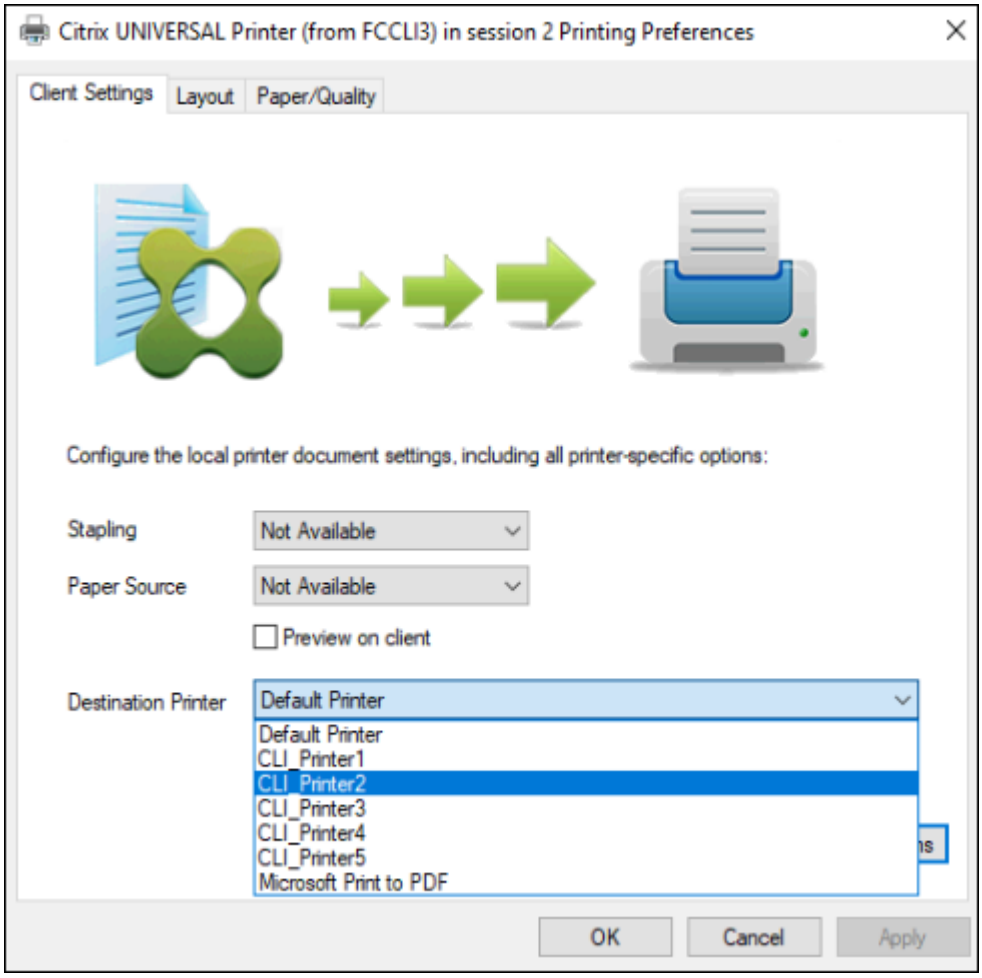
- **Imprimante universelle Citrix** : une imprimante générique créée au début des sessions qui n'est associée à aucun périphérique d'impression. Lorsque vous créez automatiquement et utilisez uniquement l'imprimante universelle Citrix, vous pouvez réduire l'utilisation des ressources et les temps de connexion des utilisateurs. L'imprimante universelle peut imprimer sur n'importe quel périphérique d'impression côté client.

  L'imprimante universelle Citrix peut ne pas fonctionner pour toutes les machines utilisateur ou applications Citrix Workspace de votre environnement. L'imprimante universelle Citrix requiert un environnement Windows et ne prend pas en charge Citrix Offline Plug-in ou les applications livrées en streaming vers le client. Utilisez les imprimantes clientes créées automatiquement et le pilote d'impression universelle pour de tels environnements.

  Si vous souhaitez utiliser une solution d'impression universelle pour les applications Citrix Workspace non Windows, utilisez l'un des autres pilotes d'impression universelle, qui sont basés sur Postscript ou PCL.

  L'imprimante universelle Citrix vous permet de sélectionner l'imprimante par défaut du client ou une imprimante cliente spécifique comme destination d'impression. Pour choisir une imprimante spécifique pour une tâche d'impression, ouvrez la boîte de dialogue **Préférences d'impression**. Sélectionnez la liste déroulante **Imprimante de destination**. L'option **Imprimante par défaut** envoie les tâches d'impression à l'imprimante par défaut du client. Toutes les imprimantes redirigées par le client connectées au terminal exécutant la session sont également répertoriées. L'imprimante que vous sélectionnez est enregistrée en tant qu'imprimante de destination pour les travaux d'impression futurs.




- **Pilotes d'impression universelle Citrix** : un pilote d'imprimante indépendant du périphérique. Si vous configurez un pilote d'impression universelle Citrix, le système utilise un pilote d'impression EMF par défaut.

  Le pilote d'impression universelle Citrix peut alors créer des tâches d'impression plus petites à l'inverse des pilotes d'imprimante plus anciens ou moins avancés. Toutefois, un pilote spécifique à la machine peut être nécessaire pour optimiser les tâches d'impression pour une imprimante spécialisée.

**Configurer l'impression universelle** : utilisez les paramètres de stratégie Citrix suivants pour configurer l'impression universelle. Pour plus d'informations, reportez-vous à l'aide des paramètres de stratégie à l'écran.

- Utilisation du pilote d'impression universelle Indique quand utiliser l'impression universelle.
- Créer automatiquement l'imprimante universelle générique. Active ou désactive la création automatique de l'objet d'imprimante universelle Citrix générique pour les sessions lorsqu'une machine utilisateur compatible avec l'impression universelle est en cours d'utilisation. Par défaut, l'objet Imprimante universelle générique n'est pas créé automatiquement.

- Préférence de pilote universel Spécifie l'ordre dans lequel le système tente d'utiliser les pilotes d'impression universelle, en commençant par la première entrée de la liste. Vous pouvez ajouter, modifier ou supprimer des pilotes et changer leur ordre dans la liste.
- Préférence d'aperçu d'impression universelle. Spécifie s'il convient d'utiliser la fonction d'aperçu d'impression pour les imprimantes universelles génériques ou créées automatiquement.
- Mode de traitement EMF de l'impression universelle. Contrôle la méthode de traitement du fichier de spoule EMF sur la machine utilisateur Windows. Par défaut, les enregistrements EMF sont spoulés directement sur l'imprimante. Le spoulage directement vers l'imprimante permet au spouleur de traiter les enregistrements plus rapidement et utiliser moins de ressources d'UC.

Vous trouverez des stratégies supplémentaires dans la section Optimiser les performances d'impression. Pour modifier les valeurs par défaut des paramètres tels que la taille du papier, la qualité du papier, la couleur, l'impression recto verso et le nombre de copies, consultez l'article CTX113148.

**Créer automatiquement des imprimantes depuis la machine de l'utilisateur** : au début de la session, le système crée automatiquement toutes les imprimantes sur la machine utilisateur par défaut. Vous pouvez contrôler quels types, le cas échéant, d'imprimantes sont provisionnés auprès des utilisateurs et empêchent la création automatique.

Utilisez le paramètre de stratégie
Citrix Créer automatiquement les imprimantes clientes pour contrôler la création automatique. Vous pouvez spécifier l'un des éléments suivants :

- toutes les imprimantes visibles pour la machine cliente, y compris les imprimantes connectées localement et les imprimantes réseau, sont créées automatiquement au début de chaque session (valeur par défaut) ;
- toutes les imprimantes locales connectées physiquement à la machine cliente sont créées automatiquement ;
- seule l'imprimante par défaut de la machine cliente est créée automatiquement.
- La création automatique est désactivée pour toutes les imprimantes clientes

Le paramètre Créer automatiquement les imprimantes clientes nécessite que le paramètre Redirection d'imprimante cliente soit Autorisé (valeur par défaut).

### Attribuer les imprimantes réseau aux utilisateurs

Par défaut, les imprimantes réseau de la machine cliente sont créées automatiquement au début des sessions. Le système vous permet de réduire le nombre d'imprimantes réseau énumérées et mappées en spécifiant les imprimantes réseau à créer dans chaque session. Certaines de ces imprimantes sont appelées Imprimantes de session.

Vous pouvez filtrer des stratégies d'imprimante de session par adresse IP pour offrir l'impression de proximité. L'impression de proximité permet aux utilisateurs se trouvant dans une plage d'adresses IP spécifiée d'accéder automatiquement aux périphériques d'impression réseau existant dans la même plage. L'impression de proximité est fournie par le Serveur d'impression universelle Citrix et ne nécessite pas la configuration décrite dans cette section.

L'impression de proximité peut impliquer le scénario suivant :

- Le réseau d'entreprise interne fonctionne avec un serveur DHCP qui attribue automatiquement les adresses IP aux utilisateurs.
- Tous les services d'une entreprise possèdent des plages d'adresses IP désignées uniques.
- Des imprimantes réseau existent dans la plage d'adresses IP de chaque service.

Lorsque l'impression de proximité est configurée et un employé voyage d'un service à un autre, aucune autre configuration du périphérique d'impression n'est requise. Lorsque la machine utilisateur est reconnue dans la plage d'adresse IP du nouveau service, elle a accès à toutes les imprimantes réseau de cette plage.

**Configurer des imprimantes spécifiques devant être redirigées dans les sessions** : pour créer des imprimantes attribuées à l'administrateur, configurez le paramètre de stratégie Citrix Imprimantes de session. Ajoutez une imprimante réseau à cette stratégie à l'aide de l'une des méthodes suivantes :

- Entrez le chemin UNC de l'imprimante au format \\nomserveur\nomimprimante.
- Rechercher un emplacement d'imprimante sur le réseau.
- Recherchez des imprimantes sur un serveur spécifique. Entrez le nom du serveur selon le format \\nomserveur et cliquez sur Parcourir.

Important : le serveur fusionne tous les paramètres d'imprimantes de session activés de toutes les stratégies appliquées en commençant par celles dont la priorité est la plus élevée. Lorsqu'une imprimante est configurée dans plusieurs objets de stratégie, les paramètres personnalisés par défaut ne sont utilisés qu'à partir de l'objet de stratégie ayant la plus haute priorité dans laquelle cette imprimante est configurée.

Les imprimantes réseau créées à l'aide du paramètre Imprimantes de session peuvent varier selon les conditions dans lesquelles la session a été initiée, en appliquant un filtre sur les objets comme les sous-réseaux.

**Spécifiez une imprimante réseau par défaut pour une session** : par défaut, l'imprimante principale de l'utilisateur est utilisée comme imprimante par défaut pour la session. Utilisez le paramètre de stratégie Citrix Imprimante par défaut pour changer la façon dont l'imprimante par défaut sur la machine utilisateur est établie dans une session.

1. Sur la page de paramètres Imprimante par défaut, sélectionnez un paramètre pour Choisir l'imprimante par défaut du client :

- Nom d'imprimante réseau. Les imprimantes ajoutées avec le paramètre de stratégie Imprimantes de session s'affichent dans ce menu. Sélectionnez l'imprimante réseau à utiliser comme valeur par défaut de cette stratégie.
- Ne pas ajuster l'imprimante par défaut de l'utilisateur. Utilise le réglage du profil utilisateur Windows ou des Services Terminal Server pour l'imprimante par défaut. Pour plus d'informations, reportez-vous à l'aide des paramètres de stratégie à l'écran.

2. Appliquez la stratégie au groupe d'utilisateurs (ou autres objets filtrés) que vous souhaitez attribuer.

**Configurer l'impression de proximité** : l'impression de proximité est également fournie par le Serveur d'impression universelle Citrix, qui ne nécessite pas la configuration décrite ici.

1. Créez une stratégie distincte pour chaque sous-réseau (ou pour correspondre à l'emplacement de l'imprimante).
2. Dans chacune de ces stratégies, ajoutez les imprimantes de l'emplacement géographique de ce sous-réseau au paramètre Imprimantes de session.
3. Attribuez au paramètre Imprimante par défaut la valeur Ne pas ajuster l'imprimante par défaut de l'utilisateur.
4. Filtrez les stratégies par adresse IP cliente. Veillez à mettre à jour ces stratégies pour refléter les modifications apportées aux plages d'adresses IP DHCP.

## Gestion de l'environnement d'impression

June 27, 2024

La gestion de votre environnement d'impression comprend :

- Gestion des pilotes d'imprimante
- Optimisation des performances d'impression
- Affichage de l'imprimante et gestion des files d'attente d'impression

### Gestion des pilotes d'imprimantes

Pour réduire les coûts administratifs et les éventuels problèmes de pilote d'impression, Citrix vous recommande d'utiliser le pilote d'imprimante universelle Citrix.

Si la création automatique échoue, par défaut, le système installe un pilote d'imprimante natif Windows fourni avec Windows. Si un pilote n'est pas disponible, le système retourne au pilote d'impression universelle. Pour de plus amples informations sur les valeurs par défaut du pilote d'imprimante,

veuillez consulter la section Recommandations, considérations en matière de sécurité et opérations par défaut.

Si le pilote d'impression universelle Citrix n'est pas une option pour tous les scénarios, mappez les pilotes d'imprimante pour réduire la quantité de pilotes installés sur les machines avec OS multi-session. En outre, le mappage des pilotes d'imprimante vous permet de :

- autoriser les imprimantes spécifiques à utiliser uniquement les pilotes d'impression universelle Citrix ;
- autoriser ou empêcher la création d'imprimantes avec un pilote spécifique ;
- remplacer les pilotes d'imprimante appropriés par des pilotes altérés ou périmés ;
- remplacer un pilote disponible sur le serveur Windows par un nom de pilote client.

**Empêcher l'installation automatique des pilotes d'imprimante** : l'installation automatique de pilotes d'impression doit être désactivée pour assurer la cohérence entre les machines avec OS multi-session. Cela peut être assuré au travers des stratégies Citrix, Microsoft ou les deux. Pour empêcher l'installation automatique des pilotes d'imprimante natifs Windows, désactivez le paramètre de stratégie Citrix Installation automatique de pilotes d'imprimante fournis avec Windows.

**Mappage des pilotes d'imprimante des clients** : chaque client fournit des informations sur les imprimantes côté client au cours de l'ouverture de session, notamment le nom du pilote d'imprimante. Lors de la création automatique de l'imprimante client, le nom des pilotes d'imprimantes des serveurs Windows sont sélectionnés de manière à correspondre aux noms des modèles d'imprimante fournis par le client. Le processus de création automatique utilise ensuite les pilotes d'imprimantes identifiés et disponibles de manière à créer les files d'impression des clients redirigés.

Le processus général de définition des règles de remplacement de pilotes et de modification des paramètres d'impression pour les pilotes d'imprimantes clientes mappées est le suivant .

1. Pour spécifier les règles de remplacement des pilotes pour les imprimantes clientes créées automatiquement, configurez le paramètre de stratégie Citrix Mappage et compatibilité du pilote d'imprimante en ajoutant le nom du pilote d'imprimante cliente et en sélectionnant le pilote de serveur à utiliser à la place du pilote d'imprimante cliente dans le menu Rechercher un pilote d'imprimante. Vous pouvez utiliser des caractères génériques dans ce paramètre. Par exemple, pour obliger toutes les imprimantes HP à utiliser un pilote spécifique, spécifiez HP* dans le paramètre de stratégie.
2. Pour interdire un pilote d'imprimante, sélectionnez le nom de pilote et choisissez le paramètre Ne pas créer.
3. Le cas échéant, vous pouvez modifier un mappage existant, supprimer un mappage ou modifier l'ordre des entrées de pilote dans la liste.
4. Pour modifier les paramètres d'impression pour les pilotes d'imprimantes clientes mappées, sélectionnez le pilote d'imprimante, cliquez sur Paramètres, puis spécifiez les paramètres tels que la qualité d'impression, l'orientation et la couleur. Si vous spécifiez une option d'

impression que le pilote d'imprimante ne prend pas en charge, cette option n'a aucun effet. Ce paramètre écrase les paramètres d'imprimante définis par l'utilisateur durant une session précédente.

5. Citrix vous recommande de tester le comportement des imprimantes en détail après le mappage des pilotes, car certaines fonctionnalités d'imprimante peuvent être disponibles uniquement avec un pilote spécifique.

Lorsque les utilisateurs ouvrent une session, le système vérifie la liste de compatibilité des pilotes d'imprimantes clients avant de configurer les imprimantes clientes.

### Optimiser les performances d'impression

Pour optimiser les performances d'impression, utilisez le Serveur d'impression universelle et un pilote d'impression universelle. Les stratégies suivantes contrôlent l'optimisation et la compression de l'impression :

- Valeurs par défaut de l'optimisation de l'impression universelle. Spécifie les valeurs par défaut de l'imprimante universelle lorsqu'elle est créée pour une session :
  - Qualité d'image souhaitée spécifie la limite de compression d'image par défaut appliquée à l'impression universelle. Par défaut, Qualité standard est activée, signifiant que les utilisateurs peuvent uniquement imprimer des images à l'aide des compressions standard ou de qualité réduite.
  - Activer la compression lourde active ou désactive la réduction de la bande passante au-delà du niveau de compression défini par l'option Qualité d'image souhaitée, sans perte de qualité d'image. Par défaut, la compression intensive est désactivée.
  - Les paramètres Cache d'image et de police spécifient si oui ou non vous pouvez cacher des images et des polices qui s'affichent plusieurs fois dans le flux d'impression, assurant ainsi que chaque image ou police est envoyée à l'imprimante une seule fois. Par défaut, les images incorporées et les polices sont mises en cache.
  - Autoriser les non-administrateurs à modifier ces paramètres spécifie si les utilisateurs peuvent ou non modifier les paramètres d'optimisation d'impression dans une session. Par défaut, les utilisateurs ne sont pas autorisés à modifier les paramètres par défaut d'optimisation de l'impression.
- Limite de compression d'image de l'impression universelle. Définit la qualité maximale et le niveau de compression minimal disponibles pour les images imprimées avec le pilote d'imprimante universelle. Par défaut, la limite de compression d'image est définie sur Meilleure qualité (compression sans perte).
- Limite de qualité d'impression de l'impression universelle. Spécifie le nombre maximal de points par pouce (dpi) disponible pour l'impression dans la session. Par défaut, aucune limite n'est spécifiée.

Par défaut, toutes les tâches d'impression sont destinées à la route d'imprimantes réseau à partir de la machine avec OS multi-session, au travers du réseau, et directement vers le serveur d'impression. Envisagez le routage des tâches d'impression via la connexion ICA si le réseau possède une certaine latence ou une bande passante limitée. Pour ce faire, désactivez le paramètre de stratégie Citrix Connexions directes aux serveurs d'impression. Les données envoyées aux clients via la connexion ICA sont compressées. Les transmissions de données sur le réseau étendu nécessitent donc moins de bande passante.

**Améliorer les performances de session en limitant la bande passante d'impression** : lors de l'impression de fichiers depuis des machines avec OS multi-session vers les imprimantes utilisateur, il se peut que d'autres canaux virtuels (vidéo, par exemple) peuvent rencontrer une baisse des performances en raison de compétition de la bande passante, spécialement si les utilisateurs accèdent à des serveurs via des réseaux lents. Pour empêcher ce type de dégradation, vous pouvez limiter la bande passante utilisée par l'impression cliente. En limitant la vitesse de transfert des données d'impression, vous pouvez augmenter la bande passante disponible dans le flux de données HDX pour le transfert des données vidéo et des informations relatives aux frappes clavier et aux clics de souris.

> **Important :**
>
> Si une limite de bande passante d'impression est définie, elle est respectée même lorsqu'aucun autre canal n'est utilisé.

Utilisez les paramètres d'imprimante de la stratégie Citrix Bande passante pour configurer les limites de session de bande passante d'impression. Pour définir les limites pour le site, réalisez cette tâche à l'aide de Studio. Pour définir les limites pour des serveurs individuels, effectuez cette tâche à l'aide de la console de gestion des stratégies de groupe dans Windows localement sur chaque machine avec OS multi-session.

- Le paramètre Limite de bande passante de redirection d'imprimante permet de spécifier la bande passante en kilobits par seconde (kbps) disponible pour l'impression.
- Le paramètre Pourcentage de limite de bande passante de redirection de l'imprimante permet de limiter la bande passante disponible pour l'impression à un pourcentage de la bande passante générale disponible.

  Remarque : pour spécifier la bande passante sous forme de pourcentage à l'aide du paramètre Pourcentage de limite de bande passante de redirection de l'imprimante, activez également le paramètre Limite de bande passante de session générale.

  Si vous entrez des valeurs pour les deux paramètres, le paramètre le plus restrictif (ayant la valeur la plus faible) est appliqué.

Pour obtenir des informations en temps réel sur la bande passante d'impression, utilisez Citrix Director.

### Équilibrer la charge des serveurs d'impression universelle

La solution de serveur d'impression universelle peut monter en charge en ajoutant davantage de serveurs d'impression dans la solution d'équilibrage de charge. Il n'existe aucun point de défaillance unique car chaque VDA dispose de son propre équilibreur de charge pour répartir la charge d'impression auprès de tous les serveurs d'impression.

Utilisez les paramètres de stratégie, Serveurs d'impression universelle d'équilibrage de la charge et Seuil au-delà duquel les serveurs d'impression universelle sont hors service, pour répartir la charge de l'impression auprès de tous les serveurs d'impression dans la solution d'équilibrage de charge.

En cas de défaillance imprévue d'un serveur d'impression, le mécanisme de basculement de l'équilibreur de charge de chaque VDA répartit automatiquement les connexions d'imprimantes attribuées aux serveurs d'impression défaillants aux autres serveurs d'impression disponibles de façon à ce que toutes les sessions existantes et entrantes fonctionnent normalement sans affecter l'expérience de l'utilisateur et sans nécessiter l'intervention immédiate de l'administrateur.

Les administrateurs peuvent surveiller l'activité des serveurs d'impression d'équilibrage de charge à l'aide d'un ensemble de compteurs de performances pour suivre les indicateurs suivants sur le VDA :

- Liste des serveurs d'impression dont la charge est équilibrée sur le VDA et leur état (disponible, indisponible)
- Nombre de connexions d'imprimantes acceptées par chaque serveur d'impression
- Nombre d'échecs de connexions d'imprimantes sur chaque serveur d'impression
- Nombre de connexions d'imprimantes actives sur chaque serveur d'impression
- Nombre de connexions d'imprimantes en attente sur chaque serveur d'impression

### Afficher et gérer les files d'attente d'impression

Le tableau suivant récapitule l'emplacement d'affichage des imprimantes et de gestion des files d'attente dans votre environnement.

| | | Piste d'impression |
|---|---|---|
| Imprimantes clientes (imprimantes connectées à la machine utilisateur) | Piste d'impression cliente | UAC activé : Composant logiciel enfichable Gestion d'impression dans la console Microsoft Management Console ; UAC désactivé : Pré-Windows 8 : Panneau de configuration, Windows 8 : Composant logiciel enfichable Gestion de l'impression |
| Imprimantes réseau (Imprimantes sur un serveur d'impression réseau) | Piste d'impression réseau | UAC activé : Serveur d'impression > Composant logiciel enfichable Gestion de l'impression dans la console Microsoft Management Console ; UAC désactivé : Serveur d'impression > Panneau de configuration |
| Imprimantes réseau (Imprimantes sur un serveur d'impression réseau) | Piste d'impression cliente | UAC activé : Serveur d'impression > Composant logiciel enfichable Gestion d'impression dans la console Microsoft Management Console ; UAC désactivé : Pré-Windows 8 : Panneau de configuration, Windows 8 : Composant logiciel enfichable Gestion de l'impression |
| Imprimantes serveur réseau locales (Imprimantes d'un serveur d'impression réseau qui sont ajoutées à une machine avec OS multi-session) | Piste d'impression réseau | UAC activé : Serveur d'impression > Panneau de configuration ; UAC désactivé : Serveur d'impression > Panneau de configuration |

> **Remarque :**
>
> Les files d'attente d'impression des imprimantes réseau utilisant la piste d'impression réseau

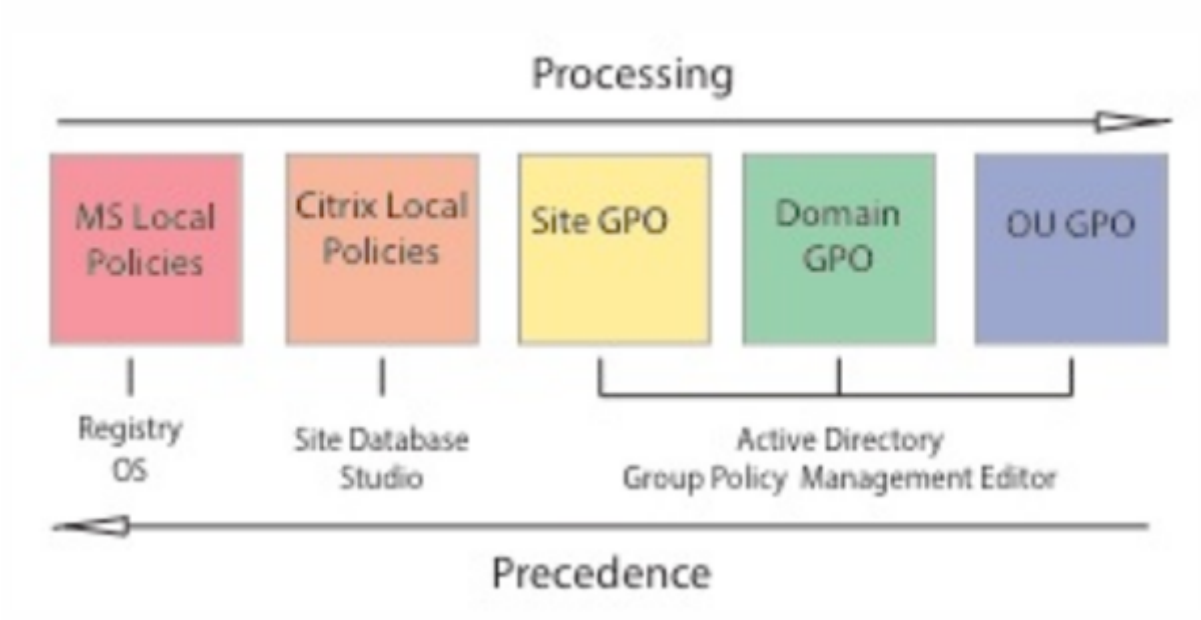
> sont privées et ne peuvent être gérées au travers du système.

## Stratégies

June 27, 2024

Les stratégies sont un ensemble de paramètres qui définissent la façon dont les sessions, la bande passante et la sécurité sont gérées pour un groupe d'utilisateurs, de machines, ou de types de connexion.

Vous pouvez appliquer des paramètres de stratégie à des machines physiques et virtuelles ou à des utilisateurs. Vous pouvez appliquer des paramètres à des utilisateurs individuels au niveau local ou dans les groupes de sécurité dans Active Directory. Les configurations définissent des critères et des règles spécifiques. Si vous n'attribuez pas spécifiquement les stratégies, les paramètres sont appliqués à toutes les connexions.




Vous pouvez appliquer des stratégies sur différents niveaux du réseau. Les paramètres de stratégie placés au niveau de l'objet de stratégie de groupe de l'unité d'organisation prennent la plus haute priorité sur le réseau. Les stratégies au niveau de l'objet de stratégie de groupe de domaine remplacent les stratégies au niveau de l'objet de stratégie de groupe du site. Le niveau de l'objet de stratégie de groupe de sites remplace les stratégies en conflit sur les deux niveaux Microsoft et Stratégies locales Citrix.

Toutes les stratégies locales Citrix sont créées et gérées dans la console Web Studio et stockées dans la base de données du site. Les stratégies de groupe sont créées et gérées à l'aide de la console de

gestion des stratégies de groupe Microsoft (GPMC) et stockées dans Active Directory. Les stratégies locales Microsoft sont créées dans le système d'exploitation Windows et sont stockées dans le Registre.

Studio utilise un assistant de modélisation pour aider les administrateurs à comparer les paramètres de configuration dans les modèles et stratégies pour vous aider à éliminer tout paramètre en conflit ou redondant. Les administrateurs peuvent définir des objets de stratégie de groupe en utilisant la console GPMC pour configurer les paramètres. Vous pouvez également les appliquer à un ensemble cible d'utilisateurs à différents niveaux du réseau.

Ces objets de stratégie de groupe sont enregistrés dans Active Directory. L'accès à l'administration de ces paramètres est limité pour la plupart des services informatiques pour des raisons de sécurité.

Les paramètres sont fusionnés selon leur priorité et leur condition. Tout paramètre désactivé remplace un paramètre d'une priorité plus faible activé. Tout paramètre de stratégie non configuré est ignoré et ne remplace pas les paramètres de priorité inférieure.

Les stratégies locales peuvent également être en conflit avec des stratégies de groupe dans Active Directory, qui peuvent se remplacer entre elles, selon le cas.

Toutes les stratégies sont traitées dans l'ordre suivant :

1. L'utilisateur ouvre une session sur une machine à l'aide des informations d'identification de domaine.
2. Les informations d'identification sont envoyées au contrôleur de domaine.
3. Active Directory applique toutes les stratégies (utilisateur final, point de terminaison, unité d'organisation et domaine).
4. L'utilisateur ouvre une session sur l'application Citrix Workspace et accède à une application ou à un bureau.
5. Citrix et les stratégies Microsoft sont traitées pour l'utilisateur et la machine qui héberge la ressource.
6. Active Directory détermine la priorité pour les paramètres de stratégie. Il les applique ensuite aux registres de la machine de point de terminaison et à la machine hébergeant la ressource.
7. L'utilisateur ferme sa session sur la ressource. Les stratégies Citrix pour l'utilisateur et la machine de point de terminaison ne sont plus actives.
8. L'utilisateur ferme sa session sur la machine utilisateur, ce qui libère les stratégies utilisateur de l'objet de stratégie de groupe.
9. L'utilisateur éteint le périphérique, ce qui libère les stratégies de machine de l'objet de stratégie de groupe.

Lorsque vous créez des stratégies pour des groupes d'utilisateurs, des périphériques et des machines, certains membres peuvent avoir différents besoins et auraient besoin d'exceptions à certains paramètres de stratégie. Les exceptions sont effectuées via des filtres dans Studio et le GPMC qui déterminent ce qui est affecté par la stratégie.

> **Remarque :**
>
> Nous ne prenons pas en charge le mélange de stratégies Windows et Citrix dans le même objet de stratégie de groupe.

# Utiliser les stratégies

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Configurez des stratégies Citrix pour contrôler l'accès utilisateur ou les environnements de session. Les stratégies Citrix constituent la méthode la plus efficace pour contrôler les paramètres de connexion, de sécurité et de bande passante. Vous pouvez créer des stratégies relatives à des groupes d'utilisateurs, des machines ou des types de connexion spécifiques. Chaque stratégie peut contenir plusieurs paramètres.

## Outils pour l'utilisation de stratégies Citrix

Vous pouvez utiliser les outils suivants avec les stratégies Citrix.

- **Web Studio.** Si vous êtes un administrateur Citrix ne disposant pas d'autorisations pour gérer la stratégie de groupe, utilisez Web Studio pour créer des stratégies pour votre site. Les stratégies créées avec Web Studio sont enregistrées dans la base de données du site et les mises à jour sont déployées vers le VDA soit lorsque celui-ci s'enregistre auprès du broker, soit lorsque l'utilisateur se connecte à ce VDA.
- **Éditeur de stratégie de groupe local** (composant logiciel enfichable de la console Microsoft Management Console). Si votre environnement réseau utilise Active Directory et que vous avez l'autorisation de gérer la stratégie de groupe, vous pouvez utiliser l'éditeur de stratégie de groupe local pour créer des stratégies pour votre site. Les paramètres que vous configurez affectent les objets de stratégie de groupe que vous spécifiez via la console de gestion des stratégies de groupe.

> **Important :**
>
> Nous vous recommandons d'utiliser l'Éditeur de stratégie de groupe local pour configurer certains paramètres de stratégie, par exemple, les paramètres liés à l'enregistrement de VDA auprès d'un contrôleur et les paramètres liés aux serveurs Microsoft App-V.
> Des validations de stratégie supplémentaires sont ajoutées. Par conséquent, une mise à niveau sur place peut entraîner la perte de données de stratégie si des paramètres de stratégie non valides sont présents. Si vous créez ou modifiez les stratégies à l'aide d'une méthode autre que Web Studio, Citrix vous recommande d'utiliser la dernière version du SDK et du composant logiciel enfichable.

## Ordre de traitement et priorité des stratégies

Les paramètres de stratégie de groupe sont traités dans l'ordre suivant :

1. GPO local
2. GPO du site Virtual Apps and Desktops (stocké dans la base de données du site)
3. GPO au niveau du site
4. GPO au niveau du domaine
5. Unités d'organisation

Toutefois, en cas de conflit, les paramètres de stratégie traités en dernier remplacent les paramètres traités en premier. L'ordre de priorité des paramètres de stratégie est le suivant :

1. Unités d'organisation
2. GPO au niveau du domaine
3. GPO au niveau du site
4. GPO du site Virtual Apps and Desktops (stocké dans la base de données du site)
5. GPO local

Par exemple, un administrateur Citrix utilise Web Studio pour créer une stratégie (Stratégie A) qui active la redirection de fichier client pour les employés du département Ventes de l'entreprise. Pendant ce temps, un autre administrateur utilise l'éditeur de stratégie de groupe pour créer une stratégie (Stratégie B) qui désactive la redirection de fichier client pour les employés des ventes. Lorsque les commerciaux se connectent aux bureaux virtuels, la stratégie B est appliquée et la stratégie A est ignorée. La raison en est que la stratégie B a été traitée au niveau du domaine et que la stratégie A a été traitée au niveau de l'objet de stratégie de groupe du site Virtual Apps and Desktops.

Toutefois lorsqu'un utilisateur lance une session ICA ou RDP (Protocole Bureau à distance), les paramètres de la session Citrix remplacent les mêmes paramètres configurés dans une stratégie Active Directory ou à l'aide de la Configuration d'hôte de session Bureau à distance. Ceci comprend les paramètres liés aux paramètres de connexion client RDP standard. Les exemples de paramètres

de connexion client RDP sont Papier peint du bureau, Animation de menu et Afficher le contenu de la fenêtre lors d'un cliquer déplacer.

Lors de l'utilisation de plusieurs stratégies, vous pouvez établir des priorités pour les stratégies qui contiennent des paramètres conflictuels. Pour plus d'informations, consultez la section Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies.

### Flux de travail des stratégies Citrix

Le processus de configuration des stratégies est le suivant :

1. Créez la stratégie.
2. Configurez les paramètres de stratégie.
3. Affectez la stratégie aux objets machine et utilisateur.
4. Définissez l'ordre de priorité de la stratégie.
5. Vérifiez la stratégie effective en exécutant l'assistant Modélisation de stratégie de groupe Citrix.

> **Remarque :**
>
> Pour ouvrir l'assistant de modélisation de stratégie de groupe Citrix, accédez à l'onglet **Stratégies > Modélisation**, puis cliquez sur **Démarrer l'assistant de modélisation** dans la barre d'actions. L'onglet **Modélisation** est disponible dans Web Studio à la demande du client.

### Naviguer vers les stratégies et paramètres Citrix

Dans l'éditeur de stratégie de groupe local, les stratégies et les paramètres apparaissent dans deux catégories : Configuration ordinateur et Configuration utilisateur. Chaque catégorie a un nœud Stratégies Citrix. Consultez la documentation Microsoft pour plus de détails sur la navigation et l'utilisation de ce composant logiciel enfichable.

Dans Web Studio, les paramètres de stratégie sont triés dans des catégories en fonction de la fonctionnalité ou fonction qu'ils affectent. Par exemple, la section **Profile Management** contient des paramètres de stratégie pour Profile Management.

- Les paramètres Ordinateur (paramètres de stratégie s'appliquant aux machines) définissent le comportement des bureaux virtuels et sont appliqués lorsqu'un bureau virtuel démarre. Ces paramètres s'appliquent même s'il n'y a pas de session utilisateur active sur le bureau virtuel.
- Les paramètres utilisateur définissent l'expérience de l'utilisateur lors de la connexion à l'aide du protocole ICA. Les stratégies utilisateur sont appliquées lorsqu'un utilisateur se connecte ou

se reconnecte à l'aide du protocole ICA. Les stratégies utilisateur ne sont pas appliquées si un utilisateur se connecte à l'aide de RDP ou ouvre une session directement sur la console.

Pour accéder aux stratégies, paramètres ou modèles, sélectionnez **Stratégies** dans le panneau gauche de Web Studio.

- L'onglet **Stratégies** répertorie toutes les stratégies. Lorsque vous sélectionnez une stratégie, les onglets ci-dessous s'affichent en bas :
  - Aperçu : nom, priorité, statut activé/désactivé et description
  - Paramètres : liste de tous les paramètres configurés
  - Attribué à : objets utilisateur et machine auxquels la stratégie est affectée.
    Pour de plus amples informations, consultez la section Créer des stratégies.
- L'onglet **Modèles** répertorie des modèles fournis par Citrix et personnalisés que vous avez créés. Lorsque vous sélectionnez un modèle, les onglets ci-dessous s'affichent en bas :
  - Description (fonction du modèle)
  - Paramètres (liste des paramètres configurés). Pour plus d'informations, veuillez consulter la section Modèles de stratégie.
- L'onglet **Comparaison** vous permet de comparer les paramètres d'une stratégie ou d'un modèle avec ceux des autres stratégies ou modèles. Par exemple, il se peut que vous souhaitiez vérifier les valeurs des paramètres pour assurer la compatibilité avec les meilleures pratiques. Pour plus d'informations, consultez la section Comparer, donner un ordre de priorité, modéliser et résoudre les problèmes des stratégies.

Pour rechercher un paramètre dans une stratégie ou un modèle :

1. Sélectionnez la stratégie ou le modèle.
2. Sélectionnez **Modifier la stratégie** ou **Modifier le modèle** dans la barre d'actions.
3. Sur la page **Paramètres**, saisissez le nom du paramètre dans le champ de **recherche** :

   Vous pouvez affiner votre recherche en sélectionnant :

   - Une version spécifique du produit
   - Une catégorie (par exemple, Bande passante)
   - Des mots clés dans le nom du paramètre
   - La case à cocher **Afficher sélectionné uniquement**
   - Pour rechercher uniquement les paramètres qui ont été ajoutés à la stratégie sélectionnée.

Pour une recherche non filtrée, sélectionnez **Tous les paramètres**.

- Pour rechercher un paramètre dans une stratégie :

  1. Sélectionnez la stratégie.

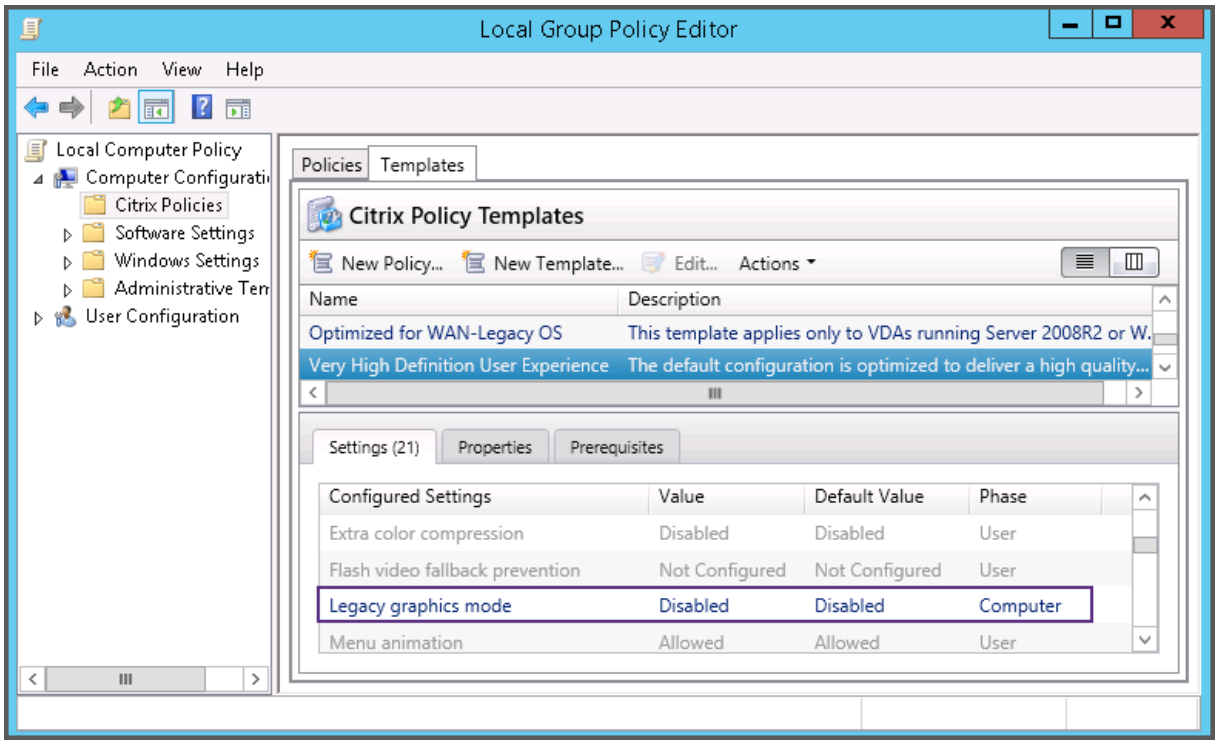
2. Sélectionnez l'onglet **Paramètres** et tapez le nom du paramètre.

Vous pouvez affiner votre recherche en sélectionnant une version spécifique du produit ou en sélectionnant une catégorie. Pour une recherche non filtrée, sélectionnez **Tous les paramètres**.

Une stratégie, une fois qu'elle a été créée, est indépendante du modèle utilisé. Vous pouvez utiliser le champ **Description** d'une nouvelle stratégie pour le suivi de la source modèle utilisé.

Dans l'éditeur de stratégie de groupe, les paramètres ordinateur et utilisateur doivent être appliqués séparément, même s'ils ont été créés à partir d'un modèle qui contient les deux types de paramètres. Dans cet exemple, vous choisissez d'utiliser le paramètre Expérience utilisateur très haute définition dans Configuration ordinateur :

- Le Mode graphique d'ancienne génération est un paramètre Ordinateur qui est utilisé dans une stratégie créée à partir de ce modèle.
- Les paramètres Utilisateur, grisés, ne sont pas utilisés dans une stratégie créée à partir de ce modèle.




## Modèles de stratégie

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Les modèles sont des ensembles de paramètres qu'il est recommandé d'utiliser pour créer des stratégies visant à obtenir des résultats spécifiques. Par exemple, les paramètres définis dans le modèle "Expérience utilisateur en très haute définition"peuvent être utilisés comme référence et point de départ pour la création de stratégies permettant de fournir une expérience utilisateur en très haute définition.

Les modèles ne sont pas des stratégies. Les modèles constituent une documentation supplémentaire pour les paramètres de stratégie Citrix. Ils présentent les fonctionnalités collectives de certains paramètres liés aux utilisateurs.

L'utilisation d'un modèle est facultative. Les administrateurs peuvent créer des stratégies sans utiliser de modèles. Les modèles sont utiles pour les administrateurs qui ont une idée générale de la manière dont un site doit être configuré, mais qui ne savent pas quels paramètres utiliser pour obtenir la configuration souhaitée.

Les administrateurs peuvent créer des modèles à l'aide d'un modèle existant ou d'une stratégie existante ou en partant de zéro.

### ADMX/ADML

Les modèles de stratégie de groupe Citrix décrits ici n'ont rien à voir avec les modèles de stratégie Windows. Les modèles décrits ici et les modèles de stratégie Windows sont deux concepts différents. Les modèles de stratégie de groupe Citrix ne sont pas des fichiers ADMX.

## Modèles Citrix incorporés

Les modèles de stratégie suivants sont disponibles :

- **Expérience utilisateur très haute définition**. Ce modèle applique les paramètres par défaut ce qui optimise l'expérience utilisateur. Utilisez ce modèle dans les scénarios dans lesquels plusieurs stratégies sont traitées par ordre de priorité.
- **Montée en charge du serveur élevée**. Appliquez ce modèle pour économiser les ressources du serveur. Ce modèle assure un excellent compromis entre expérience utilisateur et montée en charge du serveur. Il offre une expérience utilisateur des plus satisfaisantes tout en augmentant le nombre d'utilisateurs que vous pouvez héberger sur un seul serveur. Ce modèle n'utilise pas

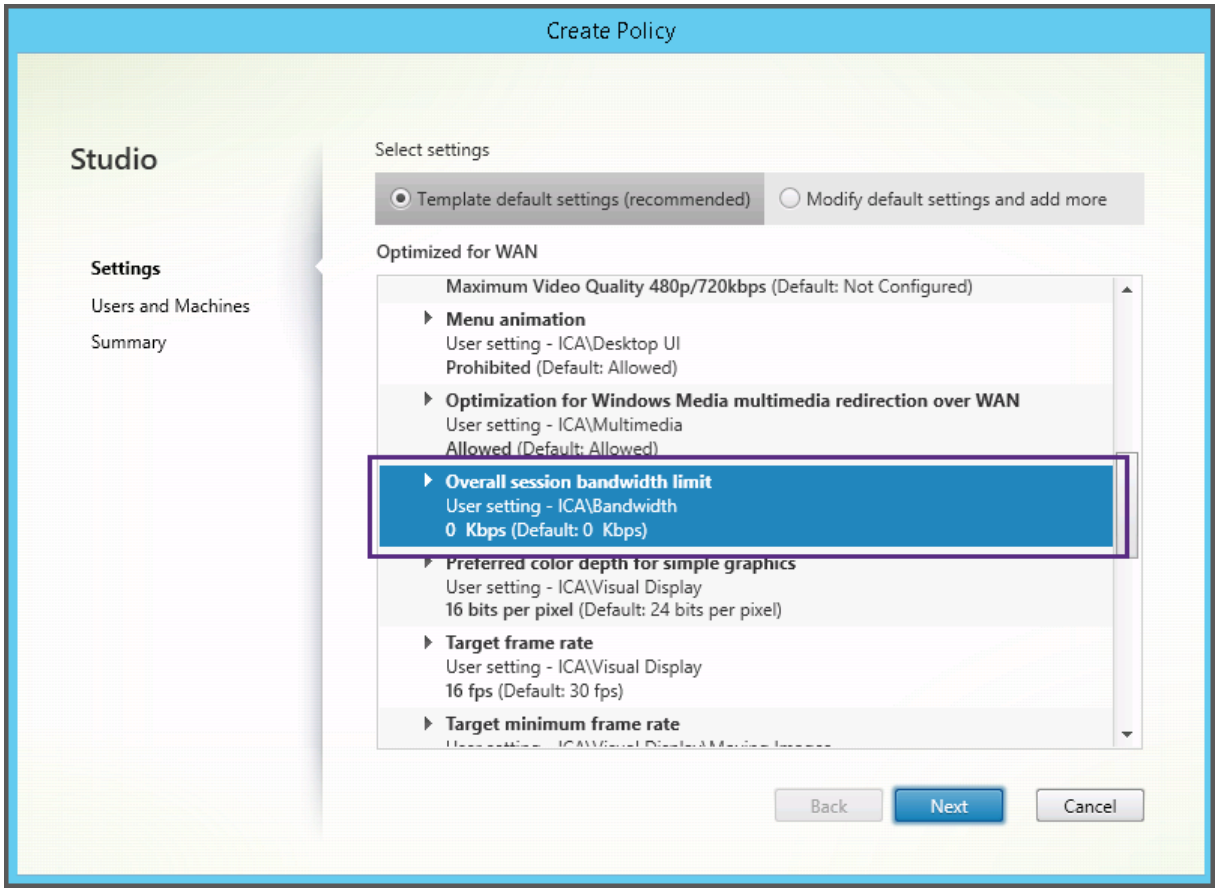
 

un codec vidéo pour la compression de graphiques et empêche la génération de multimédia côté serveur.

- **Montée en charge du serveur élevée - anciens systèmes d'exploitation**. Ce modèle de montée en charge du serveur élevée s'applique uniquement aux VDA exécutant Windows Server 2008 R2 ou Windows 7 et versions antérieures. Ce modèle s'appuie sur le Mode graphique d'ancienne génération qui est plus efficace pour ces systèmes d'exploitation.
- **Optimisé pour NetScaler SD-WAN.** Appliquez ce modèle pour les utilisateurs qui travaillent depuis des succursales avec NetScaler SD-WAN pour optimiser la mise à disposition de Citrix Virtual Desktops. (NetScaler SD-WAN est la nouvelle appellation de CloudBridge).
- **Optimisé pour les connexions WAN**. Ce modèle est conçu pour les utilisateurs qui travaillent dans des succursales (connexions WAN partagées) ou depuis des sites distants utilisant des connexions à faible bande passante qui accèdent à des applications dotées d'interfaces graphiques simples et contenant très peu de contenu multimédia. Ce modèle optimise l'efficacité de la bande passante au détriment de l'expérience de lecture vidéo et de la montée en charge du serveur.
- **Optimisé pour les connexions WAN –anciens systèmes d'exploitation**. Le modèle *Optimisé pour les connexions WAN* s'applique uniquement aux VDA exécutant Windows Server 2008 R2 ou Windows 7 et versions antérieures. Ce modèle s'appuie sur le Mode graphique d'ancienne génération qui est plus efficace pour ces systèmes d'exploitation.
- **Sécurité et contrôle**. Utilisez ce modèle dans les environnements dans lesquels la tolérance aux risques est faible, de façon à limiter les fonctionnalités activées par défaut dans Citrix Virtual Apps and Desktops. Ce modèle contient des paramètres qui désactivent l'accès à l'impression, au Presse-papiers, aux périphériques, au mappage de lecteurs, à la redirection de port et à l'accélération Flash sur les machines utilisateur. L'application de ce modèle peut consommer plus de bande passante et réduire le nombre d'utilisateurs par serveur.

Bien que nous recommandions d'utiliser les modèles Citrix intégrés avec leurs paramètres par défaut, il existe des paramètres pour lesquels aucune valeur spécifique n'a été recommandée. Par exemple, **Limite de bande passante de session générale**, qui est inclus aux modèles Optimisé pour les connexions WAN. Dans ce cas, le modèle expose le paramètre de façon à faire comprendre à l'administrateur que ce paramètre est susceptible de s'appliquer au scénario.




Si vous travaillez avec un déploiement (gestion de la stratégie et VDA) antérieur à XenApp et XenDesktop 7.6 FP3, et avez besoin de modèles Montée en charge du serveur élevée et Optimisé pour les connexions WAN, utilisez les anciennes versions de systèmes d'exploitation de ces modèles lorsqu'ils s'appliquent.

> **Remarque :**
>
> Citrix crée des modèles incorporés et les met à jour. vous ne pouvez ni modifier ni supprimer ces modèles.

### Créer et gérer des modèles à l'aide de Web Studio

Pour créer un modèle à partir d'un autre modèle :

1. Connectez-vous à Web Studio et sélectionnez **Stratégies** dans le volet de gauche.
2. Sélectionnez l'onglet **Modèles**, puis sélectionnez le modèle depuis lequel vous souhaitez créer le nouveau modèle.
3. Sélectionnez l'onglet **Créer un modèle**. L'écran **Sélectionner les paramètres** s'affiche.
4. Sélectionnez et configurez les paramètres de stratégie que vous souhaitez inclure dans le modèle.

5. Cliquez sur **Suivant**. L'écran **Résumé** s'affiche.
6. Entrez un nom pour le modèle.
7. Cliquez sur **Terminer**. Le nouveau modèle apparaît dans l'onglet **Modèles**.

Pour créer un modèle à partir d'une stratégie :

1. Connectez-vous à Web Studio et sélectionnez **Stratégies** dans le volet de gauche.
2. Sélectionnez l'onglet **Stratégies**, puis sélectionnez la stratégie à partir de laquelle vous souhaitez créer le modèle.
3. Cliquez sur l'onglet **Plus**.
4. Sélectionnez **Enregistrer comme modèle**. L'écran **Sélectionner les paramètres** s'affiche.
5. Sélectionnez et configurez tout nouveau paramètre de stratégie que vous souhaitez inclure dans le modèle.
6. Cliquez sur **Suivant**. L'écran **Résumé** s'affiche.
7. Entrez un nom et une description pour le modèle, puis cliquez sur **Terminer**.

### Modèles et Administration déléguée

Les modèles Web Studio sont stockés dans la base de données du site, contrairement aux modèles de Citrix Studio, qui sont stockés sous forme de fichiers dans le dossier de profil utilisateur de l'administrateur actuel avec une extension `.gpt`. Les modèles Citrix Studio créés par un administrateur ne sont pas visibles pour les autres administrateurs ou pour le même administrateur sur une machine différente. Les modèles Web Studio, quant à eux, sont visibles par tous les administrateurs soumis à des autorisations et à une administration déléguée.

## Créer des stratégies

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Avant de créer une stratégie, déterminez quel groupe d'utilisateurs ou de périphériques peut être affecté par celle-ci. Il se peut que vous souhaitiez créer une stratégie basée sur la fonction de l'utilisateur, son type de connexion, sa machine utilisateur ou son emplacement géographique. Vous pouvez

aussi utiliser le même critère que vous utilisez pour les stratégies de groupe Windows Active Directory.

Si vous avez déjà créé une stratégie qui s'applique à un groupe, envisagez de modifier cette stratégie au lieu d'en créer une autre. Après avoir modifié la stratégie, configurez les paramètres appropriés. Évitez de créer une stratégie uniquement pour activer un paramètre spécifique ou pour exclure certains utilisateurs de l'application de la stratégie.

Lorsque vous créez une stratégie, vous pouvez la baser sur les paramètres d'un modèle de stratégie et personnaliser les paramètres selon vos besoins. Vous pouvez la créer, sans utiliser de modèle et ajouter tous les paramètres nécessaires.

Dans Web Studio, les nouvelles stratégies créées sont définies sur Désactivé, sauf si la case à cocher **Activer la stratégie** est explicitement sélectionnée.

Lors de la création de la stratégie et de la configuration des paramètres, le système propose une option permettant d'afficher le type de paramètres. Vous pouvez consulter le type de paramètres suivant :

- Tous les paramètres - Afficher tous les paramètres applicables à toutes les versions de VDA
- Paramètres actuels uniquement : affiche les paramètres spécifiques à la version actuelle du VDA
- Paramètres d'ancienne génération uniquement : affiche uniquement les paramètres pour les versions de VDA obsolètes

Pour afficher les paramètres lors de leur configuration, procédez comme suit :

1. Connectez-vous à Web Studio et sélectionnez **Stratégies** dans le volet de gauche.
2. Dans l'onglet **Stratégies**, cliquez sur **Créer une stratégie**.
3. Dans le tableau **Sélectionner les paramètres**, cliquez sur le menu déroulant situé à côté de **Paramètres**.
4. Sélectionnez l'une des options suivantes dans le menu déroulant :

- Tous les paramètres : affiche tous les paramètres pour toutes les versions de VDA
- Paramètres actuels uniquement : affiche uniquement les paramètres pour les versions actuelles de VDA
- Paramètres d'ancienne génération uniquement : affiche uniquement les paramètres pour les versions de VDA obsolètes

1. Le tableau **Paramètres** répertorie les paramètres disponibles en fonction de l'étape précédente.

## Paramètres de stratégie

Les paramètres de stratégie peuvent être activés, désactivés ou non configurés. Par défaut, les paramètres de stratégie ne sont pas configurés, c'est-à-dire qu'ils ne sont pas ajoutés à une stratégie. Les paramètres ne sont appliqués que lorsqu'ils sont ajoutés à une stratégie.

Les paramètres de stratégie peuvent affichés l'un des états suivants :

- Autorisé ou Interdit permet ou empêche l'action contrôlée par le paramètre. Dans certains cas, les utilisateurs sont autorisés ou non à gérer l'action du paramètre dans la session. Par exemple, si le paramètre Animation de menu est défini sur Autorisé, les utilisateurs peuvent contrôler les animations de menu dans leur environnement client.
- Activé ou Désactivé active ou désactive le paramètre. Si vous désactivez un paramètre, celui-ci n'est pas activé dans les stratégies de priorité inférieure.

De plus, certains paramètres contrôlent l'efficacité des paramètres dépendants. Par exemple, Redirection de lecteur client contrôle le fait que les utilisateurs sont autorisés ou non à accéder aux lecteurs de leurs machines. Ce paramètre ainsi que le paramètre **Lecteurs réseau clients** doivent être ajoutés à la stratégie pour permettre aux utilisateurs d'accéder à leurs lecteurs réseau. Si le paramètre **Redirection de lecteur client** est désactivé, les utilisateurs ne pourront pas accéder à leurs lecteurs réseau même si le paramètre **Lecteurs réseau clients** est activé.

En général, les modifications apportées au paramètre de stratégie qui affectent les machines se produisent lorsque le bureau virtuel redémarre ou lorsqu'un utilisateur ouvre une session. Les modifications apportées au paramètre de stratégie qui affectent les utilisateurs se produisent la prochaine fois que les utilisateurs ouvrent une session. Si vous utilisez Active Directory, les paramètres de stratégie sont mis à jour lorsque Active Directory réévalue les stratégies à intervalles de 90 minutes. Les paramètres de stratégie sont appliqués lorsque le bureau virtuel redémarre ou qu'un utilisateur ouvre une session.

Pour certains paramètres de stratégie, vous pouvez entrer ou sélectionner une valeur lorsque vous ajoutez ce paramètre à une stratégie. Vous pouvez limiter la configuration du paramètre en sélectionnant Utiliser la valeur par défaut. Cette sélection désactive la configuration du paramètre et permet uniquement à la valeur par défaut du paramètre d'être utilisée lorsque la stratégie est appliquée. Cette sélection est indépendante de la valeur entrée avant la sélection de l'option Utiliser la valeur par défaut.

Si le paramètre sécurisé par défaut est activé, la priorité des paramètres de stratégie est affectée comme suit lors de l'installation du VDA :

- Le paramètre personnalisé est prioritaire
- Le paramètre sécurisé par défaut prend la deuxième priorité
- Le paramètre par défaut est le moins prioritaire

Pour voir le paramètre de sécurité par défaut d'une stratégie, procédez comme suit :

1. Connectez-vous à Web Studio.
2. Dans la barre de navigation de gauche, cliquez sur **Stratégies**.
3. Dans l'onglet **Stratégies**, cliquez sur **Créer une stratégie**.

4. Dans le tableau **Sélectionner les paramètres**, lorsque vous survolez les paramètres définis actuellement sur **Autorisé ?**, la **valeur sécurisée par défaut : Interdit** s'affiche.

   Paramètre de sécurité par défaut

Recommandations :

- Attribuez des stratégies aux groupes plutôt qu'aux utilisateurs individuels. Si vous attribuez des stratégies aux groupes, les attributions seront mises à jour automatiquement lorsque vous ajouterez des utilisateurs au groupe ou en supprimerez.
- N'activez pas les paramètres de conflit ou de chevauchement dans la configuration d'hôte de session Bureau à distance. Parfois, la configuration d'hôte de session Bureau à distance offre une fonctionnalité similaire pour les paramètres de stratégie Citrix. Chaque fois que possible, maintenez la cohérence de tous les paramètres (activés ou désactivés) pour faciliter la résolution des problèmes.
- Désactivez les stratégies non utilisées. Les stratégies sans paramètres ajoutés génèrent un traitement inutile.

### Attributions de stratégie

Lors de la création d'une stratégie, vous l'affectez à certains objets utilisateur et ordinateur. Cette stratégie est appliquée aux connexions selon des critères ou des règles spécifiques. En général, vous pouvez ajouter à une stratégie autant d'attributions que vous le souhaitez, selon une combinaison de critères.

Si vous ne spécifiez aucune attribution ou si vous spécifiez des attributions mais que vous les désactivez, la stratégie s'applique à **toutes** les connexions.

> **Remarque :**
>
> Les attributions de stratégies sont également appelées filtres de stratégie. Pour plus d'informations, consultez les rubriques suivantes :
>
> - Créer, modifier ou supprimer un filtre de stratégie
> - Comment les filtres sont-ils appliqués ?

Le tableau suivant répertorie les attributions disponibles :

| Nom de l'attribution | Applique une stratégie basée sur |
| --- | --- |
| Contrôle d'accès | Conditions de contrôle d'accès au travers desquelles un client se connecte. *Type de connexion :* si vous souhaitez appliquer la stratégie aux connexions établies avec ou sans NetScaler Gateway. *Nom de batterie NetScaler Gateway :* nom du serveur virtuel NetScaler Gateway. *Condition d'accès :* nom de la stratégie d'analyse de point de terminaison ou de session à utiliser. |
| NetScaler SD-WAN | Indique si une session utilisateur est lancée via NetScaler SD-WAN. **Remarque :** vous pouvez ajouter une seule attribution NetScaler SD-WAN à une stratégie. |
| Adresse IP cliente | Adresse IP de la machine utilisateur utilisée pour se connecter à la session : Exemples IPv4 : 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24 ; Exemples IPv6 : 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54 |
| Nom du client | Nom de la machine utilisateur. Concordance exacte : ClientABCName. Utilisation du caractère générique : Client*Name. |
| Groupe de mise à disposition | Appartenance à un groupe de mise à disposition. |
| Type de groupe de mise à disposition | Type de bureau ou d'application : bureau privé, bureau partagé, application privée ou application partagée. **Remarque :** les options de filtre de bureau privé et de bureau partagé ne sont disponibles que pour Citrix Virtual Apps and Desktops 7.x. Pour plus d'informations, consultez la section CTX219153. |
| Unité d'organisation (UO) | Unité d'organisation. |
| Balise | Balises. **Remarque :** appliquez cette stratégie à toutes les machines balisées. Les balises d'application ne sont pas incluses. |
| Utilisateur ou groupe | Nom d'utilisateur ou de groupe. |

Lorsque les utilisateurs ouvrent une session, toutes les stratégies correspondant aux attributions pour la connexion sont identifiées. Les stratégies sont triées dans un ordre de priorité et plusieurs instances de tous les paramètres sont comparées. Chaque paramètre est appliqué selon l'ordre de priorité de la stratégie. Un paramètre de stratégie qui est désactivé prévaut sur un paramètre activé doté d'une priorité plus faible. Les paramètres de stratégie qui ne sont pas configurés sont ignorés.

> **Important :**
>
> Lorsque vous configurez les stratégies Active Directory et Citrix avec la Console de gestion des stratégies de groupe, il est possible que les filtres et les paramètres ne soient pas appliqués comme prévu. Pour obtenir davantage d'informations, veuillez consulter l'article CTX127461.

Une stratégie appelée « Non filtrée » est fournie par défaut.

- Si vous utilisez Web Studio pour gérer les stratégies Citrix, les paramètres que vous ajoutez à la stratégie Non filtrée sont appliqués à l'ensemble des serveurs, des bureaux et des connexions d'un site.
- Si vous utilisez l'éditeur de stratégie de groupe pour gérer les stratégies Citrix, les paramètres que vous ajoutez à la stratégie Non filtrée sont appliqués à tous les sites et à toutes les connexions. Les sites et les connexions doivent se trouver dans l'étendue des Objets de stratégie de groupe qui contiennent la stratégie. Par exemple, L'UO Ventes contient un GPO appelé Ventes-FR qui comprend tous les membres de l'équipe de vente française. Le GPO Ventes-FR est configuré à l'aide d'une stratégie Unfiltered qui comprend plusieurs paramètres de stratégie utilisateur. Lorsque le directeur des Ventes FR ouvre une session sur le site, les paramètres de la stratégie Non filtrée sont automatiquement appliqués à la session. Cette configuration est due au fait que l'utilisateur est membre du GPO Ventes-FR.

Un mode d'attribution détermine si la stratégie s'applique uniquement aux connexions qui ne correspondent pas aux critères d'attribution. Si le mode est défini sur Autoriser (valeur par défaut), la stratégie s'applique uniquement aux connexions correspondant aux critères d'attribution. Si le mode est défini sur Refuser, la stratégie s'applique si la connexion ne correspond pas aux critères d'attribution. Les exemples suivants illustrent la manière dont les modes d'attribution affectent les stratégies Citrix lorsque plusieurs attributions sont présentes.

- **Exemple : attributions de types similaires avec des modes différents :** dans les stratégies comportant deux attributions du même type, un défini sur Autoriser et un défini sur Refuser, l'attribution définie sur Refuser a priorité, étant donné que la connexion satisfait les deux attributions. Par exemple :

  La stratégie 1 comprend les attributions suivantes :

  - Affectation A spécifie le groupe Ventes. Le mode est défini sur Autoriser.
  - L'affectation B spécifie le compte du directeur des ventes. Le mode est défini sur Refuser.

Le mode de l'attribution B étant défini sur Refuser, la stratégie n'est pas appliquée lorsque le directeur des ventes ouvre une session sur le site, bien que l'utilisateur soit membre du groupe Ventes.

- **Exemple : attributions de types différents avec des modes similaires :** dans les stratégies comportant deux attributions ou plus de types différents, défini sur Autoriser, la connexion doit satisfaire au moins une attribution de chaque type afin que la stratégie soit appliquée. Par exemple :

  La stratégie 2 comprend les attributions suivantes :

  - L'attribution C est une attribution utilisateur qui spécifie le groupe Ventes. Le mode est défini sur Autoriser.
  - L'attribution D est une attribution d'adresse IP cliente qui spécifie 10.8.169.* (le réseau d'entreprise). Le mode est défini sur Autoriser.

  Lorsque le directeur des ventes ouvre une session sur le site depuis son bureau, la stratégie est appliquée car la connexion satisfait les deux attributions.

  La stratégie 3 comprend les attributions suivantes :

  - L'attribution E est une attribution utilisateur qui spécifie le groupe Ventes. Le mode est défini sur Autoriser.
  - L'attribution F est une attribution de type contrôle d'accès qui spécifie les conditions de connexion NetScaler Gateway. Le mode est défini sur Autoriser.

  Lorsque le directeur des ventes ouvre une session sur le site depuis le bureau, la stratégie n'est pas appliquée car la connexion ne satisfait pas l'attribution F.

### Créer une stratégie basée sur un modèle à l'aide de Web Studio

1. Connectez-vous à Web Studio et sélectionnez **Stratégies** dans le volet de gauche.
2. Sélectionnez l'onglet **Modèles**, puis sélectionnez un modèle.
3. Sélectionnez **Créer une stratégie à partir du modèle** dans la barre d'actions.
4. Par défaut, la nouvelle stratégie utilise tous les paramètres par défaut du modèle. Dans ce cas, l'option **Paramètres de modèles par défaut (recommandés)** est sélectionnée. Si vous souhaitez modifier les paramètres, sélectionnez **Modifier les paramètres par défaut et en ajouter d'autres**, puis ajoutez ou supprimez des paramètres.
5. Spécifiez comment appliquer la stratégie en sélectionnant l'une des options suivantes :

   - **Objets d'utilisateur et de machine sélectionnés**, Sélectionnez cette option pour appliquer la stratégie aux objets d'utilisateur et de machine sélectionnés, puis cliquez sur **At-**

**tribuer** pour sélectionner les objets d'utilisateur et de machine auxquels la stratégie s'applique.

- **Tous les objets du site**. Sélectionnez cette option pour appliquer la stratégie à tous les objets d'utilisateur et de machine du site.

6. Entrez un nom pour la stratégie. Considérez appeler la stratégie en fonction de ce qu'elle affecte, par exemple, Service finance ou Utilisateurs distants. Facultativement, ajoutez une description.

   La stratégie est désactivée par défaut ; vous pouvez l'activer. Si vous activez la stratégie, vous pouvez l'appliquer immédiatement aux utilisateurs ouvrant une session. Si vous désactivez la stratégie, elle n'est pas appliquée. Si vous devez définir la priorité de la stratégie ou ajouter des paramètres ultérieurement, envisagez de désactiver cette stratégie jusqu'à ce que vous soyez prêt à l'appliquer.

### Créer une stratégie à l'aide de Web Studio

1. Connectez-vous à Web Studio et sélectionnez **Stratégies** dans le volet de gauche.
2. Sélectionnez l'onglet **Stratégies**.
3. Sélectionnez **Créer une stratégie** dans la barre d'actions.
4. Ajoutez et configurez les paramètres de stratégie.
5. Spécifiez comment appliquer la stratégie en choisissant l'une des options suivantes :

   - Attribuer aux objets Utilisateur et Machine sélectionnés, puis sélectionnez les objets utilisateur et machine auquel la stratégie doit s'appliquer.
   - Attribuer tous les objets d'un site pour appliquer la stratégie à tous les objets utilisateur et machine dans le site.

6. Entrez un nom pour la stratégie ou acceptez le nom par défaut. Considérez appeler la stratégie en fonction de ce qu'elle affecte, par exemple, Service finance ou Utilisateurs distants. Facultativement, ajoutez une description.

   La stratégie est activée par défaut, vous pouvez la désactiver. Si vous activez la stratégie, vous pouvez l'appliquer immédiatement aux utilisateurs ouvrant une session. Si vous désactivez la stratégie, elle n'est pas appliquée. Si vous devez définir la priorité de la stratégie ou ajouter des paramètres ultérieurement, envisagez de désactiver cette stratégie jusqu'à ce que vous soyez prêt à l'appliquer.

### Créer et gérer les stratégies à l'aide de l'éditeur de stratégie de groupe

Dans l'éditeur de stratégie de groupe, développez le nœud **Configuration ordinateur ou Configuration utilisateur**. Développez le nœud **Stratégies**, puis sélectionnez **Stratégies Citrix**. Choisissez l'

action appropriée :

| Tâche | Instruction |
| --- | --- |
| Créer une stratégie | Dans l'onglet **Stratégies**, cliquez sur **Nouveau**. |
| Modifier une stratégie existante | Sur l'onglet **Stratégies**, sélectionnez la stratégie et cliquez sur **Modifier**. |
| Modifier la priorité d'une stratégie existante | Sur l'onglet **Stratégies**, sélectionnez la stratégie et cliquez sur **Plus élevée** ou **Plus basse**. |
| Afficher des informations récapitulatives sur une stratégie | Sur l'onglet **Stratégies**, sélectionnez la stratégie et cliquez sur l'onglet **Synthèse**. |
| Afficher et modifier les paramètres d'une stratégie | Sur l'onglet **Stratégies**, sélectionnez la stratégie et cliquez sur l'onglet **Paramètres**. |
| Afficher et modifier les filtres d'une stratégie | Sur l'onglet **Stratégies**, sélectionnez la stratégie et cliquez sur l'onglet **Filtres**. Lorsque vous ajoutez plusieurs filtres à une stratégie, toutes les conditions de filtre doivent être remplies pour que la stratégie soit appliquée. |
| Activer ou désactiver une stratégie | Sur l'onglet **Stratégies**, sélectionnez la stratégie, puis sélectionnez soit **Actions > Activer** ou **Actions > Désactiver**. |
| Créer une stratégie à partir d'un modèle existant | Sur l'onglet **Modèles**, sélectionnez le modèle, puis cliquez sur **Nouvelle stratégie**. |

## Jeux de stratégies

June 27, 2024

Les jeux de stratégies sont des objets de Citrix Virtual Apps and Desktops qui regroupent des stratégies pour permettre un accès simplifié basé sur les rôles et une gestion aisée. Vous pouvez créer des jeux de stratégies reflétant les divisions logiques au sein de votre équipe d'administrateurs et de votre entreprise. Par exemple, vous pouvez créer un jeu de stratégies pour chaque région géographique, unité commerciale ou pour un cas d'utilisation spécifique. Une fois créés, les étendues et les groupes de mise à disposition sont affectés à des jeux de stratégies afin que seuls les administrateurs autorisés puissent gérer les stratégies qui s'appliquent à leurs utilisateurs et machines concernés.

> **Remarque :**
>
> Avant d'activer les ensembles de stratégies, Citrix vous recommande de prendre note des points suivants :
>
> - Des validations de stratégie supplémentaires sont ajoutées. Par conséquent, une mise à niveau sur place peut entraîner la perte de données de stratégie si des paramètres de stratégie non valides sont présents.
> - Pour détecter les données non valides, utilisez l'outil d'analyse GPO et apportez les modifications nécessaires avant la mise à niveau. Pour plus d'informations, veuillez consulter l'article CTX676686.
> - Pour toutes les mises à niveau futures, Citrix vous recommande d'utiliser le dernier SDK. La mise à jour des stratégies à l'aide d'un ancien SDK peut entraîner l'ajout de données non valides aux paramètres de stratégie et poser un risque de perte de données de stratégie.

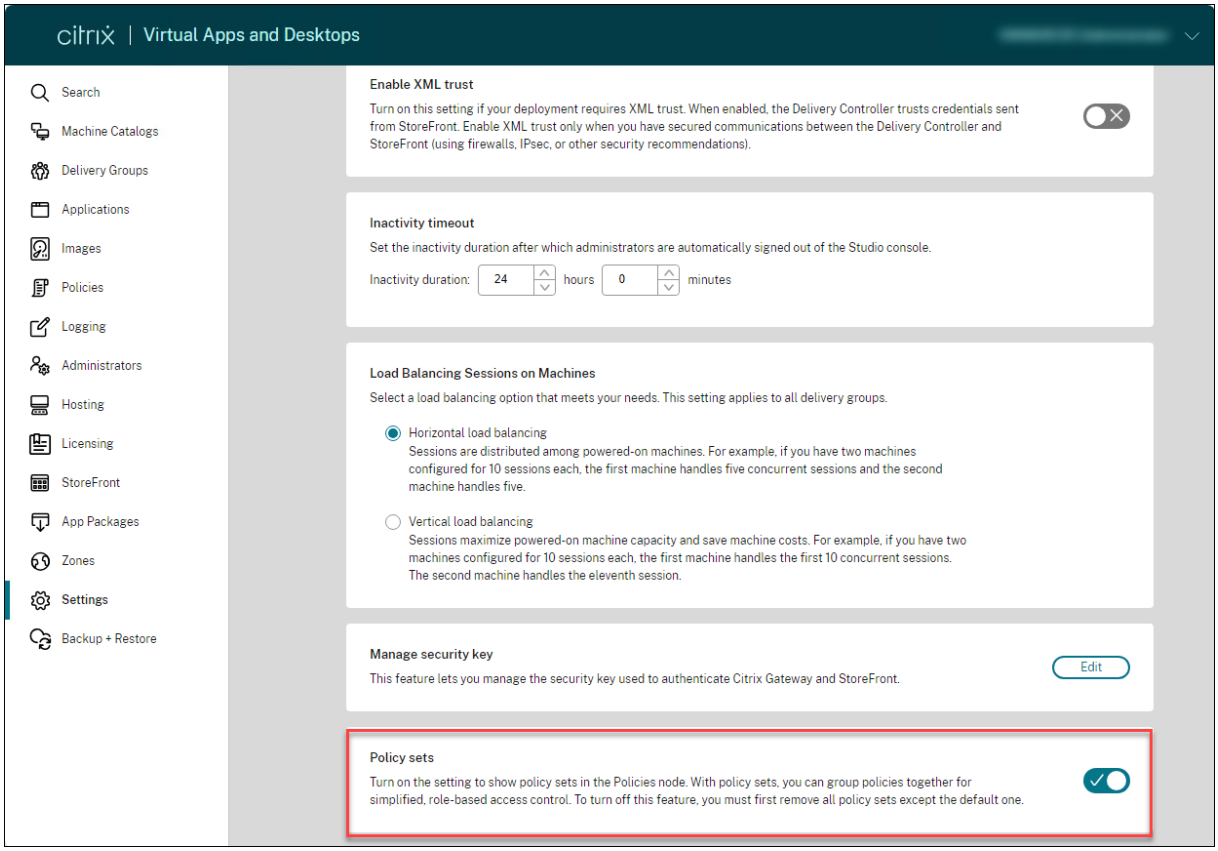
### Avantages

- Contrôle d'accès basé sur les rôles pour les équipes d'administrateurs distribuées
- Fusions, acquisitions et consolidations simplifiées
- Domaine de défaillance limité
- Prise en charge d'une utilisation multi-locataire pour les stratégies

### Activer les jeux de stratégies

Dans l'onglet **Gérer** de Virtual Apps and Desktops, cliquez sur **Paramètres** et activez le paramètre des **Jeux de stratégies**.




> **Remarque :**
>
> Vous devez activer les jeux de stratégies avant de créer un jeu de stratégies.

## Comparaison des fonctionnalités

| Avant d'appliquer les jeux de stratégies | Après avoir appliqué les jeux de stratégies |
|---|---|
| Les stratégies, les paramètres, les filtres et les priorités des stratégies pour l'ensemble du site sont configurés en un seul endroit au sein de Citrix Studio. | Les stratégies, les paramètres, les filtres et les priorités des stratégies sont configurés séparément pour chaque jeu de stratégies. |
| Si vous gérez une stratégie, vous devez gérer toutes les stratégies. | Les administrateurs titulaires peuvent déléguer à des administrateurs de niveau inférieur la capacité de gérer un jeu de stratégies particulier sur une base individuelle. |
| Les stratégies dans des environnements étendus et distribués deviennent complexes et difficiles à gérer. | Les stratégies dans des environnements étendus et distribués peuvent être divisées et gérées facilement. |

## Comment fonctionnent les jeux de stratégies ?

### Vue d'ensemble

- Les jeux de stratégies sont attribués aux groupes de mise à disposition
- Les jeux de stratégies ont un ou plusieurs domaines
- Les groupes de mise à disposition auxquels aucun jeu de stratégies n'est attribué reçoivent le jeu de stratégies par défaut
- Un groupe de mise à disposition ne peut se voir attribuer qu'un seul jeu de stratégies
- Plusieurs groupes de mise à disposition peuvent utiliser le même jeu de stratégies
- Même si les jeux de stratégies sont attribués à des groupes de mise à disposition, les jeux conservent leurs filtres

Pour plus d'informations, consultez Application des filtres. Lorsque vous utilisez des jeux de stratégie, la façon d'attribuer des stratégies ou des filtres de stratégie ne change pas. Elle s'effecue de la même manière que pour les stratégies.

### Jeu de stratégies par défaut

- Lorsque le paramètre du jeu de stratégies est activé, toutes les stratégies existantes sont regroupées dans le jeu de stratégies par défaut
- Chaque groupe de mise à disposition reçoit le jeu de stratégies par défaut, sauf si l'équipe d'administrateurs crée un jeu de stratégies et l'attribue à un groupe de mise à disposition.
- Une fois qu'un jeu de stratégies différent est attribué à un groupe de mise à disposition, celui-ci ne reçoit plus de stratégies du jeu par défaut

### Création d'un jeu de stratégies

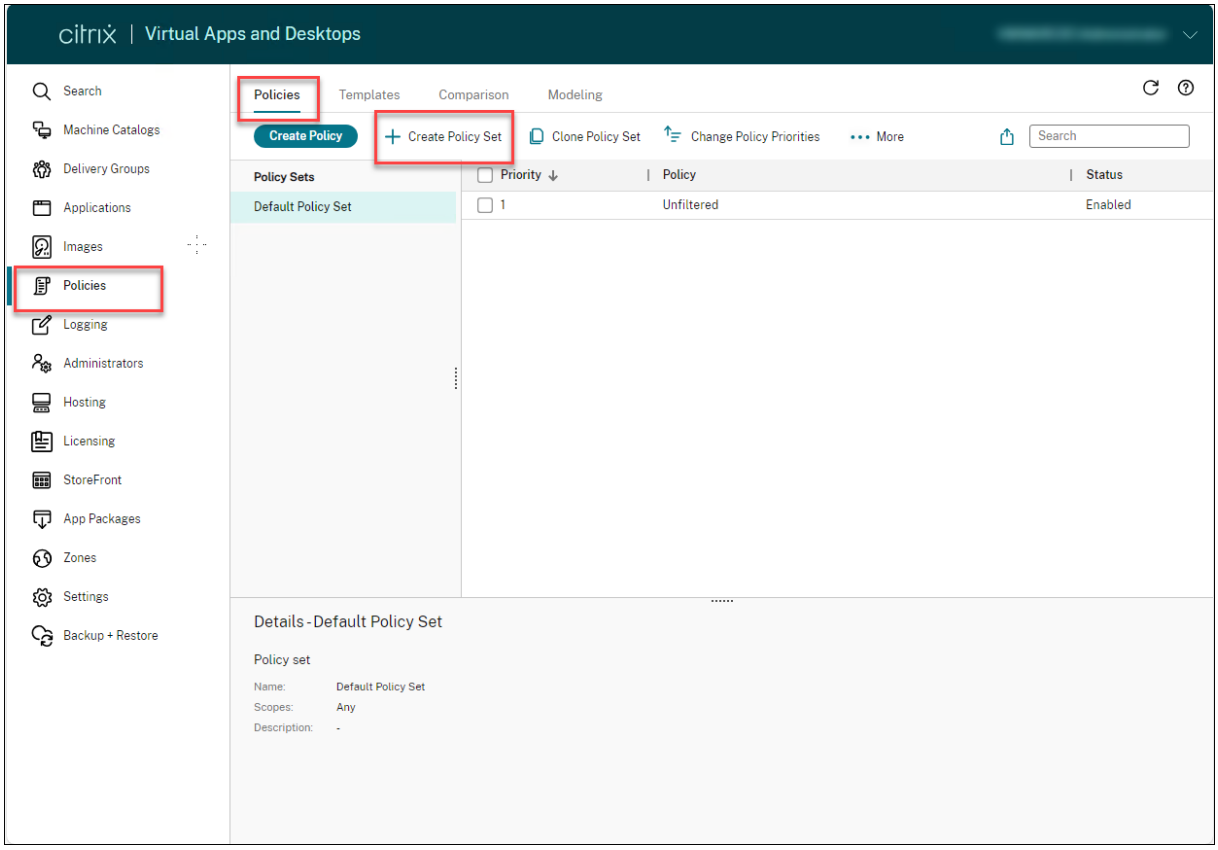
Les jeux de stratégies peuvent être créés des deux manières suivantes :

- Créer un jeu de stratégies : cette action crée un jeu de stratégies vide
- Cloner un jeu de stratégies : cette action crée un jeu de stratégies basé sur un jeu existant

### Créer des jeux de stratégies

1. Connectez-vous à Web Studio et sélectionnez **Stratégies** dans le volet de gauche.




1. Sélectionnez **Créer un jeu de stratégies**. L'onglet **Introduction** apparaît.
2. Cliquez sur **Suivant** ou sur l'onglet **Nom et description**.
3. Entrez le nom et la description du jeu de stratégies.
4. Cliquez sur **Suivant** ou sur l'onglet **Attributions**.
5. Sélectionnez un ou plusieurs groupes de mise à disposition auxquels vous souhaitez attribuer le jeu de stratégies.
6. Cliquez sur **Suivant** ou sur l'onglet **Étendues**.
7. Sélectionnez les étendues du jeu de stratégies.
8. Cliquez sur **Créer**. Le jeu de stratégies est créé avec l'affectation et l'étendue définies.

### Cloner un jeu de stratégies

1. Connectez-vous à Web Studio et sélectionnez **Stratégies** dans le volet de gauche.
2. Sélectionnez **Cloner jeu de stratégies**.
3. Modifiez le nom du jeu de stratégies.
4. Modifiez ou créez des attributions pour le jeu de stratégies et cliquez sur **Suivant**.
5. Sélectionnez ou désélectionnez les stratégies à inclure dans le jeu de stratégies cloné.
6. Modifiez l'étendue de la stratégie.
7. Cliquez sur **Créer**. Le jeu de stratégies est créé.

### Modifier des jeux de stratégies

1. Connectez-vous à Web Studio et sélectionnez **Stratégies** dans le volet de gauche.
2. Sélectionnez **Modifier jeu de stratégies**.
3. Modifiez le nom du jeu de stratégies et cliquez sur **Suivant**.
4. Modifiez ou créez des attributions pour le jeu de stratégies et cliquez sur **Suivant**.
5. Modifiez l'étendue de la stratégie.
6. Cliquez sur **Créer**.

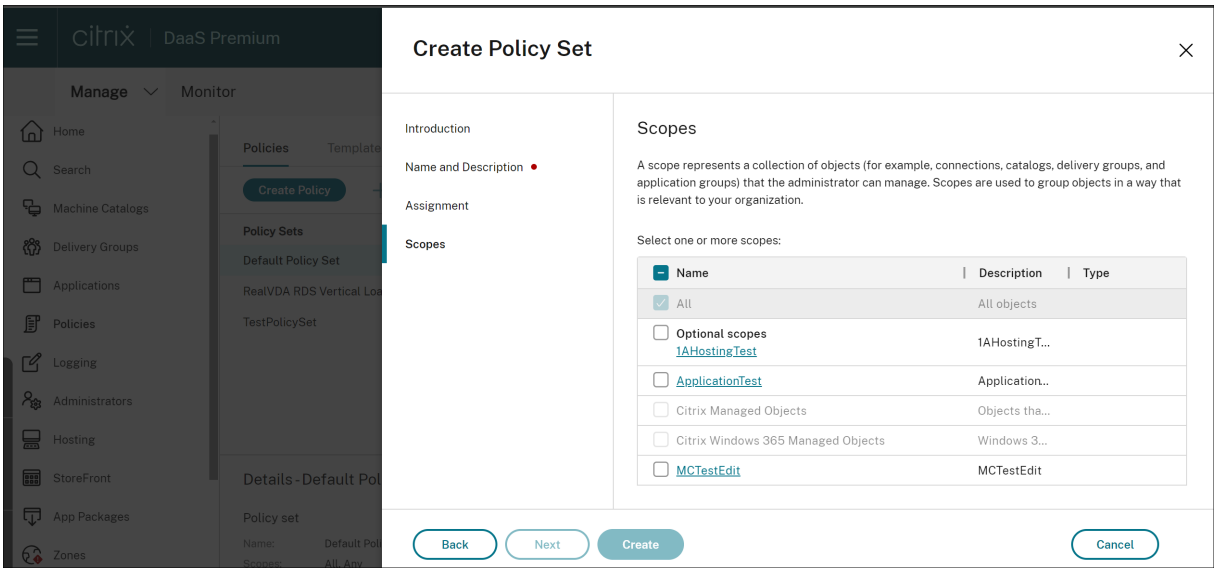
### Attribution d'un jeu de stratégies

Les jeux de stratégies sont attribués aux groupes de mise à disposition. Vous pouvez configurer les attributions lors de la création ou de la modification du jeu de stratégies. Vous pouvez également configurer les attributions lors de la création ou de la modification de groupes de mise à disposition.

### Étendues des jeux de stratégies

Les administrateurs peuvent définir l'étendue du jeu de stratégies afin que seuls les administrateurs autorisés puissent le consulter ou le modifier. Vous pouvez configurer les étendues lors de la création ou de la modification du jeu de stratégies.

L'introduction des jeux de stratégie vous permet également de créer et gérer des stratégies Citrix à l'aide de l'API. Pour plus d'informations, consultez Comment créer un jeu de stratégies dans Citrix DaaS.



# Comparer, donner un ordre de priorité, et résoudre les problèmes de stratégies

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Vous pouvez utiliser plusieurs stratégies pour personnaliser votre environnement afin de répondre aux besoins des utilisateurs, qui varient selon leur fonction, leur emplacement géographique ou leur type de connexion. Par exemple, pour renforcer la sécurité, il se peut vous deviez imposer des restrictions aux groupes d'utilisateurs qui interagissent régulièrement avec des données confidentielles.

Vous pouvez également créer une stratégie qui empêche les utilisateurs d'enregistrer les fichiers confidentiels sur leurs lecteurs clients locaux. Toutefois, si certains membres du groupe d'utilisateurs ont besoin de l'accès à leurs lecteurs locaux, vous pouvez créer une autre stratégie spécialement pour ces utilisateurs. Vous pouvez ensuite définir l'ordre de ces deux stratégies afin de définir laquelle des deux est prioritaire. Lorsque vous utilisez plusieurs stratégies, vous devez déterminer :

- Comment hiérarchiser les stratégies
- Comment créer des exceptions
- Comment afficher la stratégie effective en cas de conflit entre les stratégies

En général, les stratégies ont priorité sur les paramètres similaires configurés pour la totalité du site, pour des Delivery Controller spécifiques ou sur la machine cliente. L'exception à ce principe est la sécurité. Le paramètre de cryptage le plus élevé de votre environnement remplace toujours les autres paramètres et stratégies. Le paramètre de cryptage le plus élevé inclut le système d'exploitation et les paramètres d'observation les plus restrictifs.

Les stratégies Citrix interagissent avec celles que vous définissez dans votre système d'exploitation. Dans un environnement Citrix, les paramètres Citrix remplacent les mêmes paramètres configurés dans une stratégie Active Directory ou à l'aide de la Configuration d'hôte de session Bureau à distance. Ceci comprend les paramètres liés aux paramètres de connexion client RDP (Remote Desktop Protocol) standard. Les paramètres RDP standard incluent des paramètres tels que Papier peint du bureau, Animation de menu et Afficher le contenu de la fenêtre lors d'un cliquer déplacer.

Certains paramètres de stratégie, tels que Secure ICA, doivent correspondre aux paramètres du système d'exploitation. Si un niveau plus élevé de cryptage prioritaire est défini autre part, les

paramètres de **stratégie Secure ICA** que vous spécifiez dans la stratégie ou lorsque vous mettez à disposition une application ou des bureaux peuvent être remplacés.

Par exemple, les paramètres de cryptage que vous spécifiez lorsque vous créez des groupes de mise à disposition devraient être au même niveau que les paramètres de cryptage que vous avez spécifié au travers de votre environnement.

> **Remarque :**
>
> Dans le second hop d'un scénario double-hop, considérez les cas où un VDA avec OS mono-session se connecte à un VDA avec OS multi-session. Dans ce cas, les stratégies Citrix s'appliquent sur le VDA avec OS mono-session comme s'il s'agissait de la machine utilisateur. Par exemple, considérez les cas où les stratégies sont définies pour mettre en cache les images sur la machine utilisateur. Dans cet exemple, les images mises en cache pour le second hop dans un scénario double-hop sont mises en cache sur machine sur laquelle est installé le VDA avec OS mono-session.

## Utiliser l'assistant de modélisation de stratégie

La modélisation de stratégie vous permet de simuler les stratégies activées à l'aide de filtres à des fins de planification et de test. Seules les stratégies activées avec des filtres sont modélisées. Les stratégies désactivées ne sont jamais appliquées et les stratégies activées sans filtre sont toujours appliquées.

Effectuez les étapes suivantes pour ouvrir l'assistant **Modélisation de stratégie** :

1. Sélectionnez **Stratégies** dans le menu de navigation de gauche.
2. Sélectionnez l'onglet **Modélisation**.
3. Sélectionnez **Modélisation de stratégie** dans la barre d'actions.
4. Lisez la page **d'introduction** et cliquez sur **Suivant**.
5. Sélectionnez des utilisateurs ou des ordinateurs. Vous pouvez rechercher des conteneurs, des utilisateurs ou des ordinateurs spécifiques. Cliquez sur **Suivant**.
6. Choisissez votre évidence de filtre. Vous pouvez éventuellement obtenir une simulation plus précise en saisissant des informations supplémentaires, telles que le **groupe de mise à disposition**, les **balises**, l'**adresse IP du client**, etc. Cliquez sur **Suivant**.
7. Passez en revue le résumé de vos sélections et cliquez sur **Exécuter**.

Lorsque vous cliquez sur **Exécuter**, l'assistant génère un rapport sur les résultats de modélisation. Lorsque vous consultez ce rapport, vous pouvez :

- Choisir si vous souhaitez afficher **Tous les paramètres**, **Paramètres ordinateur** ou **Paramètres utilisateur** dans le menu déroulant.
- Utiliser la barre de recherche pour rechercher des paramètres spécifiques.

- Cliquer sur un paramètre spécifique pour afficher les détails de ce paramètre. Par exemple, si tous les paramètres utilisateur n'ont pas été appliqués pour une stratégie spécifique, le volet **Détails** indique la raison pour laquelle les paramètres n'ont pas été appliqués.
- Cliquer sur **Exporter** pour exporter les résultats de modélisation au format JSON, au format HTML ou les deux.

Une fois la modélisation de stratégie exécutée, d'autres options s'offrent à vous. Vous pouvez :

- **Afficher le rapport de modélisation** : ouvre le rapport de modélisation ci-dessus afin que vous puissiez le consulter à nouveau ou l'exporter.
- **Réexécuter la modélisation de stratégies** : vous permet de réexécuter la modélisation de stratégies avec le même ensemble de critères sélectionnés précédemment et de générer de nouveaux résultats de modélisation. Cette fonction est utile si certaines stratégies ont été modifiées et que vous souhaitez voir comment ces modifications affectent votre modèle actuel.
- **Supprimer le rapport de modélisation** : supprime le rapport de modélisation actuel.

### Comparer les stratégies et les modèles

Vous pouvez comparer les paramètres d'une stratégie ou d'un modèle avec ceux des autres stratégies ou modèles. Par exemple, il se peut que vous deviez vérifier des valeurs de paramètres afin d'assurer la compatibilité avec les meilleures pratiques. Vous pouvez également comparer les paramètres d'une stratégie ou d'un modèle avec les paramètres par défaut fournis par Citrix.

1. Connectez-vous à Web Studio et sélectionnez **Stratégies** dans le volet de gauche.
2. Cliquez sur l'onglet **Comparaison** puis cliquez sur **Sélectionner**.
3. Sélectionnez les stratégies ou les modèles à comparer. Pour inclure les valeurs par défaut dans la comparaison, sélectionnez la case à cocher **Comparer aux paramètres par défaut**.
4. Après avoir cliqué sur **Comparer**, les paramètres configurés sont affichés dans les colonnes.
5. Pour afficher tous les paramètres, sélectionnez **Afficher tous les paramètres**. Pour revenir à la vue par défaut, sélectionnez **Afficher les paramètres courants**.

### Définir les priorités des stratégies

La définition de priorités de stratégies vous permet de définir quelles sont les stratégies qui prévalent lorsqu'elles présentent des conflits de paramètres. Lorsque les utilisateurs ouvrent une session, toutes les stratégies correspondant aux attributions pour la connexion sont identifiées. Les stratégies sont triées dans un ordre de priorité et plusieurs instances de tous les paramètres sont comparées. Chaque paramètre est appliqué selon l'ordre de priorité de la stratégie.

Vous définissez la priorité des stratégies en leur donnant des numéros de priorité différents. Par défaut, la priorité d'une nouvelle stratégie est plus faible que celle d'une stratégie déjà existante.

Lorsque deux stratégies à appliquer ont des règles entrant en conflit, la stratégie dotée de la plus haute priorité (la valeur 1 représentant la plus haute priorité) prévaut sur la stratégie dotée de la priorité la plus faible. Les paramètres sont fusionnés selon leur priorité et leur condition, si le paramètre est désactivé ou activé par exemple. Tout paramètre désactivé remplace un paramètre de plus faible priorité qui est activé. Les paramètres de stratégie qui ne sont pas configurés sont ignorés ; ils ne l'emportent pas sur les paramètres dotés d'une priorité plus faible.

1. Sélectionnez **Stratégies** dans le volet de gauche. Assurez-vous de sélectionner l'onglet **Stratégies**.
2. Dans l'onglet **Stratégies**, sélectionnez **Changer les priorités de stratégie** dans la barre d'actions. La page **Changer les priorités de stratégie** s'affiche.
3. Dans la liste des priorités, utilisez les méthodes suivantes pour modifier la priorité d'une stratégie :

    - Faites glisser la stratégie vers la position souhaitée.
    - Pour la déplacer d'une position vers le haut ou vers le bas, cliquez respectivement sur l'icône de flèche vers le haut ou vers le bas.
    - Pour le déplacer en haut ou en bas de la liste, cliquez respectivement sur l'icône de flèche Haut ou Bas.
    - Pour changer le numéro de priorité, cliquez sur l'icône **Modifier**, entrez le numéro requis, puis cliquez sur **Enregistrer**.

4. Cliquez sur **Enregistrer**.

## Exceptions

Après avoir créé des stratégies pour des groupes d'utilisateurs, des machines utilisateur ou des machines, vous constaterez peut-être qu'il est nécessaire de définir, pour certains membres de ces groupes, des exceptions à certains paramètres de stratégie. Vous pouvez créer des exceptions en :

- créant une stratégie uniquement pour ces membres de groupe qui ont besoin des exceptions, et en plaçant la priorité d'une stratégie en plus haute position que la stratégie de tout le groupe ;
- utilisant le mode Refuser pour une attribution ajoutée à la stratégie.

Une attribution avec le mode défini sur Refuser applique une stratégie uniquement aux connexions qui ne correspondent pas aux critères d'attribution. Par exemple, une stratégie contient les attributions suivantes :

- L'attribution A est une attribution d'adresse IP cliente qui spécifie la plage 208.77.88.*. Le mode est défini sur Autoriser

- L'attribution B est une attribution utilisateur qui spécifie un compte utilisateur particulier. Le mode est défini sur Refuser.

La stratégie est appliquée à tous les utilisateurs qui ouvrent une session sur le site avec des adresses IP se trouvant dans la plage spécifiée dans l'attribution A. Cependant, la stratégie n'est pas appliquée à l'ouverture de session de l'utilisateur sur le site lorsque le compte utilisateur est spécifié dans l'attribution B.

### Déterminer les stratégies qui s'appliquent à une connexion

Il arrive qu'une connexion ne réponde pas comme prévu car plusieurs stratégies s'appliquent. Si une stratégie à priorité élevée s'applique également à la connexion, elle peut remplacer les paramètres configurés dans la stratégie d'origine. Vous pouvez calculer l'ensemble de stratégies résultant et déterminer le résultat final de la combinaison des paramètres de stratégie pour une connexion.

Vous pouvez calculer l'ensemble de stratégies résultant de plusieurs façons :

- Utilisez l'assistant **Modélisation de stratégie de groupe Citrix** pour simuler un scénario de connexion et déterminer comment appliquer les stratégies Citrix. Vous pouvez spécifier des conditions pour un scénario de connexion, telles que :
  - Contrôleur de domaine
  - Utilisateurs
  - Valeurs d'évidence d'attribution de stratégie Citrix
  - Paramètres d'environnement simulé comme une connexion réseau lente
    Le rapport produit par l'assistant répertorie les stratégies Citrix qui prendront effet dans le scénario. Étant donné que vous êtes connecté au Controller en tant qu'utilisateur du domaine, l'assistant calcule les résultats en utilisant les paramètres de stratégie du site et les objets de stratégie de groupe (GPO) Active Directory.
- Utilisez l'outil **Résultats de stratégie de groupe** pour créer un rapport décrivant les stratégies Citrix en vigueur pour un utilisateur et un contrôleur donnés. L'outil Résultats de stratégie de groupe vous aide à évaluer l'état actuel des objets de stratégie de groupe dans votre environnement et génère un rapport. Le rapport généré décrit de quelle façon ces objets, y compris les stratégies Citrix, sont appliqués à un utilisateur et à un contrôleur donnés.

Vous pouvez lancer l'assistant Modélisation de stratégie de groupe Citrix dans Web Studio. Vous pouvez également lancer l'outil Résultats de stratégie de groupe via la Console de gestion des stratégies de groupe de Windows.

Les paramètres de stratégie de site créés à l'aide de Web Studio ne sont pas inclus dans l'ensemble de stratégies résultant dans les cas suivants :

- Si vous exécutez l'assistant Modélisation de stratégie de groupe Citrix à partir de la Console de gestion des stratégies de groupe
- Si vous exécutez l'outil Résultats de stratégie de groupe à partir de la Console de gestion des stratégies de groupe.

Pour être certain d'obtenir l'ensemble de stratégies résultant le plus complet, Citrix vous recommande de lancer l'assistant Modélisation de stratégie de groupe Citrix depuis Web Studio, sauf si vous ne créez des stratégies qu'avec la Console de gestion des stratégies de groupe.

### Résolution des problèmes de stratégies

Les utilisateurs, adresses IP et autres objets affectés peuvent posséder plusieurs stratégies qui s'appliquent de manière simultanée. Ce scénario peut entraîner des conflits lorsqu'une stratégie ne se comporte pas de manière attendue. Lorsque vous exécutez l'assistant Modélisation de stratégie de groupe Citrix ou l'outil Résultats de stratégie de groupe, il se peut que vous découvriez qu'aucune stratégie n'est appliquée aux connexions utilisateur. Dans un tel scénario, les paramètres de stratégie ne sont pas appliqués aux utilisateurs qui se connectent à leurs applications et bureaux dans des conditions correspondant aux critères d'évaluation de stratégie. Cette situation se produit lorsque :

- aucune stratégie ne possède d'attribution correspondant au critère d'évaluation de stratégie ;
- les stratégies correspondant à l'attribution ne possèdent aucun paramètre configuré ;
- les stratégies correspondant à l'attribution sont désactivées.

Si vous souhaitez appliquer des paramètres de stratégie à des connexions répondant aux critères spécifiés, effectuez les opérations suivantes :

- Les stratégies que vous souhaitez appliquer à ces connexions sont activées.
- Les stratégies que vous souhaitez appliquer possèdent les paramètres appropriés configurés.

## Paramètres de stratégie par défaut

June 27, 2024

Les tableaux suivants répertorient les paramètres de stratégie, leur valeur par défaut, et les versions de Virtual Delivery Agent (VDA) auxquelles ils s'appliquent.

### ICA

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Transport adaptatif | Désactivé. Utiliser au choix | VDA 7.13 - 7.15 ; VDA 7.16 jusqu'à la version actuelle |
| Redirection du Presse-papiers client | Autorisé | Toutes les versions VDA |
| Formats d'écriture autorisés dans le Presse-papiers client | Aucun format spécifié | VDA 7.6 jusqu'à la version actuelle |
| Démarrages de bureaux | Interdit | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Numéro de port de l'écouteur ICA | 1494 | Toutes les versions VDA |
| Lancement de programmes non publiés lors de la connexion du client | Interdit | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Limiter le client du presse-papiers à la taille de transfert de la session | Désactivé | VDA 2009 |
| Limiter la session du Presse-papiers à la taille de transfert du client | Désactivé | VDA 2009 |
| Mode tolérance de pertes | Autorisé | VDA 2003. Remarque : le mode de tolérance de pertes n'est pas encore disponible. Cette version du VDA le prendra en charge lorsqu'elle est disponible. |
| Seuils de tolérance de pertes | Lorsque le mode de tolérance de pertes est disponible : Perte de paquets : 5 % ; Latence : 300 ms (RTT) | VDA 2003 jusqu'à la version actuelle |
| Protocole Rendezvous | Désactivé | S'applique uniquement aux sessions HDX établies via Citrix Cloud. |
| Restreindre écriture dans le Presse-papiers client | Interdit | VDA 7.6 jusqu'à la version actuelle |
| Restreindre écriture dans le Presse-papiers de session | Interdit | VDA 7.6 jusqu'à la version actuelle |

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Formats d'écriture autorisés dans le Presse-papiers de session | Aucun format spécifié | VDA 7.6 jusqu'à la version actuelle |
| Basculer en mode tablette | Activé | VDA 7.16 jusqu'à la version actuelle ; pour VDA 7.14 et 7.15 LTSR, configurez ce paramètre en utilisant le Registre. |
| Liste verte des canaux virtuels | Activé | VDA 2109 jusqu'à la version actuelle |

### ICA/Mise à disposition Adobe Flash/Redirection Flash

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Prévention du retour à la vidéo Flash | Non configuré | VDA 7.6 FP3 jusqu'à la version actuelle |
| Erreur *.swf de prévention du retour à la vidéo Flash | | VDA 7.6 FP3 jusqu'à la version actuelle |

### ICA/Audio

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Audio adaptatif | Activé | S'applique aux sessions de système d'exploitation mono-session et multisession de VDA utilisant Citrix Virtual Apps and Desktops 2109 ou version ultérieure. |
| Transport en temps réel audio via UDP | Autorisé | Toutes les versions VDA |
| Audio Plug N Play | Autorisé | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Qualité audio | Élevée : audio à définition élevée | Toutes les versions VDA |
| Redirection audio cliente | Autorisé | Toutes les versions VDA |

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Redirection du microphone client | Autorisé | Toutes les versions VDA |
| Mode de tolérance de pertes pour l'audio | Interdit | Versions VDA 2402 et supérieures |

### ICA/Reconnexion automatique des clients

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Reconnexion automatique des clients | Autorisé | Toutes les versions VDA |
| Authentification de la reconnexion automatique des clients | Ne pas requérir d' authentification | Toutes les versions VDA |
| Journalisation de la reconnexion automatique des clients | Ne pas journaliser les événements de reconnexion automatique | Toutes les versions VDA |
| Délai de reconnexion automatique des clients | 120 secondes | VDA 7.13 jusqu'à la version actuelle |
| Niveau de transparence de l' interface durant la reconnexion | 80 % | VDA 7.13 jusqu'à la version actuelle |

### ICA/Bande passante

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Limite de bande passante de la redirection audio | 0 kbps | Toutes les versions VDA |
| Pourcentage de limite de bande passante de la redirection audio | 0 | Toutes les versions VDA |
| Limite de bande passante de redirection du périphérique USB client | 0 kbps | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Pourcentage de limite de bande passante de redirection du périphérique USB client | 0 | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Limite de bande passante de redirection du Presse-papiers | 0 kbps | Toutes les versions VDA |
| Pourcentage de la limite de la bande passante de redirection du Presse-papiers | 0 | Toutes les versions VDA |
| Limite de bande passante de redirection de port COM | 0 kbps | Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre. |
| Pourcentage de limite de bande passante de redirection du port COM | 0 | Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre. |
| Limite de bande passante de redirection de fichier | 0 kbps | Toutes les versions VDA |
| Pourcentage de limite de bande passante de redirection de fichier | 0 | Toutes les versions VDA |
| Limite de bande passante d'accélération multimédia HDX MediaStream | 0 kbps | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 et VDA pour OS mono-session 7 jusqu'à la version actuelle de VDA pour OS multi-session et VDA pour OS mono-session |
| Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream | 0 | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Limite de bande passante pour la redirection du port LPT | 0 kbps | Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre. |

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Pourcentage de limite de bande passante de redirection du port LPT | 0 | Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre. |
| Limite de bande passante de session générale | 0 kbps | Toutes les versions VDA |
| Limite de bande passante de redirection d'imprimante | 0 kbps | Toutes les versions VDA |
| Pourcentage de limite de bande passante de redirection de l'imprimante | 0 | Toutes les versions VDA |
| Limite de bande passante de redirection du périphérique TWAIN | 0 kbps | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Pourcentage de limite de bande passante de redirection du périphérique TWAIN | 0 | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

### ICA/Redirection bidirectionnelle du contenu

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Autoriser la redirection bidirectionnelle du contenu | Interdit | VDA 7.13 jusqu'à la version actuelle |
| URL autorisées à être redirigées sur le client | vide | VDA 7.13 jusqu'à la version actuelle |
| URL autorisées à être redirigées sur le VDA | vide | VDA 7.13 jusqu'à la version actuelle |
| Configuration de redirection bidirectionnelle du contenu | Désactivé | VDA 2311 jusqu'à la version actuelle |

### ICA/Redirection du contenu du navigateur

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Redirection de contenu du navigateur | Autorisé | VDA 7.16 jusqu'à la version actuelle |
| Configuration de l'ACL de redirection du contenu de navigateur | `https://www.youtube.com/*` | VDA 7.16 jusqu'à la version actuelle |
| Prise en charge de l'authentification Windows intégrée pour la redirection du contenu du navigateur | Interdit | VDA 2106 jusqu'à la version actuelle |
| Configuration du proxy de redirection du contenu de navigateur | vide | VDA 7.16 jusqu'à la version actuelle |
| Authentification du proxy de récupération de contenu côté serveur de la redirection du contenu de navigateur | Interdit | VDA 2012 jusqu'à la version actuelle |

### ICA/Capteurs clients

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Autoriser les applications à utiliser l'emplacement physique de la machine cliente | Interdit | VDA 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

### ICA/IU de bureau

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Redirection de composition du Bureau | Désactivé (7.6 FP3 jusqu'à la version actuelle) ; Activé (5.6 à 7.6 FP2) | VDA 5.6, VDA pour OS mono-session 7 jusqu'à la version 7.15 |

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Qualité graphique de redirection Desktop Composition | Moyen | VDA 5.6, VDA pour OS mono-session 7 jusqu'à la version 7.15 |
| Papier peint du bureau | Autorisé | Toutes les versions VDA |
| Animation de menu | Autorisé | Toutes les versions VDA |
| Afficher le contenu de la fenêtre lors d'un cliquer déplacer | Autorisé | Toutes les versions VDA |

### ICA/Contrôle de l'utilisateur final

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Calcul des boucles ICA | Activé | Toutes les versions VDA |
| Intervalle de calcul des boucles ICA | 15 secondes | Toutes les versions VDA |
| Calcul des boucles ICA pour les connexions inactives | Désactivé | Toutes les versions VDA |

### ICA/Expérience de bureau améliorée

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Expérience de bureau améliorée | Autorisé | VDA pour OS multi-session 7 jusqu'à la version actuelle |

### ICA/Redirection de fichier

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Connecter automatiquement les lecteurs clients | Autorisé | Toutes les versions VDA |
| Redirection de lecteur client | Autorisé | Toutes les versions VDA |
| Lecteurs fixes clients | Autorisé | Toutes les versions VDA |

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Lecteurs de disquette clients | Autorisé | Toutes les versions VDA |
| Lecteurs réseau clients | Autorisé | Toutes les versions VDA |
| Lecteurs optiques clients | Autorisé | Toutes les versions VDA |
| Lecteurs amovibles clients | Autorisé | Toutes les versions VDA |
| Redirection hôte vers client | Désactivé | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Préserver les lettres de lecteurs clients | Désactivé | VDA 5, 5.5, 5.6 FP1, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Accès en lecture unique sur le lecteur client | Désactivé | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Redirection de dossiers spéciaux | Autorisé | Déploiements Interface Web uniquement ; VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Utiliser les écritures asynchrones | Désactivé | Toutes les versions VDA |

### ICA/graphiques

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Autoriser la compression visuelle sans perte | Désactivé | VDA 7.6 jusqu'à la version actuelle |
| Limite de mémoire d'affichage | 65,536 Ko | VDA 5, 5.5, 5.6 FP1, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Préférence de dégradation du mode d'affichage | Réduire d'abord le nombre de couleurs | Toutes les versions VDA |

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Aperçu de fenêtres dynamiques | Activé | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Indicateur d'état des graphiques | Désactivé | VDA 7.16 jusqu'à la version actuelle |
| Mise en cache d'image | Activé | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Mode graphique d'ancienne génération | Désactivé | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Nombre de couleurs maximal autorisé | 32 bits par pixel | Toutes les versions VDA |
| Notifier l'utilisateur lorsque le mode d'affichage se dégrade | Désactivé | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Optimiser pour la charge des graphiques 3D | Désactivé | VDA 7.17 jusqu'à la version actuelle |
| Mise en file d'attente et suppression | Activé | Toutes les versions VDA |
| Partage d'écran | Désactivé | VDA 2112 |
| Utiliser codec vidéo pour la compression | Utiliser un codec vidéo au choix | VDA 7.6 FP3 jusqu'à la version actuelle |
| Utiliser le codage matériel pour le codec vidéo | Activé | VDA 7.11 jusqu'à la version actuelle |

### ICA/graphiques/mise en cache

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Seuil de cache permanent | 3 000 000 bps | VDA pour OS multi-session 7 jusqu'à la version actuelle |

### ICA/graphiques/Framehawk

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Canal d'affichage Framehawk | Désactivé | VDA 7.6 FP2 jusqu'à la version actuelle |
| Plage de ports du canal d'affichage Framehawk | 3224, 3324 | VDA 7.6 FP2 jusqu'à la version actuelle |

### ICA/Persistance

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Délai d'expiration de persistance ICA | 60 secondes | Toutes les versions VDA |
| Persistances ICA | Ne pas envoyer de messages de persistance ICA | Toutes les versions VDA |

### Clavier/ICA et éditeur IME

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME | Désactivé | S'applique uniquement à 1912 LTSR CU2 et versions ultérieures. |
| Activer le mappage du clavier Unicode | Interdit | S'applique uniquement à 1912 LTSR CU2 et versions ultérieures. |
| Masquer la boîte de dialogue de changement de clavier | Interdit | S'applique uniquement à 1912 LTSR CU2 et versions ultérieures. |

### ICA/Local App Access

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Autoriser Local App Access | Interdit | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Liste de blocage de redirection d'adresse URL | Aucun site n'est spécifié. | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Liste d'autorisation de redirection d'adresse URL | Aucun site n'est spécifié. | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

### ICA/Expérience mobile

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Affichage automatique du clavier | Interdit | VDA 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Démarrer un bureau tactile | Autorisé | VDA 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle Ce paramètre est désactivé et n'est pas disponible pour les machines Windows 10 et Windows Server 2016. |
| Contrôler à distance les zones de liste déroulantes | Interdit | VDA 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

### ICA/multimédia

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Redirection vidéo HTML5 | Interdit | VDA 7.12 jusqu'à la version actuelle |
| Limiter la qualité vidéo | Non configuré | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Redirection de Microsoft Teams | Autorisé | VDA pour OS multi-session 1906 jusqu'à la version actuelle, VDA pour OS mono-session 1906 jusqu'à la version actuelle |
| Conférences multimédia | Autorisé | Toutes les versions VDA |
| Optimisation de la redirection multimédia de Windows Media sur un réseau étendu | Autorisé | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Utiliser GPU pour l'optimisation de la redirection multimédia Windows Media sur un réseau étendu | Interdit | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Prévention du retour à Windows Media | Non configuré | VDA 7.6 FP3 jusqu'à la version actuelle |
| Récupération de contenu Windows Media côté client | Autorisé | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Redirection Windows Media | Autorisé | Toutes les versions VDA |
| Taille de tampon de redirection Windows Media | 5 secondes | VDA 5, 5.5, 5.6 FP1 jusqu'à la version actuelle |
| Utilisation de la taille de tampon de redirection Windows Media | Désactivé | VDA 5, 5.5, 5.6 FP1 jusqu'à la version actuelle |

### ICA/Connexions Multi-Stream

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Audio sur UDP | Autorisé | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Plage de port UDP audio | 16500, 16509 | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Stratégie Multi-Port | Le port principal (2598) a une priorité élevée | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Paramètre Ordinateur Multi-Stream | Désactivé | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Paramètre Utilisateur Multi-Stream | Désactivé | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Paramètre d'attribution de flux de canaux virtuels Multi-Stream | Voir Paramètre d'attribution de flux de canaux virtuels Multi-Stream pour les attributions de flux par défaut | VDA 2003 |

### ICA/Redirection de ports

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Connecter automatiquement les ports COM du client | Désactivé | Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre. |

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Connecter automatiquement les ports LPT du client | Désactivé | Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre. |
| Redirection de port COM client | Interdit | Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre. |
| Redirection de port LPT client | Interdit | Toutes les versions VDA ; pour le VDA 7.0 jusqu'à la version 7.8, configurez ce paramètre en utilisant le Registre. |

### ICA/Impression

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Redirection d'imprimante cliente | Autorisé | Toutes les versions VDA |
| Imprimante par défaut | Définir l'imprimante par défaut sur l'imprimante principale du client | Toutes les versions VDA |
| Attributions d'imprimantes | L'imprimante actuelle de l'utilisateur est utilisée comme imprimante par défaut pour la session. | Toutes les versions VDA |
| Préférence de journalisation des événements de création automatique des imprimantes | Journaliser les erreurs et les avertissements | Toutes les versions VDA |
| Imprimantes de session | Aucune imprimante n'est spécifiée. | Toutes les versions VDA |
| Attendre la création d'imprimantes (bureau) | Désactivé | Toutes les versions VDA |

### ICA/Impression/Imprimantes clientes

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Créer automatiquement les imprimantes clientes | Créer automatiquement toutes les imprimantes clientes | Toutes les versions VDA |
| Créer automatiquement l'imprimante universelle générique | Désactivé | Toutes les versions VDA |
| Noms des imprimantes clientes | Noms d'imprimantes standards | VDA 5.6 |
| Diriger les connexions vers les serveurs d'impression | Activé | Toutes les versions VDA |
| Mappage et compatibilité du pilote d'imprimante | Aucune règle n'est spécifiée. | Toutes les versions VDA |
| Rétention des propriétés de l'imprimante | Contenu dans le profil uniquement si non enregistré sur le client | Toutes les versions VDA |
| Imprimantes clientes conservées et restaurées | Autorisé | VDA 5, 5.5, 5.6 FP1 |

### ICA/Impression/Pilotes

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Installation automatique de pilotes d'imprimante fournis par défaut | Activé | Toutes les versions VDA |
| Préférence de pilote universel | EMF ; XPS ; PCL5c ; PCL4 ; PS | Toutes les versions VDA |
| Utilisation du pilote d'impression universelle | Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible | Toutes les versions VDA |

### ICA/Impression/Serveur d'impression universelle

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Activer le serveur d'impression universelle | Désactivé | Toutes les versions VDA |
| Port (CGP) du flux de données d'impression du serveur d'impression universelle | 7229 | Toutes les versions VDA |
| Limite de bande passante d'entrée du flux d'impression du serveur d'impression universelle (kbps) | 0 | Toutes les versions VDA |
| Port (HTTP/SOAP) du service Web du serveur d'impression universelle | 8080 | Toutes les versions VDA |
| Serveurs d'impression universelle d'équilibrage de la charge | | VDA 7.9 jusqu'à la version actuelle |
| Seuil au-delà duquel les serveurs d'impression universelle sont hors service | 180 (secondes) | VDA 7.9 jusqu'à la version actuelle |

### ICA/Impression/Impression universelle

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Mode de traitement de l'impression universelle EMF | Spouler directement vers l'imprimante | Toutes les versions VDA |
| Limite de compression d'image de l'impression universelle | Meilleure qualité (compression sans perte) | Toutes les versions VDA |
| Valeur par défaut d'optimisation de l'impression universelle | Compression d'image : Qualité d'image désirée = Qualité standard, Activer la compression lourde = Faux ; Cache d'image et de police : Autoriser la mise en cache des images incorporées = Vrai ; Autoriser les non administrateurs à modifier ces paramètres = Faux ; | Toutes les versions VDA |

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Préférence d'aperçu d'impression universelle | Ne pas utiliser l'aperçu pour les imprimantes créées automatiquement ou universelles génériques | Toutes les versions VDA |
| Limite de qualité d'image de l'impression universelle | Durée illimitée | Toutes les versions VDA |

### ICA/sécurité

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Niveau de cryptage minimum SecureICA | De base | VDA pour OS multi-session 7 jusqu'à la version actuelle |

### ICA/Limites de serveur

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Intervalle d'horloge inactive du serveur | 0 millisecondes | VDA pour OS multi-session 7 jusqu'à la version actuelle |

### ICA/Limites de session

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Horloge de session déconnectée | Désactivé | VDA 5, 5.5, 5.6 FP1, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Horloge de session déconnectée Remote PC Access | Désactivé | VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Intervalle d'horloge de session déconnectée | 1440 minutes | VDA 5, 5.5, 5.6 FP1, VDA pour OS mono-session 7 jusqu'à la version actuelle |

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Horloge de connexion de session | Désactivé | VDA 5, 5.5, 5.6 FP1, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Intervalle d'horloge de connexion de session | 1440 minutes | VDA 5, 5.5, 5.6 FP1, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Horloge inactive de session | Activé | VDA 5, 5.5, 5.6 FP1, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Intervalle d'horloge inactive de session | 1440 minutes | VDA 5, 5.5, 5.6 FP1, VDA pour OS mono-session 7 jusqu'à la version actuelle |

### ICA/Fiabilité de session

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Connexions de fiabilité de session | Autorisé | Toutes les versions VDA |
| Numéro de port de la fiabilité de session | 2598 | Toutes les versions VDA |
| Expiration de délai de la fiabilité de session | 180 secondes | Toutes les versions VDA |

### ICA/Contrôle de fuseau horaire

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Estimation de l'heure locale des anciens clients | Activé | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Restaurer le fuseau horaire du système d'exploitation mono-session lors de la déconnexion de session ou de la fermeture de session | Activé | Version actuelle du VDA |

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Utiliser l'heure locale du client | Utiliser le fuseau horaire du serveur | Toutes les versions VDA |

### Périphériques ICA/TWAIN

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Redirection de périphérique TWAIN client | Autorisé | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Niveau de compression TWAIN | Moyen | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

### Périphériques ICA/USB

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Règles d'optimisation des périphériques USB clients | Activé (VDA 7.6 FP3 jusqu'à la version actuelle) ; Désactivé (VDA 7.11 jusqu'à la version actuelle) ; Par défaut, aucune règle n'est spécifiée | VDA 7.6 FP3 jusqu'à la version actuelle |
| Redirection de périphérique USB client | Interdit | Toutes les versions VDA |
| Règles de redirection de périphérique USB client | Aucune règle n'est spécifiée. | Toutes les versions VDA |
| Redirection de périphérique Plug and Play USB client | Autorisé | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

### ICA/Affichage visuel

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Nombre de couleurs préféré pour les graphiques simples | 24 bits par pixel | VDA 7.6 FP3 jusqu'à la version actuelle |
| Taux de trames cible | 30 fps | Toutes les versions VDA |
| Qualité visuelle | Moyen | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

### ICA/Affichage visuel/Images en mouvement

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Qualité d'image minimale | Normal | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Compression d'images en mouvement | Activé | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Niveau de compression progressif | Aucun | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Valeur de seuil de compression progressif | 2 147 483 647 Kbits/s | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Taux de trame minimum cible | 10 fps | VDA 5.5, 5.6 FP1, VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

> **Remarque :**
>
> La stratégie **Taux de trame minimum cible** n'est plus prise en charge.

### ICA/Affichage visuel/Images fixes

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Compression de couleur supplémentaire | Désactivé | Toutes les versions VDA |
| Seuil de compression de couleur supplémentaire | 8 192 Kbits/s | Toutes les versions VDA |
| Compression lourde | Désactivé | Toutes les versions VDA |
| Niveau de compression avec perte | Moyen | Toutes les versions VDA |
| Valeur de seuil de compression avec perte | 2 147 483 647 Kbits/s | Toutes les versions VDA |

### ICA/WebSockets

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Connexions WebSockets | Interdit | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Numéro de port WebSockets | 8008 | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Liste des serveurs d'origine approuvés WebSockets | Le caractère générique est utilisé pour faire confiance à toutes les adresses URL Receiver pour Web. | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

### Gestion de la charge

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Tolérance d'ouvertures de session simultanée | 2 | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Utilisation du processeur | Désactivé | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Priorité de processus exclue de l'utilisation UC | Inférieure à la normale ou Basse | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Utilisation du disque | Désactivé | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Nombre maximum de sessions | 250 | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Utilisation de la mémoire | Désactivé | VDA pour OS multi-session 7 jusqu'à la version actuelle |
| Charge de base d'utilisation mémoire | Charge zéro : 768 Mo | VDA pour OS multi-session 7 jusqu'à la version actuelle |

### Profile Management/Paramètres avancés

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Désactiver la configuration automatique | Désactivé | Toutes les versions VDA |
| Fermer la session de l'utilisateur si un problème se produit | Désactivé | Toutes les versions VDA |
| Nombre de tentatives d'accès à des fichiers verrouillés | 5 | Toutes les versions VDA |

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Traiter les cookies Internet à la fermeture de session | Désactivé | Toutes les versions VDA |

### Profile Management/Paramètres de base

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Réécriture active | Désactivé | Toutes les versions VDA |
| Activer Profile Management | Désactivé | Toutes les versions VDA |
| Groupes exclus | Désactivé. Tous les membres des groupes d'utilisateurs sont traités. | Toutes les versions VDA |
| Prise en charge des profils déconnectés | Désactivé | Toutes les versions VDA |
| Chemin d'accès au magasin de l'utilisateur | Windows | Toutes les versions VDA |
| Traiter les connexions des administrateurs locaux | Désactivé | Toutes les versions VDA |
| Groupes traités | Désactivé. Tous les membres des groupes d'utilisateurs sont traités. | Toutes les versions VDA |

### Profile Management/Paramètres multi-plateformes

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Paramètres multi-plateformes des groupes d'utilisateurs | Désactivé. Tous les groupes d'utilisateurs spécifiés dans Groupes traités sont traités. | Toutes les versions VDA |
| Activer les paramètres multi-plateformes | Désactivé | Toutes les versions VDA |
| Chemin d'accès aux définitions multi-plateformes | Désactivé. Aucun chemin n'est spécifié. | Toutes les versions VDA |

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au magasin des paramètres multi-plateformes | Désactivé. Windows\PM_CM est utilisé. | Toutes les versions VDA |
| Source utilisée pour créer les paramètres multi-plateformes | Désactivé | Toutes les versions VDA |

### Profile Management/Système de fichiers/Exclusions

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Liste d'exclusion - répertoires | Désactivé. Tous les dossiers du profil utilisateur sont synchronisés. | Toutes les versions VDA |
| Liste d'exclusion - fichiers | Désactivé. Tous les fichiers du profil utilisateur sont synchronisés. | Toutes les versions VDA |

### Profile Management/Système de fichiers/Synchronisation

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Répertoires à synchroniser | Désactivé. Seuls les dossiers non exclus sont synchronisés. | Toutes les versions VDA |
| Fichiers à synchroniser | Désactivé. Seuls les fichiers non exclus sont synchronisés. | Toutes les versions VDA |
| Dossiers en miroir | Désactivé. Aucun dossier n'est mis en miroir. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Accorder l'accès administrateur | Désactivé | Toutes les versions VDA |
| Inclure le nom de domaine | Désactivé | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/AppData(Roaming)

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin AppData (Roaming) | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du dossier AppData(Roaming) | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie AppData(Roaming). | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Contacts

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au dossier Contacts | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du dossier Contacts | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie **Chemin d'accès au dossier Contacts**. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Bureau

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au dossier Bureau | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du dossier Bureau | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie **Chemin d'accès au dossier Bureau**. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Documents

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au dossier Mes documents | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du dossier Mes documents | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie **Chemin d'accès au dossier Mes documents**. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Téléchargements

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au dossier Téléchargements | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du dossier Téléchargements | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie **Chemin d'accès au dossier Téléchargements**. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Favoris

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au dossier Favoris | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du dossier Favoris | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie **Chemin d'accès au dossier Favoris**. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Liens

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au dossier Liens | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du dossier Liens | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie **Paramètres de redirection du dossier Liens**. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Musique

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au dossier Ma musique | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du dossier Ma musique | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie **Chemin d'accès au dossier Ma musique**. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Images

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au dossier Mes images | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du dossier Mes images | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie **Chemin d'accès au dossier Mes images**. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Parties enregistrées

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au dossier Parties enregistrées | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du dossier Parties enregistrées | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie **Chemin d'accès au dossier Parties enregistrées**. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Recherches

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au dossier Recherches | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du dossier Recherches | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie **Chemin d'accès au dossier Recherches**. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Menu Démarrer

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au menu Démarrer | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection du menu Démarrer | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie Chemin Menu Démarrer. | Toutes les versions VDA |

### Profile Management/Redirection de dossiers/Vidéo

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin d'accès au dossier Vidéo | Désactivé. Aucun emplacement n'est spécifié. | Toutes les versions VDA |
| Paramètres de redirection pour la vidéo | Le contenu est redirigé vers le chemin UNC spécifié dans les paramètres de stratégie **Chemin d'accès au dossier Vidéo**. | Toutes les versions VDA |

### Profile Management/Paramètres du journal

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Actions Active Directory | Désactivé | Toutes les versions VDA |
| Informations courantes | Désactivé | Toutes les versions VDA |
| Avertissements courants | Désactivé | Toutes les versions VDA |
| Activer la journalisation | Désactivé | Toutes les versions VDA |
| Actions du système de fichiers | Désactivé | Toutes les versions VDA |
| Notifications du système de fichiers | Désactivé | Toutes les versions VDA |
| Fermeture de session | Désactivé | Toutes les versions VDA |
| Ouverture de session | Désactivé | Toutes les versions VDA |
| Taille maximale du fichier journal | 1048576 | Toutes les versions VDA |
| Chemin vers le fichier journal | Désactivé. Les fichiers journaux sont enregistrés à l'emplacement par défaut ; %System-Root%\System32\Logfiles\UserProfileManager. | Toutes les versions VDA |
| Informations utilisateur personnalisées | Désactivé | Toutes les versions VDA |
| Valeurs de stratégie à l'ouverture et fermeture de session | Désactivé | Toutes les versions VDA |
| Actions du registre | Désactivé | Toutes les versions VDA |

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Différences de registre à la fermeture de session | Désactivé | Toutes les versions VDA |

### Management/Profile Management/Traitement des profils

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Délai avant la suppression des profils mis en cache | 0 | Toutes les versions VDA |
| Supprimer les profils mis en cache localement à la fermeture de session | Désactivé | Toutes les versions VDA |
| Gestion des conflits de profils locaux | Utiliser profil local | Toutes les versions VDA |
| Migration des profils existants | Locaux et itinérants | Toutes les versions VDA |
| Chemin d'accès au profil modèle | Désactivé. Les nouveaux profils utilisateur sont créés à partir du profil utilisateur par défaut sur la machine sur laquelle un utilisateur ouvre une session. | Toutes les versions VDA |
| Le profil modèle remplace le profil local | Désactivé | Toutes les versions VDA |
| Le profil modèle remplace le profil itinérant | Désactivé | Toutes les versions VDA |
| Profil modèle utilisé en tant que profil Citrix obligatoire pour toutes les ouvertures de session | Désactivé | Toutes les versions VDA |

### Profile Management/Registre

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Liste d'exclusion | Désactivé. Toutes les clés de registre dans la ruche HKCU sont traitées lorsqu'un utilisateur ferme sa session. | Toutes les versions VDA |
| Liste d'inclusion | Désactivé. Toutes les clés de registre dans la ruche HKCU sont traitées lorsqu'un utilisateur ferme sa session. | Toutes les versions VDA |

### Profile Management/Profils utilisateur streamés

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Toujours mettre en cache | Désactivé | Toutes les versions VDA |
| Taille au-delà de laquelle toujours mettre en cache | 0 Mo | Toutes les versions VDA |
| Streaming des profils | Désactivé | Toutes les versions VDA |
| Groupes des profils utilisateurs streamés | Désactivé. Tous les profils utilisateur d'une unité d'organisation sont traités normalement. | Toutes les versions VDA |
| Délai de réécriture des fichiers en cas de verrouillage (jours) | 1 jour | Toutes les versions VDA |

### Receiver

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Liste de comptes StoreFront | Aucun magasin n'est spécifié. | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |

### Couche de personnalisation de l'utilisateur

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Chemin du référentiel de couche utilisateur | Désactivé. Aucun chemin n'est spécifié. | VDA 19.12 et versions ultérieures |
| Taille de la couche utilisateur en Go | 10 Go. Une couche utilisateur est un disque à allocation dynamique qui s'étend à la taille définie. Les couches utilisateur ne diminuent jamais en taille. | VDA 19.12 ou versions ultérieures |

### Virtual Delivery Agent

| Nom | Paramètre par défaut | VDA |
| --- | --- | --- |
| Masque réseau IPv6 d'enregistrement du contrôleur | Aucun masque réseau n'est spécifié. | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Port d'enregistrement du contrôleur | 80 | Toutes les versions VDA |
| SID de Contrôleur | Aucun SID n'est spécifié. | Toutes les versions VDA |
| Controller | Aucun contrôleur n'est spécifié. | Toutes les versions VDA |
| Activer la mise à jour automatique des contrôleurs | Activé | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| Uniquement utiliser l'enregistrement du contrôleur IPv6 | Désactivé | VDA pour OS multi-session 7 jusqu'à la version actuelle, VDA pour OS mono-session 7 jusqu'à la version actuelle |
| GUID de site | Aucun GUID n'est spécifié. | Toutes les versions VDA |

### Virtual Delivery Agent/HDX 3D Pro

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Activer sans perte | Activé | VDA 5.5, 5.6 FP1 |
| Paramètres de qualité HDX 3D Pro | | VDA 5.5, 5.6 FP1 |

### Virtual Delivery Agent/Surveillance

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Activer le suivi des processus | Désactivé | VDA 7.11 jusqu'à la version actuelle |
| Activer le suivi des ressources | Activé | VDA 7.11 jusqu'à la version actuelle |

### Adresse IP virtuelle

| Nom | Paramètre par défaut | VDA |
|---|---|---|
| Prise en charge du bouclage d'adresse IP virtuelle | Désactivé | VDA 7.6 jusqu'à la version actuelle |
| Liste de programmes de bouclage virtuel d'adresse IP virtuelle | Aucun | VDA 7.6 jusqu'à la version actuelle |

## Référence des paramètres de stratégie

June 27, 2024

Les stratégies contiennent des paramètres qui sont mis en œuvre lorsqu'elles sont appliquées. Les descriptions de cette section indiquent également si des paramètres supplémentaires sont requis pour activer une fonctionnalité ou sont similaires à un paramètre.

### Référence rapide

Les tableaux suivants présentent les paramètres que vous pouvez configurer au sein d'une stratégie. Recherchez la tâche que vous souhaitez effectuer dans la colonne de gauche, puis situez le paramètre

qui lui correspond dans la colonne de droite.

Une liste complète de tous les paramètres de stratégie est disponible au format .CHM ( HTML compilé) et .CSV. Ces fichiers sont disponibles dans le dossier `\program files\citrix\grouppolicy` sur le serveur sur lequel le broker (Delivery Controller) est installé. Vous pouvez également télécharger la dernière version des paramètres de stratégie en cliquant ici.

### Audio

| Pour cette tâche | Utilisez ce paramètre de stratégie |
|---|---|
| Spécifier si l'utilisation de plusieurs périphériques audio est autorisée | Audio Plug N Play |
| Spécifier si l'entrée audio des microphones sur la machine utilisateur est autorisée | Redirection du microphone client |
| Contrôler la qualité audio sur la machine utilisateur | Qualité audio |
| Contrôler le mappage audio vers les haut-parleurs sur la machine utilisateur | Redirection audio cliente |

### Bande passante des machines utilisateur

| Pour limiter la bande passante utilisée pour | Utilisez ce paramètre de stratégie |
|---|---|
| Mappage audio client | Limite de bande passante de redirection audio ou Pourcentage de limite de bande passante de redirection audio |
| La copie et le collage à l'aide du Presse-papiers local | Limite de bande passante de redirection du Presse-papiers ou Pourcentage de limite de bande passante de redirection du Presse-papiers |
| L'accès aux lecteurs clients locaux dans les sessions | Limite de bande passante de redirection de fichier ou Pourcentage de limite de bande passante de redirection de fichier |
| Accélération multimédia HDX MediaStream | Limite de bande passante d'accélération multimédia HDX MediaStream ou Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream |
| Session cliente | Limite de bande passante de session générale |

| Pour limiter la bande passante utilisée pour | Utilisez ce paramètre de stratégie |
| --- | --- |
| Impression | Limite de bande passante de redirection d'imprimante ou Pourcentage de limite de bande passante de redirection de l'imprimante |
| Périphériques TWAIN (appareils photo, scanners, etc.) | Limite de bande passante de redirection du périphérique TWAIN ou Pourcentage de limite de bande passante de redirection du périphérique TWAIN |
| Périphériques USB | Limite de bande passante de redirection du périphérique USB client ou Pourcentage de limite de bande passante de redirection du périphérique USB client |

### Redirection des lecteurs clients et de machines utilisateur

| Pour cette tâche | Utilisez ce paramètre de stratégie |
| --- | --- |
| Spécifier si les lecteurs de la machine utilisateur sont connectés lorsque les utilisateurs se connectent au serveur | Connecter automatiquement les lecteurs clients |
| Contrôler le transfert des données copiées ou coupées entre le serveur et le Presse-papiers local | Redirection du Presse-papiers client |
| Déterminer la méthode de mappage des lecteurs de la machine utilisateur | Redirection de lecteur client |
| Contrôler si les disques durs locaux des utilisateurs sont disponibles dans une session | Lecteurs fixes clients et Redirection de lecteur client |
| Contrôler si les lecteurs de disquette locaux des utilisateurs sont disponibles dans une session | Lecteurs de disquette clients et Redirection du lecteur client |
| Contrôler si les lecteurs réseau des utilisateurs sont disponibles dans une session | Lecteurs réseau clients et Redirection du lecteur client |
| Contrôler si les lecteurs de CD, de DVD ou Blu-ray locaux des utilisateurs sont disponibles dans une session | Lecteurs optiques clients et Redirection du lecteur client |
| Contrôler si les lecteurs amovibles locaux des utilisateurs sont disponibles dans une session | Lecteurs amovibles clients et Redirection de lecteur client |

| Pour cette tâche | Utilisez ce paramètre de stratégie |
| --- | --- |
| Contrôler si les périphériques TWAIN des utilisateurs, tels que les scanners et les appareils photo, sont disponibles dans une session et contrôler la compression des transferts de données d'image | Redirection de périphérique TWAIN client ; Redirection de compression TWAIN |
| Contrôler si les périphériques USB sont disponibles dans une session | Redirection de périphérique USB client et règles de redirection de périphérique USB client |
| Améliorer la vitesse d'écriture et de copie des fichiers sur les disques clients via des réseaux étendus | Utiliser les écritures asynchrones |

### Redirection de contenu

| Pour cette tâche | Utilisez ce paramètre de stratégie |
| --- | --- |
| Choisir d'utiliser ou non la redirection de contenu des serveurs vers la machine utilisateur | Redirection hôte vers client |

### Interface de bureau

| Pour cette tâche | Utilisez ce paramètre de stratégie |
| --- | --- |
| Choisir d'utiliser ou non le papier peint du bureau dans les sessions des utilisateurs | Papier peint du bureau |
| Afficher le contenu d'une fenêtre pendant son déplacement | Afficher le contenu de la fenêtre lors d'un cliquer déplacer |

### Graphiques et multimédia

> **Important :**
>
> La stratégie Flash est conservée uniquement pour permettre aux clients disposant d'anciens VDA d'utiliser des contrôleurs plus récents (par exemple, les contrôleurs de la version 1912) tout en continuant à utiliser Flash. Cette version de VDA ne prend pas en charge Flash.

| Pour cette tâche | Utilisez ce paramètre de stratégie |
| --- | --- |
| Choisir le nombre maximal de trames par seconde envoyées depuis les bureaux virtuels vers les machines utilisateur | Taux de trames cible |
| Contrôler la qualité visuelle des images affichées sur la machine utilisateur | Qualité visuelle |
| Indiquer si les sites Web peuvent afficher du contenu Flash lors de l'accès aux sessions | Liste d'adresse URL de récupération de contenu Flash côté serveur ; Liste de compatibilité d'adresses URL Flash ; Paramètre de stratégie de prévention du retour à la vidéo Flash ; Erreur *.swf de prévention du retour à la vidéo Flash |
| Contrôler la compression de la vidéo rendue par le serveur | Utiliser codec vidéo pour la compression ; Utiliser le codage matériel pour le codec vidéo |
| Contrôler la diffusion du contenu Web multimédia HTML5 pour les utilisateurs | Redirection vidéo HTML5 |

### Définition des priorités du trafic réseau multi-stream

| Pour cette tâche | Utilisez ce paramètre de stratégie |
| --- | --- |
| Spécifier les ports pour le trafic ICA au travers de plusieurs connexions et établir des priorités de réseau | Stratégie Multi-Port |
| Activer la prise en charge des connexions multi-stream entre les serveurs et les machines utilisateur | Multi-Stream (paramètres ordinateur et utilisateur) |

### Imprimer

| Pour cette tâche | Utilisez ce paramètre de stratégie |
| --- | --- |
| Contrôler la création des imprimantes clientes sur la machine utilisateur | Créer automatiquement les imprimantes clientes et Redirection d'imprimante cliente |
| Choisir l'emplacement où les propriétés de l'imprimante sont stockées | Rétention des propriétés de l'imprimante |
| Définir si le client ou le serveur traite les requêtes d'impression | Diriger les connexions vers les serveurs d'impression |

| Pour cette tâche | Utilisez ce paramètre de stratégie |
| --- | --- |
| Indiquer si les utilisateurs peuvent accéder aux imprimantes connectées à leurs machines utilisateur | Redirection d'imprimante cliente |
| Contrôler l'installation des pilotes Windows natifs lors de la création automatique des imprimantes client et réseau | Installation automatique de pilotes d'imprimante fournis par défaut |
| Indiquer quand utiliser le pilote d'imprimante universel | Utilisation du pilote d'impression universelle |
| Choisir une imprimante en fonction des informations de la session de l'utilisateur itinérant | Imprimante par défaut |
| Équilibrer la charge et définir le seuil de basculement pour les serveurs d'impression universels | Serveurs d'impression universelle d'équilibrage de la charge ; Seuil au-delà duquel les serveurs d'impression universelle sont hors service |

> **Remarque :**
>
> Les stratégies ne peuvent pas être utilisées pour activer un écran de veille dans une session de bureau ou d'application. Pour les utilisateurs qui ont besoin d'économiseurs d'écran, l'économiseur d'écran peut être implémenté sur la machine utilisateur.

## Paramètres de stratégie ICA

June 27, 2024

> **Remarque :**
>
> Cette page fournit des descriptions et les valeurs de configuration prises en charge pour les paramètres de stratégie ICA. Pour plus d'informations sur l'utilisation des stratégies, consultez la section Utiliser les stratégies .

### Transport adaptatif

Ce paramètre autorise ou empêche le transport de données via l'EDT comme transport principal et le retour vers TCP.

Par défaut, le transport adaptatif est activé (**Préféré**), et EDT est utilisé autant que possible, avec retour vers TCP. Vous pouvez modifier ses paramètres selon vos besoins :

- **Préféré**. Le transport adaptatif via EDT est utilisé autant que possible, avec retour vers TCP.
- **Mode de diagnostic**. EDT est activé de force et le retour vers TCP est désactivé. Nous vous recommandons de n'utiliser ce paramètre qu'à des fins de dépannage.
- **Désactivé**. TCP est activé de force et EDT est désactivé.

Pour plus d'informations, consultez la section Transport adaptatif.

### Paramètre Glisser-déplacer

Ce paramètre autorise ou empêche le déplacement de fichiers entre le client et les applications ou bureaux virtuels. Par défaut, la stratégie Glisser-déplacer est désactivée. Vous pouvez activer cette stratégie si nécessaire.

### Délai d'attente de lancement des applications

Ce paramètre spécifie le délai d'attente en millisecondes pendant lequel une session attend que la première application démarre. Si le démarrage de l'application dépasse ce délai, la session se termine.

Vous pouvez choisir le délai par défaut (10 000 millisecondes) ou spécifier un nombre de millisecondes.

### Redirection du Presse-papiers client

Ce paramètre permet d'autoriser ou d'empêcher le mappage du Presse-papiers sur la machine utilisateur au Presse-papiers du serveur.

Par défaut, la redirection du Presse-papiers est autorisée.

Pour empêcher le transfert des données par copier-coller entre une session et le Presse-papiers local, sélectionnez **Interdire**. Les utilisateurs peuvent toujours copier-coller des données entre les applications exécutées dans les sessions.

Après avoir autorisé ce paramètre, configurez la bande passante maximale autorisée que le Presse-papiers peut consommer dans une connexion client. Utilisez la **limite de bande passante de redirection du Presse-papiers** ou les paramètres de **pourcentage de limite de bande passante de redirection du Presse-papiers**.

**Formats d'écriture autorisés dans le Presse-papiers client**

Lorsque le paramètre **Restreindre écriture dans le Presse-papiers client** est **activé**, les données du Presse-papiers hôte ne peuvent pas être partagées avec le point de terminaison client. Vous pouvez utiliser ce paramètre pour autoriser des formats de données spécifiques à être partagés avec le Presse-papiers de point de terminaison client. Pour utiliser ce paramètre, activez-le et ajoutez les formats spécifiques à autoriser.

Les formats de Presse-papiers suivantes sont définis par le système :

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Les formats de Presse-papiers suivants sont prédéfinis dans XenApp et XenDesktop et Citrix Virtual Apps and Desktops :

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- CFX_FILE

Le format HTML est désactivé par défaut. Pour activer cette fonctionnalité :

- Vérifiez que le paramètre **Redirection de Presse-papiers client** est défini sur **Autorisé**.
- Vérifiez que le paramètre **Restreindre écriture dans le Presse-papiers client** est défini sur **Activé**.
- Ajoutez une entrée pour **CF_HTML** (et les formats que vous souhaitez prendre en charge) dans **Formats d'écriture autorisés dans le Presse-papiers client**.

Vous pouvez ajouter d'autres formats personnalisés. Le nom de format personnalisé doit correspondre aux formats à enregistrer avec le système. Les noms de format sont sensibles à la casse.

Ce paramètre ne s'applique pas si la stratégie **Redirection de Presse-papiers client** est définie sur **Interdit** ou si la stratégie **Restreindre l'écriture dans le Presse-papiers client** est définie sur **Désactivé**.

> **Remarque :**
>
> L'activation de la prise en charge de la copie Presse-papiers du format HTML (CF_HTML) copie les scripts depuis la source du contenu copié vers la destination. Assurez-vous que vous faites confiance à la source avant d'effectuer la copie. Si vous copiez un contenu contenant des scripts, ils ne seront actifs que si vous enregistrez le fichier de destination en tant que fichier HTML et l'exécutez.

#### Limiter le client du presse-papiers à la taille de transfert de la session

Ce paramètre spécifie la taille maximale des données du Presse-papiers qu'un utilisateur peut transférer d'un point de terminaison client vers une session virtuelle au cours d'une opération de copier-coller unique.

Pour limiter la taille du transfert du Presse-papiers, activez le paramètre **Limiter le client du Presse-papiers à la taille de transfert de la session**. Ensuite, dans le champ **Limite de taille**, entrez une valeur en kilo-octets pour définir la taille du transfert de données entre le Presse-papiers local et une session.

Par défaut, ce paramètre est désactivé et aucune limite sur les transferts entre le client et une session n'est définie.

#### HDX Direct

HDX Direct permet aux clients d'établir automatiquement une connexion directe avec l'hôte de session lorsqu'une communication directe est disponible. Les connexions sont établies de manière sécurisée à l'aide d'un cryptage au niveau du réseau.

#### Mode HDX Direct

HDX Direct peut être utilisé pour établir des connexions directes avec les hôtes de session pour les clients internes et externes. Ce paramètre détermine si HDX Direct est disponible pour les clients internes uniquement ou pour les clients internes et externes.

Lorsqu'il est réglé sur **Interne** uniquement, HDX Direct tente d'établir des connexions directes pour les clients du réseau interne uniquement.

Lorsqu'il est réglé sur **Interne** et **Externe**, HDX Direct tente d'établir des connexions directes pour les clients internes et externes.

Par défaut, HDX Direct est configuré pour les clients internes uniquement.

#### Plage de ports de HDX Direct

La plage de ports utilisés par HDX Direct pour les connexions provenant d'utilisateurs externes.
Par défaut, HDX Direct utilise la plage de ports : 55000—55250.

#### Limiter la session du Presse-papiers à la taille de transfert du client

Ce paramètre spécifie la taille maximale des données du Presse-papiers qu'un utilisateur peut transférer d'une session virtuelle vers un point de terminaison client au cours d'une opération de copier-coller unique.

Pour limiter la taille du transfert du Presse-papiers, activez le paramètre **Limiter la session du Presse-papiers à la taille de transfert du client**. Ensuite, dans le champ **Limite de taille**, entrez une valeur en kilo-octets pour définir la taille du transfert de données entre une session et le Presse-papiers local.

Par défaut, ce paramètre est désactivé et aucune limite sur les transferts entre le client et une session n'est définie.

#### Restreindre écriture dans le Presse-papiers client

Si ce paramètre est **Activé**, les données du Presse-papiers hôte ne peuvent pas être partagées avec le point de terminaison client. Vous pouvez autoriser des formats spécifiques en activant le paramètre **Formats autorisés d'écriture dans le Presse-papiers client**.

Par défaut, ce paramètre est **Désactivé**.

**Restreindre écriture dans le Presse-papiers de session**

Si ce paramètre est **Activé**, les données du Presse-papiers client ne peuvent être partagées dans la session utilisateur. Vous pouvez autoriser des formats spécifiques en activant le paramètre **Formats autorisés d'écriture dans le Presse-papiers de session**.

Par défaut, ce paramètre est **Désactivé**.

**Formats d'écriture autorisés dans le Presse-papiers de session**

Lorsque le paramètre **Restreindre l'écriture dans le Presse-papiers de session** est défini sur **Activé**, les données du Presse-papiers client ne peuvent être partagées avec les applications de session. Vous pouvez utiliser ce paramètre pour autoriser des formats de données spécifiques à être partagés avec le Presse-papiers de session.

Les formats de Presse-papiers suivantes sont définis par le système :

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Les formats de Presse-papiers suivants sont prédéfinis dans XenApp et XenDesktop et Citrix Virtual Apps and Desktops :

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

Le format HTML est désactivé par défaut. Pour activer cette fonctionnalité :

- Vérifiez que le paramètre **Redirection de Presse-papiers client** est défini sur **Autorisé**.
- Vérifiez que le paramètre **Restreindre écriture dans le Presse-papiers de session** est défini sur **Activé**.
- Ajoutez une entrée pour **CF_HTML** (et les formats que vous souhaitez prendre en charge) dans **Formats d'écriture autorisés dans le Presse-papiers de session**.

Vous pouvez ajouter d'autres formats personnalisés. Le nom de format personnalisé doit correspondre aux formats à enregistrer avec le système. Les noms de format sont sensibles à la casse.

Ce paramètre ne s'applique pas si la stratégie **Redirection de Presse-papiers client** est définie sur **Interdit** ou si la stratégie **Restreindre l'écriture dans le Presse-papiers de session** est définie sur **Désactivé**.

> **Remarque :**
>
> L'activation de la prise en charge de la copie Presse-papiers du format HTML (CF_HTML) copie les scripts depuis la source du contenu copié vers la destination. Assurez-vous que vous faites confiance à la source avant d'effectuer la copie. Si vous copiez un contenu contenant des scripts, ils ne seront actifs que si vous enregistrez le fichier de destination en tant que fichier HTML et l'exécutez.

### Le bureau démarre

Ce paramètre autorise ou empêche la connexion à une session sur ce VDA à l'aide d'une connexion ICA par des utilisateurs qui ne sont pas des administrateurs d'un groupe d'utilisateurs DirectAccess dans un VDA.

Par défaut, les utilisateurs qui ne sont pas des administrateurs ne peuvent pas se connecter à ces sessions.

Ce paramètre n'a aucun effet sur les utilisateurs qui ne sont pas des administrateurs d'un groupe d'utilisateurs DirectAccess dans un VDA et qui utilisent une connexion Bureau à distance. Ces utilisateurs peuvent se connecter au VDA que ce paramètre soit activé ou désactivé. Ce paramètre n'a aucun effet sur les utilisateurs qui ne sont pas des administrateurs n'appartenant pas à un groupe d'utilisateurs DirectAccess dans un VDA. Ces utilisateurs peuvent se connecter au VDA que ce paramètre soit activé ou désactivé.

### Redirection FIDO2

Ce paramètre active ou désactive la redirection FIDO2. La redirection FIDO2 permet aux utilisateurs de tirer parti des composants FIDO2 du point de terminaison local dans une machine virtuelle. Les utilisateurs peuvent s'authentifier dans leur session virtuelle à l'aide des clés de sécurité FIDO2 ou de la biométrie intégrée sur des périphériques dotés du TPM 2.0 et de Windows Hello.

Lorsque ce paramètre est défini sur **Autorisé**, les utilisateurs peuvent effectuer l'authentification FIDO2 à l'aide des fonctionnalités du point de terminaison local. Par défaut, ce paramètre est **autorisé**.

### Expiration de délai de la connexion à l'écouteur ICA

Ce paramètre spécifie le temps d'attente maximal d'établissement d'une connexion utilisant le protocole ICA.

Par défaut, le temps d'attente maximal est de 120 000 millisecondes, soit deux minutes.

### Numéro de port de l'écouteur ICA

Ce paramètre spécifie le numéro de port TCP/IP utilisé par le protocole ICA sur le serveur.

Le numéro port est défini par défaut sur 1494.

Les numéros de port doivent être compris entre 0 et 65535 et ne doit pas entrer en conflit avec d'autres ports identifiés. Si vous modifiez le numéro de port, redémarrez le serveur pour prendre en compte la nouvelle valeur. Si vous modifiez le numéro de port sur le serveur, vous devez également le modifier sur chaque application Citrix Workspace ou plug-in qui se connecte à ce serveur.

### Éditeur de méthode de clavier et d'entrée (IME)

Ce paramètre active ou désactive les éléments suivants :

- Synchronisation dynamique de la disposition du clavier
- Éditeur de méthode d'entrée (IME)
- Mappage de disposition du clavier Unicode
- Masquage ou affichage de la boîte de dialogue de notification liée au changement de la disposition du clavier

1. Dans Web Studio, sélectionnez **Clavier et IME**.
2. Sélectionnez **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME** pour contrôler la synchronisation dynamique de la disposition du

clavier et les fonctionnalités IME (Input Method Editor) du client générique dans le VDA. Vous pouvez configurer les éléments suivants :

**Désactivé** : synchronisation dynamique de la disposition du clavier et éditeur de méthode d'entrée (IME) du client générique.

**Prise en charge de la synchronisation dynamique de la disposition du clavier client** : active la synchronisation dynamique de la disposition du clavier.

**Prise en charge de la synchronisation dynamique de la disposition du clavier client et des améliorations apportées à l'éditeur IME** : active à la fois la synchronisation dynamique de la disposition du clavier et l'éditeur de méthode d'entrée (IME) du client générique.

3. Sélectionnez **Activer le mappage du clavier Unicode** pour activer ou désactiver le mappage du clavier Unicode.
4. Sélectionnez **Masquer la boîte de dialogue de changement de clavier** pour contrôler si un message s'affiche ou non, indiquant que la disposition du clavier se synchronise lorsque l'utilisateur modifie la disposition du clavier client. Si vous empêchez l'affichage du message, les utilisateurs doivent attendre quelques instants avant de taper pour éviter une saisie incorrecte des caractères.

Paramètres par défaut :

- **Synchronisation de la disposition du clavier client et améliorations apportées à l'éditeur IME**
  - Désactivé dans Windows Server 2016 et Windows Server 2019.
  - Prise en charge de la synchronisation dynamique de la disposition du clavier client et des améliorations apportées à l'éditeur IME dans Windows Server 2012 et Windows 2010.
- **Désactiver le mappage du clavier Unicode**
- **Afficher la boîte de dialogue de changement de clavier**

Cette stratégie remplace les paramètres de registre répertoriés dans la section **Description** des paramètres de stratégie.

### Retard du démarrage de vérification de fermeture de session

Ce paramètre spécifie la durée pendant laquelle retarder le démarrage de la vérification de fermeture de session. Cette stratégie permet de définir le délai (en secondes) pendant lequel une session client attend avant de déconnecter la session.

Ce paramètre augmente également le temps nécessaire à un utilisateur pour se déconnecter du serveur.

### Mode tolérance de pertes

> **Important :**
>
> - La fonctionnalité nécessite au minimum l'application Citrix Workspace 2002 pour Windows. Cette version du VDA le prendra en charge lorsqu'elle est disponible.
> - Le mode tolérance de pertes pour les graphiques n'est pas pris en charge sur Citrix Gateway ou Citrix Gateway Service. Ce mode n'est disponible qu'avec des connexions directes.

Ce paramètre active ou désactive le mode tolérance de pertes pour les graphiques.

Par défaut, le mode tolérance de pertes pour les graphiques est défini sur **Autorisé**.

Lorsqu'il est autorisé, le mode est activé lorsque la perte de paquets et la latence dépassent un certain seuil. Vous pouvez définir les seuils à l'aide de la stratégie des seuils de tolérance de pertes.

### Seuils de tolérance de pertes

Lorsque le Mode tolérance de pertes est disponible, ce paramètre indique les seuils de mesures réseau qui font passer la session en mode tolérance de pertes pour les graphiques.

Les seuils par défaut sont :

- Perte de paquets : 5 %
- Latence : 300 ms (RTT)

Pour de plus amples informations, consultez Mode tolérance de pertes.

### Mode de tolérance de pertes pour l'audio

Ce paramètre active ou désactive le mode tolérance de pertes pour le son.

Lorsque cette option est activée, le son est envoyé via le mode tolérance de pertes.

Par défaut, le mode tolérance de pertes pour le son est **Interdit**.

Pour activer la stratégie, modifiez le registre du mode tolérance de pertes pour la stratégie audio sur **Autorisé**.

Le transport EDT est requis pour activer le mode tolérance de pertes pour le son.

### Protocole Rendezvous

Ce paramètre modifie la façon dont les sessions HDX sont transmises par proxy lors de l'utilisation du service Citrix Gateway. Lorsque cette option est activée, le trafic HDX ne circule plus dans Citrix Cloud

Connector. Au lieu de cela, le VDA établit une connexion sortante directement avec Citrix Gateway Service (améliorant l'évolutivité du Cloud Connector).

> **Important :**
>
> Une bascule de fonctionnalité dans Citrix Cloud et un paramètre de stratégie HDX contrôlent cette fonctionnalité. Le commutateur de fonctionnalité Citrix Cloud est activé par défaut tandis que le paramètre HDX est désactivé par défaut. Le paramètre HDX affecte uniquement les sessions HDX établies via Citrix Gateway Service. Les sessions établies directement entre le client et le VDA ou via un Citrix Gateway local ne sont pas affectées par ce paramètre.

Pour plus d'informations, consultez Protocole Rendezvous.

### Configuration du proxy Rendezvous

Ce paramètre vous permet de configurer un proxy explicite à utiliser avec le protocole Rendezvous. Si vous utilisez un proxy transparent, ce paramètre n'a pas besoin d'être activé.

Par défaut, ce paramètre est désactivé.

Lorsqu'il est désactivé, le VDA n'achemine pas le trafic sortant via des proxy non transparents lorsqu'il tente d'établir une connexion Rendez-vous avec Gateway Service.

Lorsqu'il est activé, le VDA tente d'établir une connexion Rendez-vous avec Gateway Service via le proxy défini dans ce paramètre.

Le VDA prend en charge l'utilisation de proxy HTTP et SOCKS5 pour les connexions Rendezvous. Pour configurer le VDA afin qu'il utilise un proxy pour la connexion Rendezvous, vous devez activer ce paramètre. Vous devez également spécifier l'adresse du proxy ou le chemin d'accès au fichier PAC. Par exemple :

- Adresse proxy : `http://<URL or IP>:<port>` ou `socks5://<URL or IP>:<port>`
- Fichier PAC : `http://<URL or IP>/<path>/<filename>.pac`

  VDA version 2103 est la version minimale prise en charge pour la configuration de proxy avec un fichier PAC. Pour plus d'informations sur le schéma de fichier PAC pour les proxies SOCKS5, reportez-vous à la section Configuration du proxy.

> **Remarque :**
>
> Seuls les proxies SOCKS5 prennent en charge le transport de données via EDT. Pour un proxy HTTP, utilisez TCP comme protocole de transport pour ICA.

Pour plus d'informations, consultez Protocole Rendezvous.

### Démarrage de programmes non publiés lors de la connexion du client

Ce paramètre spécifie si les applications initiales peuvent être lancées via RDP sur le serveur.

Par défaut, le lancement d'applications via RDP sur le serveur n'est pas autorisé.

### Paramètres de stratégie Basculer en mode tablette

La stratégie Basculer en mode tablette optimise l'aspect et le comportement des applications de magasin, des applications Win32 et du shell Windows sur le VDA. Elle bascule automatiquement le bureau virtuel en mode tablette lors de la connexion à partir de périphériques de petite taille tels que des téléphones et des tablettes ou tout périphérique tactile.

Si cette stratégie est désactivée, le VDA est dans le mode défini par l'utilisateur et conserve le même mode, quel que soit le type de client.

## Paramètres de stratégie Reconnexion automatique des clients

June 27, 2024

La section **Reconnexion automatique des clients** contient des paramètres de stratégie permettant de contrôler la reconnexion automatique des sessions.

### Reconnexion automatique des clients

Ce paramètre permet d'activer ou de désactiver la reconnexion automatique par un même client après l'interruption d'une connexion.

Pour Citrix Receiver pour Windows 4.7 et versions ultérieures et l'application Citrix Workspace 1808 et versions ultérieures, la reconnexion automatique des clients utilise uniquement les paramètres de stratégie de Citrix Studio. Les mises à jour de ces stratégies dans Studio synchronisent la reconnexion automatique des clients du serveur vers le client. Avec les versions antérieures de Citrix Receiver pour Windows, pour configurer la reconnexion automatique des clients, utilisez une stratégie Studio et modifiez le Registre ou le fichier default.ica.

L'activation de la reconnexion automatique des clients permet aux utilisateurs de retrouver leur session dans l'état dans lequel elle se trouvait lors de l'interruption de la connexion. La fonction de reconnexion automatique détecte les connexions interrompues, puis reconnecte les utilisateurs à leurs sessions.

Si le cookie de l'application Citrix Workspace contenant la clé de l'ID de session et les informations d'identification n'est pas utilisé, la reconnexion automatique peut entraîner le démarrage d'une nouvelle session, plutôt que la reconnexion à une session existante. Le cookie n'est pas utilisé s'il a expiré. Par exemple, le cookie peut expirer en raison d'un délai de reconnexion ou si les informations d'identification doivent être à nouveau entrées. La reconnexion automatique du client n'est pas déclenchée lorsqu'un utilisateur se déconnecte volontairement de sa session.

Une fenêtre de session est grisée lorsqu'une reconnexion est en cours. Un minuteur affiche la durée restante avant la reconnexion de la session. Une fois que la session a expiré, elle est déconnectée.

Pour les sessions d'application, lorsque la reconnexion automatique est autorisée, un minuteur s'affiche dans la zone de notification. Ce minuteur indique la durée restante avant la reconnexion de la session. L'application Citrix Workspace essaie de reconnecter une session jusqu'à ce que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion.

Pour les sessions de bureau, si la reconnexion automatique est autorisée, l'application Citrix Workspace tente de se reconnecter à la session pendant une période de temps spécifiée, à moins que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion. Par défaut, cette durée est de cinq minutes. Pour modifier ce délai, modifiez la stratégie.

Par défaut, la reconnexion automatique des clients est autorisée. Vous pouvez le désactiver en définissant la stratégie sur **Interdit**.

### Authentification de la reconnexion automatique des clients

Ce paramètre indique si l'authentification est requise pour les reconnexions automatiques des clients.

Lorsqu'un utilisateur ouvre initialement une session, ses informations d'identification sont cryptées, stockées dans la mémoire et un cookie est créé contenant la clé de cryptage. Le cookie est envoyé à l'application Citrix Workspace. Lorsque ce paramètre est configuré, les cookies ne sont pas utilisés. Au lieu de cela, une boîte de dialogue s'affiche auprès des utilisateurs, leur demandant de fournir leurs informations d'identification lorsque l'application Citrix Workspace tente de se reconnecter automatiquement.

Par défaut, l'authentification n'est pas requise.

### Journalisation de la reconnexion automatique des clients

Ce paramètre permet d'activer ou de désactiver l'enregistrement des reconnexions automatiques des clients dans le journal d'événements.

Lorsqu'elle est activée, le Journal système du ou des serveurs reçoit les informations relatives aux échecs et aux réussites des tentatives de reconnexion automatique. Un site ne fournit pas de journal combinant les événements de reconnexion de tous les serveurs.

Par défaut, la journalisation est désactivée.

### Délai de reconnexion automatique des clients

Par défaut, le délai de reconnexion automatique des clients est réglé sur 120 secondes ; la valeur maximale configurable pour le délai de reconnexion automatique des clients est de 300 secondes. Utilisez cette stratégie pour définir la valeur du délai.

### Niveau de transparence de l'interface durant la reconnexion

Ce paramètre vous permet de spécifier le niveau d'opacité appliqué à la fenêtre de session XenApp ou XenDesktop lors du délai de reconnexion de la fiabilité de session.

Par défaut, la transparence de l'interface durant la reconnexion est définie sur 80 %.

## Paramètres de stratégie audio

June 27, 2024

La section **Audio** contient des paramètres de stratégie pour autoriser une machine utilisateur à recevoir et à envoyer des données audio dans une session sans altérer les performances.

### Audio adaptatif

Ce paramètre active ou désactive l'audio adaptatif. Lorsque vous activez cette stratégie, les paramètres de qualité audio sont ajustés de façon dynamique pour offrir la meilleure expérience utilisateur. Ce paramètre s'applique aux sessions de système d'exploitation mono-session et multi-session de VDA utilisant Citrix Virtual Apps and Desktops 2109 ou version ultérieure.

Lorsque ce paramètre est interdit, la stratégie de qualité audio est appliquée. Pour plus d'informations, reportez-vous à la section Qualité audio.

Par défaut, la stratégie Audio adaptatif est activée.

### Transport en temps réel audio via UDP

Ce paramètre permet ou empêche la transmission et la réception des données audio entre le VDA et la machine utilisateur sur RTP via le protocole UDP (User Datagram Protocol). Lorsque ce paramètre est désactivé, l'audio est envoyé et reçu sur TCP.

Par défaut, l'audio sur UDP est autorisé.

### Audio Plug N Play

Ce paramètre autorise ou empêche l'utilisation de plusieurs machines audio destinées à enregistrer et lire du son.

Par défaut, l'utilisation de plusieurs périphériques audio est autorisée.

Ce paramètre s'applique uniquement aux machines équipées du système d'exploitation multi-session Windows.

### Qualité audio

Ce paramètre spécifie le niveau de qualité sonore reçu dans les sessions utilisateur.

Par défaut, la qualité audio est définie sur Élevée : audio à définition élevée.

Pour contrôler la qualité du son, choisissez l'une des options suivantes :

- Sélectionnez Faible : pour les connexions à basse vitesse pour les connexions disposant d'une faible bande passante. Les sons envoyés à la machine utilisateur sont compressés jusqu'à 16 Kbps. Cette compression s'accompagne d'une baisse significative de la qualité du son. Mais elle permet également des performances raisonnables pour une connexion à faible bande passante.
- Sélectionnez Moyenne : optimisée pour le son de la voix pour mettre à disposition des applications Voix sur IP (VoIP). Ce paramètre met à disposition des applications multimédia pour des connexions réseau difficiles avec des lignes à moins de 512 Kbps, ou dans lesquelles les pertes de paquets sont importantes du fait de l'encombrement. Ce codec offre des temps de codage rapides, ce qui est idéal pour une utilisation avec des softphones et des applications de communications unifiées lorsque le traitement multimédia doit s'effectuer du côté serveur.

  L'audio envoyé à la machine utilisateur est compressé jusqu'à 64 Kbps. Cette compression s'accompagne d'une baisse modérée de la qualité de l'audio restitué sur la machine utilisateur, tout en offrant une faible latence et consommant une faible bande passante. Si la qualité VoIP n'est pas satisfaisante, assurez-vous que le paramètre de stratégie transport en temps réel audio via UDP est défini sur Autorisé.

À l'heure actuelle, le protocole RTP via UDP n'est pris en charge que lorsque cette qualité audio est sélectionnée. Utilisez également cette qualité audio pour la mise à disposition d'applications multimédia dans les connexions réseau difficiles comme les lignes basses (moins de 512 Kbps). Également, en cas de congestion et de perte de paquets sur le réseau.

- Pour les connexions disposant d'une bande passante élevée et pour lesquelles la qualité sonore est importante, sélectionnez Élevée : audio haute définition. Les sons sont alors transmis aux clients à leurs taux d'origine. Les sons sont compressés à un niveau de qualité similaire à la qualité CD et utilisent une bande passante maximale de 112 Kbps. La transmission d'une telle quantité de données peut solliciter l'UC de façon intensive et provoquer un engorgement du réseau.

La bande passante n'est utilisée que lors d'un enregistrement ou d'une lecture. Si les deux opérations sont effectuées en même temps, la consommation de bande passante est doublée.

Pour spécifier la quantité maximale de bande passante, configurez le paramètre **Limite de bande passante de la redirection audio** ou **Pourcentage de limite de bande passante de la redirection audio**.

### Redirection audio cliente

Ce paramètre spécifie si les applications hébergées sur le serveur peuvent lire des sons par l'intermédiaire d'un périphérique audio installé sur la machine utilisateur. Ce paramètre spécifie également si les utilisateurs peuvent enregistrer l'entrée audio.

Par défaut, la redirection audio est autorisée.

Après avoir activé ce paramètre, vous pouvez limiter la bande passante utilisée par la lecture ou l'enregistrement audio. Le fait de limiter la bande passante utilisée par l'audio peut améliorer les performances des applications, mais aussi dégrader la qualité sonore. La bande passante n'est utilisée que lors d'un enregistrement ou d'une lecture. Si les deux opérations sont effectuées en même temps, la consommation de bande passante est doublée. Pour spécifier la quantité maximale de bande passante, configurez le paramètre **Limite de bande passante de la redirection audio** ou **Pourcentage de limite de bande passante de la redirection audio**.

Sur les machines équipées d'un système d'exploitation multi-session Windows, vous devez également vous assurer que le paramètre **Plug N Play audio** est Activé pour prendre en charge plusieurs périphériques audio.

Important : l'interdiction de la redirection audio du client désactive toutes les fonctionnalités HDX audio.

### Redirection du microphone client

Ce paramètre active ou désactive la redirection du microphone client. Lorsqu'il est activé, les clients peuvent utiliser des microphones pour enregistrer l'entrée audio dans une session.

Par défaut, la redirection du microphone est autorisée.

Pour des raisons de sécurité, les utilisateurs sont avertis si des serveurs non approuvés par leurs machines clientes essaient d'accéder à leurs micros. Les utilisateurs peuvent alors accepter ou refuser l'accès. Les utilisateurs peuvent désactiver l'alerte sur l'application Citrix Workspace.

Sur les machines équipées d'un système d'exploitation multi-session Windows, vous devez également vous assurer que le paramètre Plug N Play audio est Activé pour prendre en charge plusieurs périphériques audio.

Si le paramètre **Redirection audio du client** est désactivé sur la machine cliente, cette règle n'a aucun effet.

## Paramètres de stratégie de bande passante

June 27, 2024

La section **Bande passante** contient des paramètres de stratégie pour éviter les problèmes de performances liés à l'utilisation de la bande passante des sessions clientes.

Important : l'utilisation de ces paramètres de stratégie avec les paramètres de **stratégie Multi-Stream** peut produire des résultats inattendus. Si vous utilisez les paramètres Multi-Stream dans une stratégie, assurez-vous que ces paramètres de stratégie de limite de bande passante ne sont pas inclus.

### Limite de bande passante de la redirection audio

Ce paramètre spécifie la bande passante maximale autorisée pour la lecture ou l'enregistrement de données audio dans une session utilisateur. La bande passante maximale autorisée est spécifiée en kilobits par seconde.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Pourcentage de limite de bande passante de la redirection audio**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

### Pourcentage de limite de bande passante de la redirection audio

Ce paramètre spécifie la limite de bande passante maximale autorisée pour la lecture ou l'enregistrement de données audio sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Limite de bande passante de la redirection audio**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre **Limite de bande passante globale de session** qui spécifie la bande passante totale disponible pour les sessions clientes.

### Limite de bande passante de redirection du périphérique USB client

Ce paramètre spécifie la bande passante maximale autorisée pour la redirection des périphériques USB vers et depuis le client. La bande passante maximale autorisée est spécifiée en kilobits par seconde.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Pourcentage de limite de bande passante de redirection du périphérique USB client**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

### Pourcentage de limite de bande passante de redirection du périphérique USB client

Ce paramètre spécifie la bande passante maximale autorisée pour la redirection de périphériques USB vers et depuis le client sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Limite de bande passante de redirection du périphérique USB client**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre **Limite de bande passante globale de session** qui spécifie la bande passante totale disponible pour les sessions clientes.

### Limite de bande passante de redirection du Presse-papiers

Ce paramètre spécifie la bande passante maximale autorisée pour le transfert des données entre une session et le Presse-papiers local. La bande passante maximale autorisée est spécifiée en kilobits par

seconde.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Pourcentage de limite de la bande passante de redirection du Presse-papiers**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

### Pourcentage de la limite de la bande passante de redirection du Presse-papiers

Ce paramètre spécifie la bande passante maximale autorisée pour le transfert de données entre une session et le Presse-papiers local sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Limite de bande passante de redirection du Presse-papiers**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre **Limite de bande passante globale de session** qui spécifie la bande passante totale disponible pour les sessions clientes.

### Limite de bande passante de redirection de port COM

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.

Ce paramètre spécifie la bande passante maximale autorisée, en kilobits par seconde, pour l'accès à un port COM dans une connexion cliente. Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Pourcentage de limite de bande passante de redirection du port COM**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

### Pourcentage de limite de bande passante de redirection du port COM

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.

Ce paramètre spécifie la bande passante maximale autorisée pour l'accès aux ports COM dans une connexion cliente, sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Limite de bande passante pour la redirection du port COM**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre **Limite de bande passante globale de session** qui spécifie la bande passante totale disponible pour les sessions clientes.

### Limite de bande passante de redirection de fichier

Ce paramètre spécifie la bande passante maximale autorisée pour l'accès à un lecteur client dans une session utilisateur. La bande passante maximale autorisée est spécifiée en kilobits par seconde.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Pourcentage de limite de bande passante de redirection de fichier**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

### Pourcentage de limite de bande passante de redirection de fichier

Ce paramètre spécifie la limite de bande passante maximale autorisée pour l'accès aux lecteurs clients sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Limite de bande passante de redirection de fichier**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre **Limite de bande passante globale de session** qui spécifie la bande passante totale disponible pour les sessions clientes.

### Limite de bande passante d'accélération multimédia HDX MediaStream

Ce paramètre spécifie la bande passante maximale autorisée pour la mise à disposition d'audio et de vidéo à l'aide de l'accélération multimédia HDX MediaStream. La bande passante maximale autorisée est spécifiée en kilobits par seconde.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

### Pourcentage de limite de bande passante d'accélération multimédia HDX MediaStream

Ce paramètre spécifie la bande passante maximale autorisée pour la mise à disposition d'audio et de vidéo à l'aide de l'Accélération multimédia HDX MediaStream sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Limite de bande passante d'accélération multimédia HDX MediaStream**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre **Limite de bande passante globale de session** qui spécifie la bande passante totale disponible pour les sessions clientes.

### Limite de bande passante pour la redirection du port LPT

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.

Ce paramètre spécifie la bande passante maximale autorisée pour les tâches d'impression utilisant un port LPT dans une session utilisateur unique. La bande passante maximale autorisée est spécifiée en kilobits par seconde.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Pourcentage de limite de bande passante de redirection du port LPT**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

### Pourcentage de limite de bande passante de redirection du port LPT

Remarque : pour Virtual Delivery Agent 7.0 à 7.8, configurez ce paramètre à l'aide du registre ; consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre.

Ce paramètre spécifie la limite de bande passante pour les tâches d'impression utilisant un port LPT dans une session cliente unique sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Limite de bande passante pour la redirection du port LPT**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre **Limite de bande passante globale de session** qui spécifie la bande passante totale disponible pour les sessions clientes.

### Limite de bande passante de session générale

Ce paramètre spécifie la bande passante totale disponible, en kilobits par seconde, pour les sessions utilisateur.

La limite de bande passante maximale exécutoire est de 20 Mbps (20 000 Kbps). Par défaut, aucun maximum (zéro) n'est spécifié.

Le fait de limiter la bande passante utilisée par une connexion cliente peut améliorer les performances lorsque d'autres applications en dehors de la connexion cliente sont en concurrence et que la bande passante disponible est réduite.

### Limite de bande passante de redirection d'imprimante

Ce paramètre spécifie la bande passante maximale autorisée pour l'accès à des imprimantes dans une session utilisateur. La bande passante maximale autorisée est spécifiée en kilobits par seconde.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Pourcentage de limite de bande passante de redirection de l'imprimante**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

### Pourcentage de limite de bande passante de redirection de l'imprimante

Ce paramètre spécifie la bande passante maximale autorisée pour l'accès aux imprimantes clientes sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Limite de bande passante de redirection d'imprimante**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre **Limite de bande passante globale de session** qui spécifie la bande passante totale disponible pour les sessions clientes.

### Limite de bande passante de redirection du périphérique TWAIN

Ce paramètre spécifie la bande passante maximale autorisée pour le contrôle des périphériques d'images TWAIN à partir d'applications publiées. La bande passante maximale autorisée est spécifiée en kilobits par seconde.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Pourcentage de limite de bande passante de redirection du périphérique TWAIN**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

### Pourcentage de limite de bande passante de redirection du périphérique TWAIN

Ce paramètre spécifie la bande passante maximale autorisée pour le contrôle des périphériques d'images TWAIN à partir d'applications publiées sous forme de pourcentage de la bande passante totale de session.

Par défaut, aucun maximum (zéro) n'est spécifié.

Si vous entrez une valeur pour ce paramètre et une autre pour le paramètre **Limite de bande passante de redirection du périphérique TWAIN**, le paramètre le plus restrictif (ayant la valeur la plus faible) s'applique.

Si vous configurez ce paramètre, vous devez également configurer le paramètre **Limite de bande passante globale de session** qui spécifie la bande passante totale disponible pour les sessions clientes.

## Paramètres de stratégie Redirection bidirectionnelle du contenu

June 27, 2024

La section **Redirection bidirectionnelle du contenu** contient des paramètres de stratégie permettant d'activer ou de désactiver la redirection d'adresse URL du client vers le VDA et du VDA vers le client.

Les stratégies de serveur sont définies dans Web Studio. À partir de la version 2311 de l'application Citrix Workspace, ce paramètre remplace les trois paramètres d'ancienne génération suivants de Web Studio qui sont obsolètes :

- Autoriser la redirection bidirectionnelle du contenu
- URL autorisées à être redirigées sur le VDA

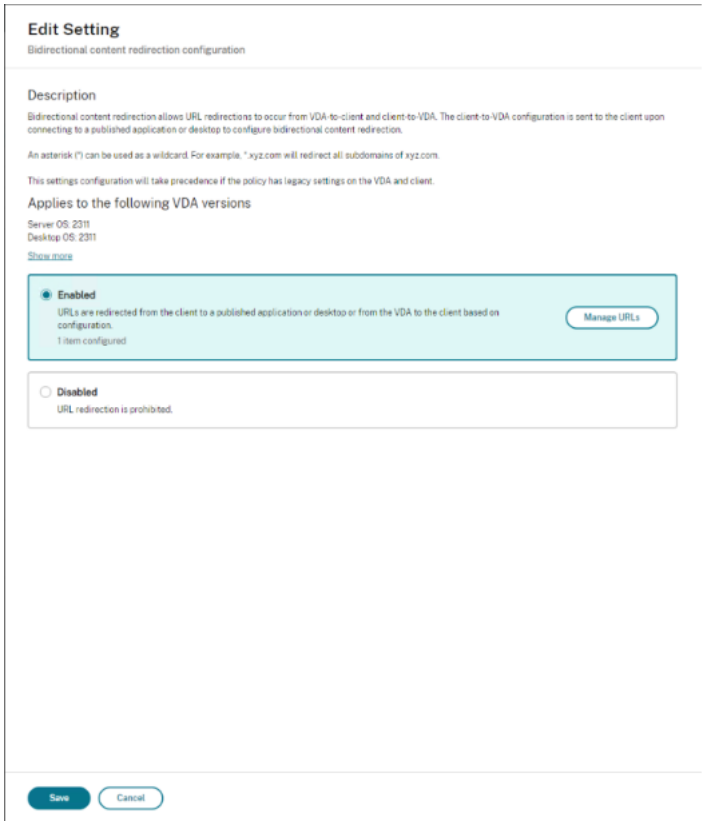
 

- URL autorisées à être redirigées sur le client

Il remplace également les trois paramètres d'objet de stratégie de groupe (GPO) locaux suivants sur les clients Windows :

- Redirection bidirectionnelle du contenu
- Remplacements de la redirection bidirectionnelle du contenu
- Redirection OAuth

Si ce paramètre est activé, les paramètres client vers VDA sont envoyés au client lors de la connexion à une application ou à un bureau publié pour configurer la redirection bidirectionnelle du contenu.




Si ce paramètre est configuré, il a priorité sur les paramètres d'ancienne génération dans Web Studio et sur le client. Citrix recommande d'utiliser uniquement les nouveaux paramètres de stratégie et de supprimer tous les paramètres existants pour éviter tout comportement inattendu.

Les stratégies client ne doivent pas être définies si le VDA et le DDC exécutent la version 2311 ou une version ultérieure. Les stratégies client sont définies depuis le modèle d'administration de l'objet de stratégie de groupe de l'application Citrix Workspace.

Citrix propose la redirection hôte vers client et Local App Access la redirection client vers URL. Toutefois, nous vous recommandons d'utiliser la redirection bidirectionnelle du contenu pour les clients Windows joints à un domaine.

Citrix recommande d'utiliser la nouvelle interface utilisateur de Web Studio pour configurer la fonctionnalité au lieu de Desktop Studio.

### Redirection par caractères génériques

La redirection bidirectionnelle du contenu prend en charge l'utilisation de caractères génériques lors de la définition des URL à rediriger. Pour plus de détails et configurer la redirection bidirectionnelle du contenu, consultez les instructions de configuration.
Dans Web Studio, définissez l'URL générique en modifiant la chaîne JSON en tant que valeur dans la clé `url` du tableau `hostToClientUrls` ou du tableau `clientToHostUrls`.

> **Remarque :**
>
> - Ne définissez pas la même URL dans `hostToClientUrls` et `clientToHostUrls` pour éviter des boucles infinies.
> - Les domaines de premier niveau ne sont pas gérés. Par exemple, https://www.citrix.* et http://www.citrix.co* ne sont pas redirigés.

### Configuration de redirection bidirectionnelle du contenu

Définissez cette stratégie sur `Enabled` pour commencer à configurer la fonctionnalité, puis cliquez sur **Gérer les URL**. Définissez les configurations suivantes :

- **Redirection VDA vers client**
- **Redirection client vers VDA**

#### Redirection VDA vers client

Pour rediriger les URL du VDA vers le client, entrez une URL par ligne. Les caractères génériques sont autorisés.
La redirection OAuth vous permet d'utiliser le navigateur sur le terminal client pour effectuer l'authentification et renvoyer le jeton au VDA.

**Avantages :**

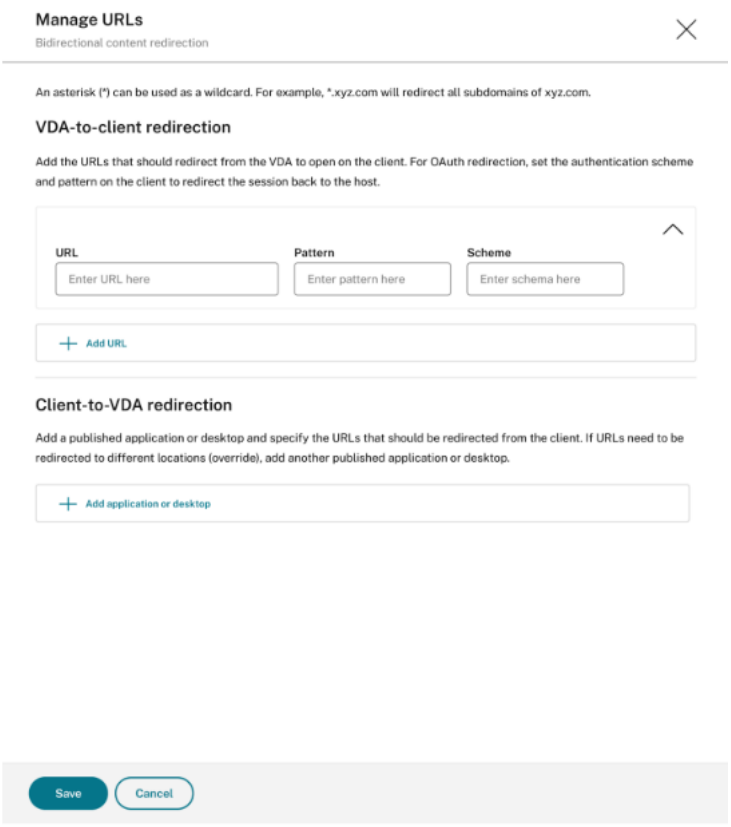
- Vous pouvez éviter de stocker ces informations d'identification dans l'environnement hébergé.
- Vous pouvez utiliser les fonctionnalités biométriques disponibles sur le terminal et non sur le VDA.

**Configurations :**

Pour configurer la redirection VDA vers client pour l'URL, spécifiez ce qui suit :

- **URL** (obligatoire) : ajoutez l'URL qui doit déclencher la redirection depuis le VDA pour s'ouvrir sur le client. Pour la **redirection OAuth**, définissez le schéma et le modèle d'authentification sur le client afin de rediriger la session vers l'hôte.
- **Modèle** (facultatif) : expression régulière d'URL qui, lorsqu'elle est redirigée vers le client via la redirection d'adresse URL du VDA vers le client, est suivie comme si un flux d'authentification OAuth avait commencé ; lorsque le flux se termine (détecté par le schéma résultant ou le modèle d'URL de redirection en cours d'ouverture), cette URL résultante est redirigée vers le VDA hôte qui a initié ce flux.
- **Schéma** (facultatif) : si un **schéma** est spécifié, l'URL de fin doit être au format : `<scheme>://<something>`. Le schéma considéré n'est pas précisé (vide). Dans ce cas, le modèle d'URL d'origine résultant est extrait du modèle via un groupe de capture d'expression régulière (doit être spécifié dans le modèle), et l'URL d'origine est réécrite pour utiliser une URL de redirection `citrix-oauth-redir://`. Une fois le flux terminé, l'URL de redirection d'origine est redirigée vers l'hôte (VDA). Dans ce cas, tout serveur d'autorisation OAuth doit être configuré pour autoriser les URL de redirection `citrix-oauth-redir://byIndex/1 (2, 3, ... N)`.




> **Remarque :**
>
> Bien que le **modèle** et le **schéma** soient facultatifs, si le **modèle** est indiqué, vous devez égale-

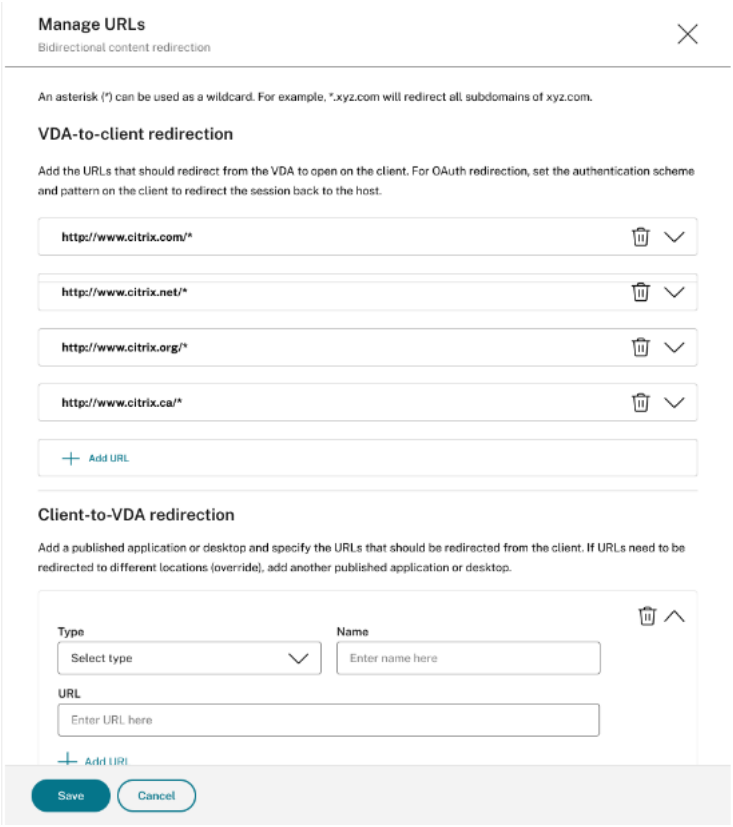
 

> ment indiquer le **schéma**.

### Redirection client vers VDA

Pour rediriger les URL du client vers le VDA, procédez comme suit :

1. Configurez la destination des URL des clients.
2. Sélectionnez Application publiée ou Bureau publié.
3. Spécifiez le nom de cette ressource.
4. Ajoutez toutes les URL qui doivent être redirigées vers cette ressource.
   Vous pouvez remplacer cette ressource par défaut en ajoutant une nouvelle application ou un nouveau bureau, puis en spécifiant les URL à rediriger vers cette ressource.




### Desktop Studio

> **Remarque :**
>
> Citrix recommande d'utiliser Web Studio pour configurer cette fonctionnalité à partir de la version 2402 de Citrix Virtual Apps and Desktops.

Pour configurer la redirection de contenu bidirectionnelle pour la version 2311, créez une chaîne JSON au format suivant :

```
{

  "version": 1,
  "hostToClientConfig": [
    {

      "hostToClientUrls": [
        {

          "url": "http://www.citrix.com/*"
         }
 ,
        {

          "url": "www.example.com"
         }
 ,
        {

          "url": "https://login.example.org/*",
          "oAuthRedirectionPattern": "https://login.example.org/oauth2
             ?.*",
          "oAuthScheme": "idm.desktop-authentication"
         }

      ]
     }

 ],
  "clientToHostConfig": [
    {

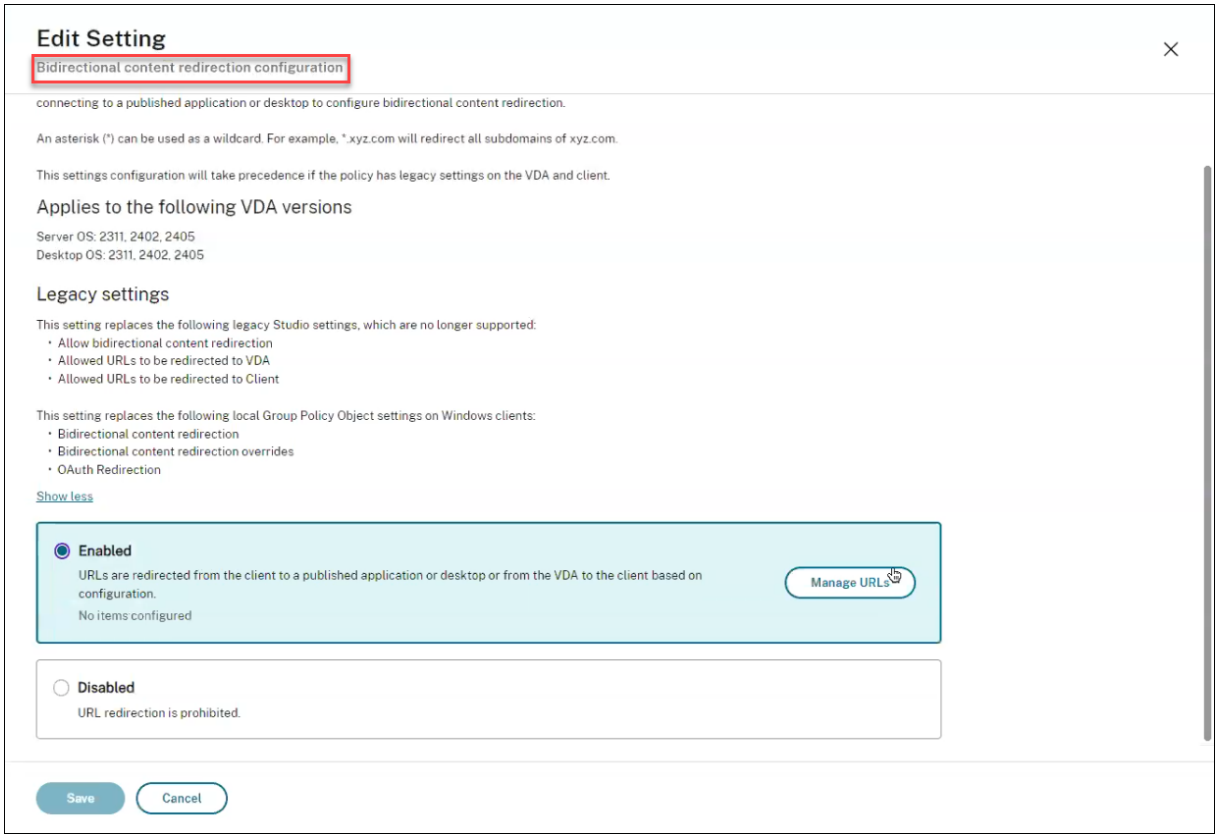
      "publishedAppOrDesktopNameType": "Desktop",
      "publishedAppOrDesktopName": "Win11Desktop",
      "clientToHostUrls": [
        "https://www.example.net",
        "https://*.citrix.example"
      ]
     }
 ,
    {

      "publishedAppOrDesktopNameType": "Application",
      "publishedAppOrDesktopName": "Chrome",
      "clientToHostUrls": [
        "https://tibco.example"
      ]
     }

 ]
}

<!--NeedCopy-->
```

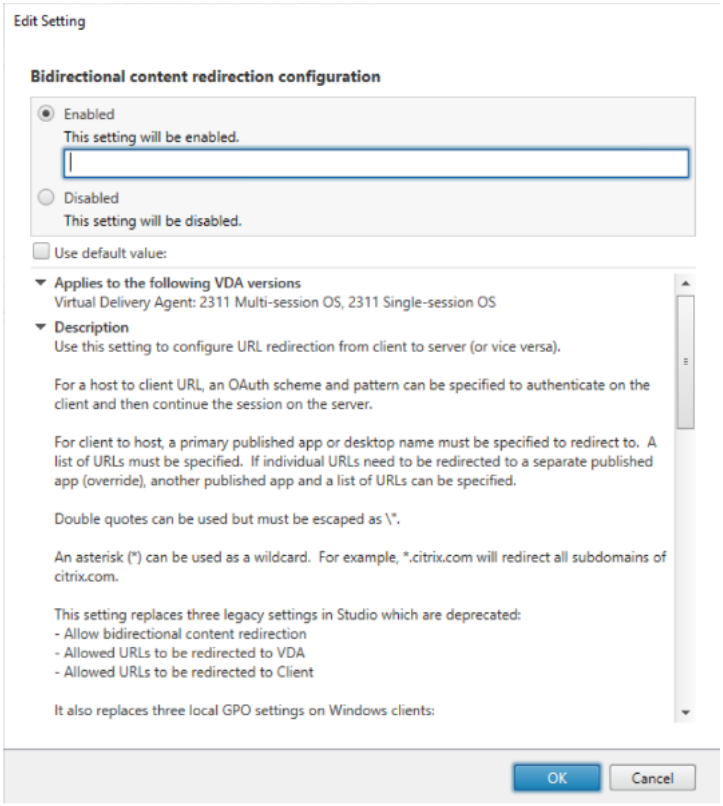
 




Les paramètres suivants doivent être définis :

- **version** : (obligatoire) définissez-le sur 1.
- Pour la redirection d'adresse URL du VDA vers le client, créez un `hostToClientConfig` unique.
- `hostToClientUrls`: (Obligatoire) Liste des URL à rediriger de l'hôte (VDA) vers le client. Les caractères génériques sont autorisés. Si `hostToClientConfig` est spécifié, mais que la redirection d'un VDA client vers l'hôte n'est pas nécessaire, vous devez spécifier `clientToHostConfig` avec `publishedAppOrDesktopNameType` et laisser `publishedAppOrDesktopName` et `clientToHostUrls` vides.




### Redirection OAuth

La redirection OAuth vous permet d'utiliser le navigateur de points de terminaison client pour effectuer l'authentification et renvoyer le jeton au VDA.

**Avantages** :

- Vous pouvez éviter de stocker ces informations d'identification dans l'environnement hébergé.
- Vous pouvez utiliser les fonctionnalités biométriques disponibles sur le terminal et non sur le VDA.

Pour configurer la redirection OAuth pour l'URL, précisez les paramètres suivants :

- **oAuthRedirectionPattern** : (facultatif) expression régulière d'URL qui, lorsqu'elle est redirigée vers le client via la redirection d'adresse URL VDA vers client, est suivie comme si un flux d'authentification OAuth avait commencé ; lorsque le flux se termine (détecté par le schéma résultant ou le modèle d'URL de redirection en cours d'ouverture), cette URL résultante est redirigée vers le VDA hôte qui a initié ce flux.
- **oAuthScheme** : (facultatif) si un schéma est spécifié, l'URL de fin doit être au format : `<scheme>://<something>`. Le schéma considéré n'est pas précisé (vide). Dans ce cas, le modèle d'URL d'origine résultant est extrait du modèle via un groupe de capture d'expression régulière

(doit être spécifié dans le modèle), et l'URL d'origine est réécrite pour utiliser une URL de redirection `citrix-oauth-redir://`. Une fois le flux terminé, l'URL de redirection d'origine est redirigée vers l'hôte (VDA). Dans ce cas, tout serveur d'autorisation OAuth doit être configuré pour autoriser les URL de redirection `citrix-oauth-redir://byIndex/1 (2, 3, ... N)`.

Pour une redirection client vers VDA, créez un paramètre **clientToHostConfig** pour chaque ressource à rediriger.
Pour chaque ressource, incluez les paramètres suivants :

- **publishedAppOrDesktopNameType** : (obligatoire) un bureau publié (« Bureau ») ou une application publiée (« Application ») configurée dans Web Studio. Si la ressource n'est pas valide, la redirection ne fonctionne pas correctement.
- **publishedAppOrDesktopName** : (obligatoire) nom de la ressource tel que configuré dans Web Studio.
- **clientToHostUrls** : (obligatoire) liste des URL à rediriger du client vers l'hôte (VDA). Les caractères génériques sont autorisés.

### Limitation connue

Lorsque vous lancez un navigateur à l'aide de PowerShell avec un schéma d'URL personnalisé (ni HTTP ni HTTPS), les URL personnalisées ne sont pas redirigées vers le client.

## Paramètres de stratégie Redirection du contenu du navigateur

June 27, 2024

La section Redirection du contenu du navigateur contient des paramètres de stratégie permettant de configurer cette fonctionnalité.

La redirection du contenu du navigateur permet de contrôler et d'optimiser la manière dont Citrix Virtual Apps and Desktops fournissent le contenu du navigateur Web (par exemple, HTML5) aux utilisateurs. Seule la zone visible du navigateur où le contenu est affiché est redirigée.

La redirection vidéo HTML5 et la redirection du contenu du navigateur sont des fonctionnalités indépendantes. Les stratégies de redirection vidéo HTML5 ne sont pas requises pour que cette fonctionnalité fonctionne. Toutefois, le service de redirection vidéo HTML5 Citrix HDX est utilisé pour la redirection du contenu du navigateur. Pour plus d'informations, consultez la section Redirection du contenu du navigateur.

> **Remarque :**
>
> Les paramètres de stratégie disponibles dans Web Studio peuvent être remplacés par des clés de registre sur le VDA, mais les clés de registre sont facultatives.

### Redirection du contenu du navigateur et TLS

Vous pouvez utiliser la redirection du contenu du navigateur pour rediriger les sites Web HTTPS. Le code JavaScript injecté sur ces sites Web doit établir une connexion TLS avec le service de redirection vidéo Citrix HDX HTML5 (WebSocketService.exe) en cours d'exécution sur le VDA. Pour obtenir cette redirection et préserver l'intégrité TLS de la page Web, le service de redirection vidéo Citrix HDX HTML5 génère deux certificats personnalisés dans le magasin de certificats sur le VDA.

HdxVideo.js utilise des sockets Secure Web pour communiquer avec WebSocketService.exe en cours d'exécution sur le VDA. Ce processus s'exécute sur le système local et effectue le mappage de session utilisateur et d'arrêt SSL.

WebSocketService.exe écoute le port 9001 127.0.0.1.

### Redirection de contenu du navigateur

Par défaut, l'application Citrix Workspace tente une récupération client et un rendu client. Le rendu côté serveur est essayé lorsque la récupération client et le rendu client échouent. Si vous activez également la stratégie de configuration du proxy de redirection du contenu du navigateur, application Citrix Workspace tente uniquement une récupération serveur et un rendu client.

Par défaut, ce paramètre est autorisé.

### Prise en charge de l'authentification Windows intégrée pour la redirection du contenu du navigateur

La redirection de contenu du navigateur active la superposition qui utilise le schéma Negotiate pour l'authentification. Cette amélioration fournit l'authentification unique à un serveur Web configuré avec l'authentification Windows intégrée (IWA) dans le même domaine que le VDA.

Lorsqu'elle est définie sur **Autorisé**, la superposition de redirection de contenu du navigateur obtient un ticket Negotiate à l'aide des informations d'identification VDA de l'utilisateur. L'utilisateur s'authentifie ensuite auprès du serveur Web avec une authentification unique.

Lorsque la valeur est **Interdite**, la superposition de redirection de contenu du navigateur ne demande pas de ticket Negotiate au VDA. L'utilisateur s'authentifie auprès d'un serveur Web à l'aide d'une

méthode d'authentification de base. Cette méthode d'authentification nécessite que les utilisateurs saisissent leurs informations d'identification VDA chaque fois qu'ils accèdent au serveur Web.

Par défaut, cette option est définie sur Interdit.

### Le serveur de redirection de contenu du navigateur récupère le paramètre d'authentification proxy Web

Ce paramètre achemine le trafic HTTP provenant d'une superposition via un proxy Web en aval. Le proxy Web en aval autorise et authentifie le trafic HTTP à l'aide des informations d'identification de domaine de l'utilisateur VDA via le schéma d'authentification Negotiate.

Vous devez configurer la redirection du contenu de navigateur pour le mode de récupération du serveur dans le fichier PAC à l'aide de la stratégie Configuration du proxy de redirection du contenu de navigateur. Dans le script PAC, fournissez des instructions pour acheminer le trafic de superposition via un proxy Web en aval. Configurez ensuite le proxy Web en aval pour authentifier les utilisateurs VDA via le schéma d'authentification Negotiate.

Lorsqu'il est défini sur **Autorisé**, le proxy Web répond avec une demande 407 Negotiate, contenant un en-tête **Proxy-Authenticate : Negotiate**. La redirection du contenu de navigateur obtient alors un ticket de service Kerberos à l'aide des informations d'identification de domaine de l'utilisateur VDA. Inclut également le ticket de service dans les demandes ultérieures adressées au proxy Web.

Lorsque la valeur est **Interdit**, la redirection du contenu de navigateur relaie tout le trafic TCP entre la superposition et le proxy Web sans interférer. La superposition utilise des informations d'authentification de base ou d'autres informations d'identification disponibles pour s'authentifier auprès du proxy Web.

Par défaut, cette option est définie sur Interdit.

### Paramètres de la stratégie de configuration de la liste de contrôle d'accès (ACL) de redirection de contenu du navigateur

Utilisez ce paramètre pour configurer une liste de contrôle d'accès (ACL) des URL pouvant utiliser la redirection du contenu du navigateur ou dont la redirection du contenu du navigateur leur est refusée.

Les URL autorisées sont les URL de la liste d'autorisation dont le contenu est redirigé vers le client.

Le caractère générique * est autorisé, mais n'est pas autorisé dans le protocole ou la partie de l'adresse de domaine de l'URL. Toutefois, à partir de Citrix Virtual Apps and Desktops 7 2206, le caractère générique * est autorisé dans la partie de l'adresse du sous-domaine de l'URL.

Autorisé : `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`, `http://*.xyz.com/`

Non autorisée : `http://*.*.com/`

Vous pouvez obtenir une meilleure granularité en spécifiant des chemins d'accès dans l'URL. Par exemple, si vous spécifiez `https://www.xyz.com/sports/index.html`, seule la page index.html est redirigée.

Par défaut, ce paramètre est défini sur `https://www.youtube.com/*`

Pour plus d'informations, consultez l'article CTX238236 du centre de connaissances.

> **Remarque :**
>
> Vous pouvez configurer l'ACL pour permettre à la redirection de contenu du navigateur de rediriger les sites Web vers le point de terminaison et les sites d'authentification peuvent être configurés pour autoriser les fournisseurs d'identité (IdP), tels qu'Okta et Duo, pour l'authentification utilisée sur l'URL configurée.

### Sites d'authentification de redirection du contenu du navigateur

Utilisez ce paramètre pour configurer une liste d'URL. Les sites redirigés à l'aide de la redirection du contenu du navigateur utilisent cette liste pour authentifier un utilisateur. Ce paramètre spécifie les URL pour lesquelles la redirection du contenu du navigateur reste active (redirigée) lors de la navigation à partir d'une URL figurant sur la liste d'autorisation.

Un scénario classique est un site Web qui utilise un fournisseur d'identité (IdP) pour l'authentification. Par exemple, un site Web `www.xyz.com` doit être redirigé vers le point de terminaison, mais un fournisseur d'identité tiers, comme Okta (`www.xyz.okta.com`), gère la partie authentification. L'administrateur utilise la stratégie de configuration ACL de redirection du contenu du navigateur pour ajouter `www.xyz.com` à la liste d'autorisation. Utilise ensuite les sites d'authentification de redirection de contenu du navigateur pour ajouter `www.xyz.okta.com` à la liste d'autorisation.

Pour plus d'informations, consultez l'article CTX238236 du centre de connaissances.

### Paramètre de liste de blocage de redirection du contenu du navigateur

Ce paramètre fonctionne avec le paramètre de configuration ACL de redirection du contenu du navigateur. Supposez que les URL sont présentes dans le paramètre de configuration ACL de redirection de contenu du navigateur et le paramètre de configuration de la liste de blocage. Dans ce cas, la configuration de la liste de blocage est prioritaire et le contenu du navigateur de l'URL n'est pas redirigé.

**URL non autorisées :** spécifie les URL sur la liste de blocage dont le contenu du navigateur n'est pas redirigé vers le client, mais rendu sur le serveur.

Le caractère générique * est autorisé, mais n'est pas autorisé dans le protocole ou la partie de l'adresse de domaine de l'URL.

Autorisée : `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

Non autorisée : `http://*.xyz.com/`

Vous pouvez obtenir une meilleure granularité en spécifiant des chemins d'accès dans l'URL. Par exemple, si vous spécifiez `https://www.xyz.com/sports/index.html`, seule la page index.html est placée dans la liste de blocage.

### Paramètre de proxy de redirection du contenu du navigateur

Ce paramètre fournit des options de configuration pour les paramètres proxy sur le VDA pour la redirection du contenu du navigateur. Si cette option est activée avec une adresse proxy et un numéro de port valides, une URL PAC/WPAD ou un paramètre Direct/Transparent, l'application Citrix Workspace essaie uniquement la récupération serveur et la restitution client.

Si elle est désactivée ou non configurée et utilise une valeur par défaut, l'application Citrix Workspace tente une récupération client et un rendu client.

Par défaut, cette option est définie sur Interdit.

**Modèle autorisé pour un proxy explicite :**

`http://\<hostname/ip address\>:\<port\>`

**Exemple :**

```
http://proxy.example.citrix.com:80
http://10.10.10.10:8080
```

**Modèles autorisés pour des fichiers PAC/WPAD :**

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

**Exemple :** `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

**Exemple :** `http://10.10.10.10/configuration/pac/wpad.dat`

**Modèles autorisés pour des proxys directs ou transparents :**

Tapez le mot **DIRECT** dans la zone de texte de la stratégie.

### Remplacements de clé du registre de redirection de contenu du navigateur

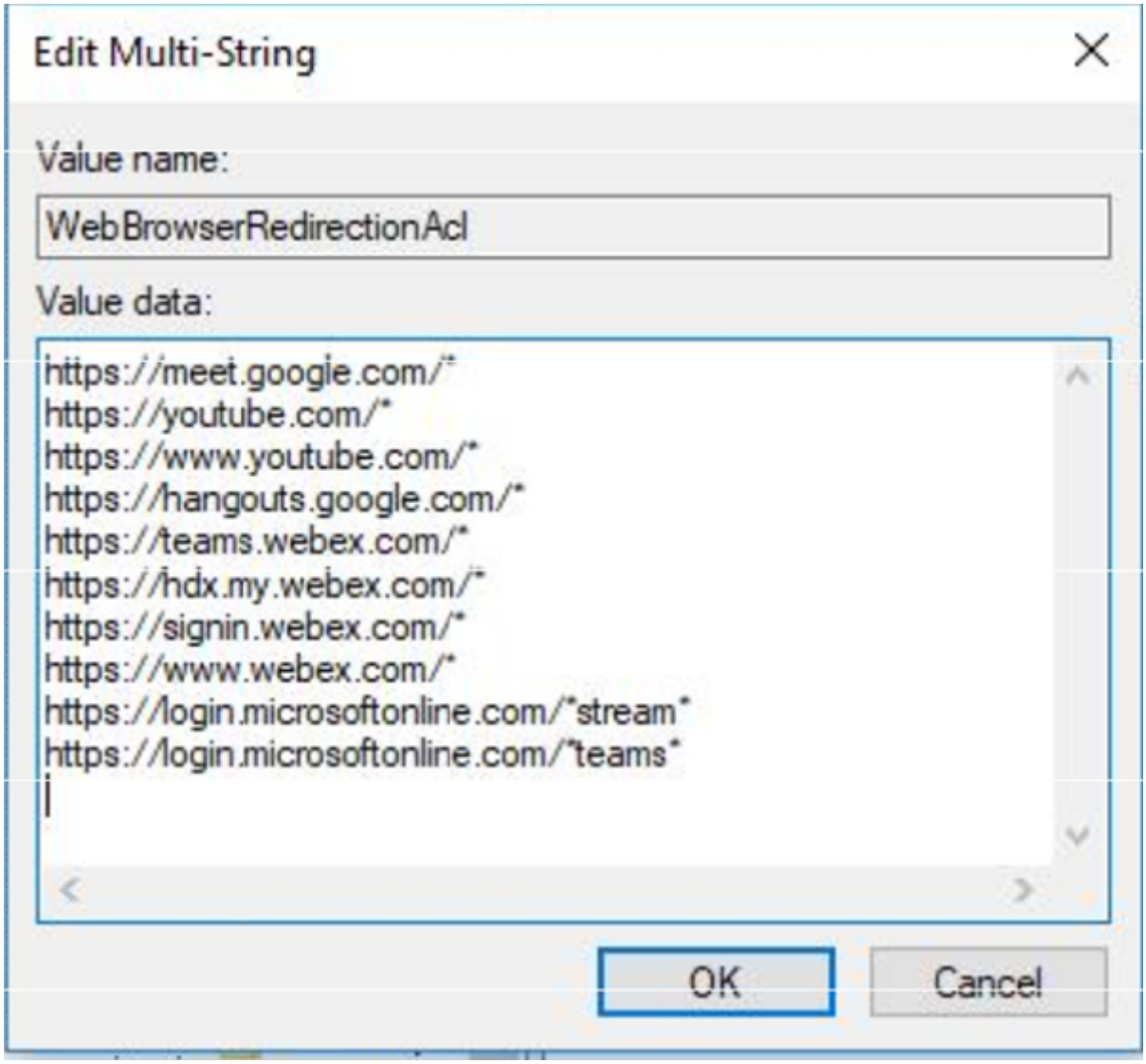
 

> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.
>
> Options de remplacement du registre pour les paramètres de stratégie :

`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

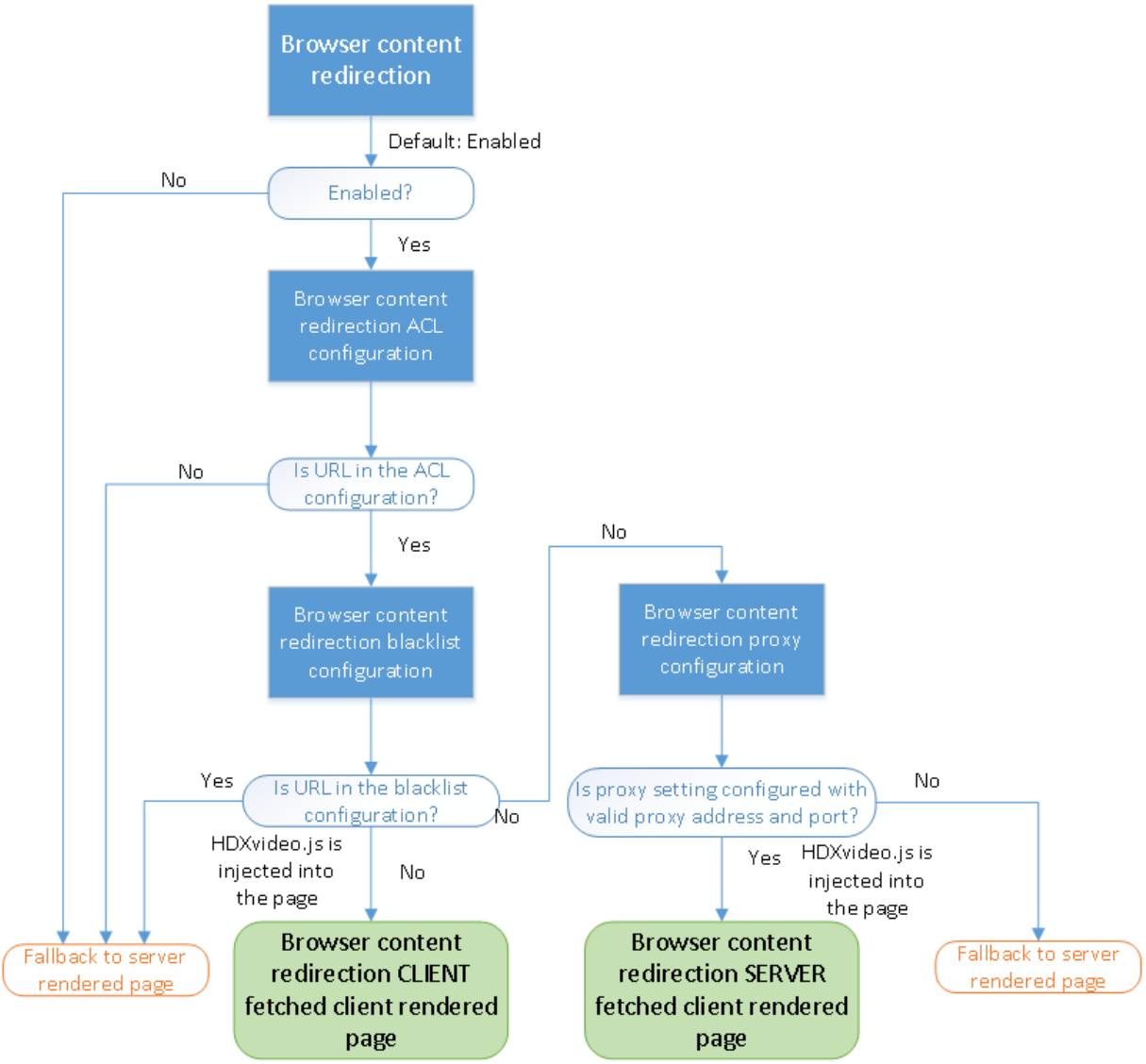
| Nom | Type | Valeur |
|---|---|---|
| WebBrowserRedirection | DWORD | 1=Autorisé, 0=Interdit |
| WebBrowserRedirectionAcl | REG_MULTI_SZ | |
| WebBrowserRedirectionAuthenticationSites | REG_MULTI_SZ | |
| WebBrowserRedirectionProxyAddress | REG_SZ | `http://myproxy.citrix.com:8080` ou `http://10.10.10.10:8888` |
| WebBrowserRedirectionBlacklist | REG_MULTI_SZ | |



### Insertion de HDXVideo.js pour la redirection du contenu du navigateur




HdxVideo.js est injecté sur la page Web à l'aide de l'extension Chrome de redirection du contenu du navigateur ou de l'objet Application d'assistance du navigateur Internet Explorer (BHO). Le BHO est un modèle de plug-in pour Internet Explorer. Il fournit des hooks pour les API de navigateur et permet au plug-in d'accéder au DOM (Document Object Model) de la page pour contrôler la navigation.

Le BHO décide si HdxVideo.js doit être injecté sur une page donnée. La décision est basée sur les stratégies d'administration illustrées dans le diagramme précédent.

Une fois qu'il a été décidé d'injecter le JavaScript et de rediriger le contenu du navigateur vers le client, la page Web du navigateur Internet Explorer sur le VDA est vierge. Définir **document.body.innerHTML** sur 'empty' supprime le corps entier de la page Web sur le VDA. La page est prête à être envoyée au client pour être affichée sur le navigateur de superposition (Hdxbrowser.exe) sur le client.

# Paramètres de stratégie Capteurs clients

June 27, 2024

La section **Capteurs clients** contient des paramètres de stratégie permettant de contrôler la manière dont les informations de capteurs d'appareils mobiles sont gérées dans une session utilisateur.

## Autoriser les applications à utiliser l'emplacement physique de la machine cliente

Ce paramètre détermine si les applications exécutées dans une session sur un appareil mobile sont autorisées à utiliser l'emplacement physique de la machine cliente.

Par défaut, l'utilisation des informations d'emplacement est interdite.

Lorsque ce paramètre est interdit, les tentatives par une application de récupération des informations d'emplacement retournent une valeur de « permission refusée ».

Lorsque ce paramètre est activé, un utilisateur peut interdire l'utilisation des informations d'emplacement en refusant une requête de l'application Citrix Workspace pour accéder à l'emplacement. Les appareils Android et iOS invitent la saisie des informations d'emplacement lors de la première requête de chaque session.

Lors du développement d'applications hébergées qui utilisent le paramètre Permettre aux applications d'utiliser l'emplacement physique de la machine cliente, considérez ce qui suit :

- Assurez-vous qu'une application pour laquelle l'emplacement est activé ne compte pas sur la disponibilité des informations d'emplacement, car :
  - Il se peut qu'un utilisateur n'ait pas accès aux informations d'emplacement.
  - Il se peut que l'emplacement ne soit pas disponible ou soit modifié lors de l'exécution de l'application.
  - Il se peut qu'un utilisateur se connecte à la session d'application depuis une machine différente qui ne prend pas en charge les informations d'emplacement.
- Une application pour laquelle l'emplacement est activé doit :
  - posséder la fonctionnalité d'emplacement désactivée par défaut ;
  - offrir une option utilisateur pour permettre ou interdire la fonctionnalité lors de l'exécution de l'application ;
  - offrir une option utilisateur pour effacer les données d'emplacement cachées par l'application. (l'application Citrix Workspace ne cache pas les données d'emplacement.)
- Une application prenant en charge la localisation doit gérer la granularité des informations d'emplacement. Cette gestion garantit que les données acquises sont adaptées à l'objectif de l'

application. Et aussi qu'elles sont conformes à la réglementation en vigueur dans toutes les juridictions pertinentes.
- Appliquez une connexion sécurisée (par exemple, en utilisant TLS ou un VPN) lors de l'utilisation des services d'emplacement. Connectez l'application Citrix Workspace aux serveurs de confiance.
- Considérez l'obtention de conseils juridiques quant à l'utilisation des services d'emplacement.

## Paramètres de stratégie Interface utilisateur de bureau

June 27, 2024

La section **UI de bureau** contient des paramètres de stratégie qui contrôlent les effets visuels, tels que le papier peint du bureau, les animations de menu et le glisser-déplacer des images. Ces paramètres de stratégie permettent de gérer la bande passante utilisée dans les connexions clientes. Vous pouvez améliorer les performances des applications sur un réseau étendu en limitant la consommation de la bande passante.

> **Important :**
>
> Nous ne prenons pas en charge le mode graphique d'ancienne génération et la Redirection de composition du Bureau (DCR) dans cette version. Cette stratégie est incluse uniquement pour des raisons de rétrocompatibilité lors de l'utilisation des produits suivants :
>
> - XenApp 7.15 LTSR
> - XenDesktop 7.15 LTSR
> - Versions précédentes de VDA avec Windows 7 et Windows 2008 R2.

### Redirection de composition du Bureau

Ce paramètre indique s'il faut utiliser la capacité de traitement des éléments suivants pour la restitution des graphiques DirectX locaux pour offrir aux utilisateurs une expérience de bureau Windows plus fluide.

- Unité de traitement graphique (GPU) sur la machine utilisateur
- Ou
- Processeur graphique intégré (IGP) sur la machine utilisateur

Lorsque cette option est activée, la **redirection de la composition du bureau** offre une expérience Windows très réactive tout en conservant une évolutivité élevée sur le serveur.

Par défaut, la **Redirection de composition du Bureau** est désactivée.

Pour désélectionner la **redirection de composition du Bureau** et réduire la bande passante requise dans les sessions utilisateur, sélectionnez **Désactivée** lorsque vous ajoutez ce paramètre à une stratégie.

### Qualité graphique de redirection Desktop Composition

Ce paramètre spécifie la qualité des graphiques utilisés pour la redirection Desktop Composition.

La valeur par défaut est Élevée.

Choisissez entre les qualités Élevée, Moyenne, Basse ou Sans perte.

### Papier peint du bureau

Ce paramètre autorise ou empêche l'affichage du papier-peint dans les sessions utilisateur.

Par défaut, les sessions utilisateur peuvent afficher le papier peint.

Pour désélectionner le papier peint et réduire la bande passante requise dans les sessions utilisateur, sélectionnez **Interdit** lorsque vous ajoutez ce paramètre à la stratégie.

### Animation de menu

Ce paramètre autorise ou empêche les animations de menu dans les sessions utilisateur.

Par défaut, l'animation de menu est autorisée.

L'animation de menu est un paramètre de préférence personnelle Microsoft destiné à faciliter l'accès. Lorsque cette option est activée, elle entraîne l'affichage d'un menu après un bref délai, en effectuant un défilement ou un fondu. Une icône de flèche s'affiche en bas du menu. Le menu s'affiche lorsque vous placez la souris sur cette flèche.

L'animation de menu est activée sur un bureau si ce paramètre de stratégie est réglé sur **Autorisé** et que le paramètre de préférence personnelle de Microsoft est activé.

> **Remarque :**
>
> Toute modification apportée au paramètre de préférence personnelle de Microsoft est apportée au bureau. Supposons que vous configurez le bureau pour qu'il ignore les modifications à la fin de la session. Dans ce cas, un utilisateur qui a activé les animations de menu peut ne pas avoir d'animation de menu dans les sessions suivantes. Pour les utilisateurs qui nécessitent l'animation de menu, activez le paramètre Microsoft dans l'image principale du bureau ou assurez-vous que le bureau conserve les modifications apportées par l'utilisateur.

### Afficher le contenu de la fenêtre lors d'un cliquer déplacer

Ce paramètre autorise ou empêche l'affichage des contenus de fenêtre lors d'un glisser-déplacer d'une fenêtre au travers de l'écran.

Par défaut, l'affichage du contenu de la fenêtre est autorisé.

S'il a la valeur **Autorisé**, la fenêtre entière semble se déplacer lorsque vous la faites glisser. S'il a la valeur **Interdit**, seul le contour de la fenêtre semble se déplacer jusqu'à ce que vous relâchiez le bouton.

## Paramètres de stratégie Contrôle de l'utilisateur final

June 27, 2024

La section **Contrôle de l'utilisateur final** contient des paramètres de stratégie permettant de mesurer le trafic de session.

### Calcul des boucles ICA

Ce paramètre détermine si les calculs de boucle ICA sont exécutés pour les connexions actives.

Par défaut, les calculs des connexions actives sont activés.

Par défaut, chaque initiation de mesure de boucle ICA est retardée. Ce délai dure jusqu'à ce qu'un certain trafic indiquant une interaction utilisateur se produise. Ce retard, dont la longueur peut s'avérer indéfinie, est conçu pour empêcher que la mesure des boucles ICA devienne la seule raison du trafic ICA.

### Intervalle de calcul des boucles ICA

Ce paramètre spécifie la fréquence d'exécution (en secondes) des calculs des boucles ICA.

Par défaut, les boucles ICA sont calculées toutes les 15 secondes.

### Calcul des boucles ICA pour les connexions inactives

Ce paramètre détermine si les calculs de boucle ICA sont exécutés pour les connexions inactives.

Par défaut, les calculs ne sont pas exécutés pour les connexions inactives.

Par défaut, chaque initiation de mesure de boucle ICA est retardée. Ce délai dure jusqu'à ce qu'un certain trafic indiquant une interaction utilisateur se produise. Ce retard, dont la longueur peut s'avérer indéfinie, est conçu pour empêcher que la mesure des boucles ICA devienne la seule raison du trafic ICA.

## Paramètre de stratégie Expérience de bureau améliorée

June 27, 2024

Les sessions du paramètre de stratégie Expérience de bureau améliorée exécutées sur des systèmes d'exploitation serveur afin de ressembler à des bureaux Windows 7 locaux.

Par défaut, ce paramètre est autorisé.

Si un profil utilisateur avec un thème Windows Classic existe sur le bureau virtuel, l'activation de cette stratégie n'offre pas une expérience utilisateur améliorée pour cet utilisateur. Supposons qu'un utilisateur avec un profil utilisateur utilisant un thème Windows 7 ouvre une session sur un bureau virtuel exécutant Windows Server 2012. De plus, cette stratégie n'est pas configurée ou est désactivée. Dans ce cas, cet utilisateur voit un message d'erreur indiquant que le thème n'a pas été appliqué.

Dans les deux cas, la réinitialisation du profil utilisateur résout le problème.

Si vous désactivez la stratégie sur un bureau virtuel avec des sessions utilisateur actives, l'interface de ces sessions devient incohérente sur les bureaux Windows 7 et Windows Classic. Pour éviter ce problème, assurez-vous de redémarrer le bureau virtuel après la modification de ce paramètre de stratégie. Supprimez ensuite tous les profils itinérants sur le bureau virtuel. Citrix recommande également de supprimer tous les profils d'utilisateur sur le bureau virtuel pour éviter des incohérences entre les profils.

Supposons que vous utilisez des profils utilisateur itinérants dans votre environnement. Dans ce cas, assurez-vous que la fonctionnalité Expérience de bureau améliorée est activée ou désactivée pour tous les bureaux virtuels qui partagent un profil.

Citrix ne recommande pas de partager les profils itinérants entre bureaux virtuels exécutant des systèmes d'exploitation serveur et des systèmes d'exploitation clients. Les profils des systèmes d'exploitation client et serveur diffèrent. Le partage de profils itinérants entre les deux types peut entraîner des incohérences dans les propriétés de profil lorsqu'un utilisateur se déplace de l'un à l'autre.

# Paramètres de stratégie de la redirection de fichier

June 27, 2024

La section **Redirection de fichier** contient les paramètres de stratégie liés au mappage des lecteurs clients et à leur optimisation.

## Connecter automatiquement les lecteurs clients

Ce paramètre autorise ou empêche la connexion automatique des lecteurs clients lorsque les utilisateurs ouvrent une session.

Par défaut, la connexion automatique est autorisée.

Lorsque vous ajoutez ce paramètre à une stratégie, assurez-vous d'activer les paramètres pour les types de lecteurs que vous souhaitez connecter automatiquement. Par exemple, pour permettre la connexion automatique des lecteurs de CD-ROM des utilisateurs, configurez ce paramètre ainsi que le paramètre **Lecteurs optiques clients**.

Les paramètres de stratégie suivants sont associés :

- **Redirection de lecteur client**
- **Lecteurs de disquette clients**
- **Lecteurs optiques clients**
- **Lecteurs fixes clients**
- **Lecteurs réseau clients**
- **Lecteurs amovibles clients**

## Redirection de lecteur client

Ce paramètre active ou désactive la redirection de lecteur depuis et vers les lecteurs de la machine utilisateur.

Par défaut, la redirection de fichiers est activée.

> **Remarque :**
>
> Les paramètres de stratégie de la redirection de lecteur client ne s'appliquent pas aux lecteurs mappés à des sessions à l'aide de la redirection USB générique.

Lorsqu'il est activé, les utilisateurs peuvent enregistrer des fichiers dans tous leurs lecteurs clients. Lorsqu'il est désactivé, toute redirection de fichiers est empêchée. Cette configuration est applicable

quel que soit l'état des paramètres de redirection de fichiers individuels. Les paramètres de redirection de fichiers individuels incluent les lecteurs de disquettes clients et les lecteurs réseau clients.

Les paramètres de stratégie suivants sont associés :

- **Lecteurs de disquette clients**
- **Lecteurs optiques clients**
- **Lecteurs fixes clients**
- **Lecteurs réseau clients**
- **Lecteurs amovibles clients**

### Lecteurs fixes clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs de disque fixes de la machine utilisateur.

Par défaut, l'accès aux lecteurs fixes clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre **Redirection de lecteur client** est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs fixes clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement, quel que soit l'état du paramètre **Lecteurs de disque fixe clients**.

Configurez le paramètre **Connecter automatiquement les lecteurs clients** pour être certain que les lecteurs de disque fixe sont automatiquement connectés lorsque les utilisateurs ouvrent une session.

### Lecteurs de disquette clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs de disquette de la machine utilisateur.

Par défaut, l'accès aux lecteurs de disquette clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre **Redirection de lecteur client** est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs de disquette clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement, quel que soit l'état du paramètre **Lecteurs de disquette clients**.

Pour garantir la connexion automatique des lecteurs de disquette lors de l'ouverture de session des utilisateurs, configurez le paramètre **Connecter automatiquement les lecteurs clients**.

### Lecteurs réseau clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs réseau (distants) par l'intermédiaire de la machine utilisateur.

Par défaut, l'accès aux lecteurs réseau clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre **Redirection de lecteur client** est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs réseau clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement. Cette configuration est applicable quel que soit l'état du paramètre **Lecteurs réseau clients**.

Pour garantir la connexion automatique des lecteurs réseau lors de l'ouverture de session des utilisateurs, configurez le paramètre **Connecter automatiquement les lecteurs clients**.

### Lecteurs optiques clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les éléments suivants :

- CD-ROM sur la machine utilisateur
- DVD-ROM sur la machine utilisateur
- Lecteurs BD-ROM sur la machine utilisateur

Par défaut, l'accès aux lecteurs optiques clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre **Redirection de lecteur client** est présent et défini sur **Autorisé**. Si ces paramètres sont désactivés, les lecteurs optiques clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement. Cette configuration est applicable quel que soit l'état du paramètre **Lecteurs optiques clients**.

Pour garantir la connexion automatique des lecteurs optiques lors de l'ouverture de session des utilisateurs, configurez le paramètre **Connecter automatiquement les lecteurs clients**.

### Lecteurs amovibles clients

Ce paramètre autorise ou empêche les utilisateurs d'accéder à des fichiers ou d'en enregistrer sur les lecteurs USB de la machine utilisateur.

Par défaut, l'accès aux lecteurs amovibles clients est autorisé.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre **Redirection de lecteur client** est présent et défini sur Autorisé. Si ces paramètres sont désactivés, les lecteurs amovibles clients ne sont pas mappés et les utilisateurs ne peuvent pas y accéder manuellement. Cette configuration est applicable quel que soit l'état du paramètre **Lecteurs amovibles clients**.

Configurez le paramètre **Connecter automatiquement les lecteurs clients** pour garantir la connexion automatique des lecteurs amovibles lors de l'ouverture de session des utilisateurs.

### Redirection hôte vers client

Ce paramètre active ou désactive les associations de type de fichier pour les URL et le contenu de certains supports devant être ouverts sur la machine utilisateur. Lorsqu'elles sont désactivées, le contenu s'ouvre sur le serveur.

Par défaut, l'association de type de fichier est désactivée.

Ces types d'URL sont ouverts localement lorsque vous activez ce paramètre :

- HTTP
- HTTPS
- Real Player et QuickTime (RTSP) ;
- Real Player et QuickTime (RTSPU) ;
- anciennes versions de Real Player (PNM) ;
- Microsoft Media Server (MMS).

### Préserver les lettres de lecteurs clients

Ce paramètre active ou désactive le mappage des lecteurs client sur la même lettre de lecteur dans la session.

Par défaut, les lettres de lecteur client ne sont pas conservées.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre **Redirection de lecteur client** est présent et défini sur Autorisé.

### Accès en lecture unique sur le lecteur client

Ce paramètre autorise ou empêche les utilisateurs et les applications d'effectuer les actions suivantes :

- Création de fichiers sur des lecteurs clients mappés
- Modification de fichiers sur des lecteurs clients mappés
- Modification de dossiers sur des lecteurs clients mappés

Par défaut, les fichiers et les dossiers sur les lecteurs clients mappés peuvent être modifiés.

Si cette option est définie sur Activée, les fichiers et dossiers sont accessibles avec des permissions en lecture seule.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre **Redirection de lecteur client** est présent et défini sur Autorisé.

### Redirection de dossiers spéciaux

Ce paramètre autorise ou empêche les utilisateurs de l'application Citrix Workspace et de l'Interface Web de voir leurs dossiers spéciaux Documents et Bureau locaux à partir d'une session.

Par défaut, la redirection vers les dossiers spéciaux est autorisée.

Ce paramètre empêche les objets filtrés via une stratégie d'être redirigés vers les dossiers spéciaux, quels que soient les paramètres existant ailleurs. Lorsque ce paramètre est interdit, tous les paramètres connexes spécifiés pour StoreFront, l'Interface Web ou l'application Citrix Workspace sont ignorés.

Pour déterminer les utilisateurs autorisés à disposer d'une redirection vers les dossiers spéciaux, sélectionnez **Autorisé** et incluez ce paramètre dans une stratégie filtrée sur les utilisateurs que vous souhaitez voir disposer de cette fonctionnalité. Ce paramètre remplace tous les autres paramètres de redirection vers les dossiers spéciaux.

Les paramètres de stratégie qui empêchent les utilisateurs d'accéder à leurs lecteurs de disque fixe locaux et d'y enregistrer des fichiers empêchent également la redirection vers les dossiers spéciaux de fonctionner. Cette situation se produit parce que la redirection vers les dossiers spéciaux doit interagir avec la machine utilisateur.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre **Lecteurs fixes clients** est présent et défini sur Autorisé.

### Stratégies de transfert de fichiers

Par défaut, le transfert de fichiers est activé. Utilisez Web Studio pour modifier ces stratégies. Elles se trouvent sous **Paramètres utilisateur > ICA\Redirection de dossiers**. Tenez compte de ce qui suit lors de l'utilisation des stratégies de transfert de fichiers :

- **Transfert de fichiers pour l'application Citrix Workspace pour Chrome OS/HTML5** : autorise ou empêche les utilisateurs de transférer des fichiers entre une session Citrix Virtual Apps and Desktops et leurs appareils.
- **Charger un fichier pour l'application Citrix Workspace pour Chrome OS/HTML5** : autorise ou empêche les utilisateurs de charger des fichiers depuis leur appareil sur une session Citrix Virtual Apps and Desktops.
- **Télécharger le fichier pour l'application Citrix Workspace pour Chrome OS/HTML5** : autorise ou empêche les utilisateurs de télécharger des fichiers depuis une session Citrix Virtual Apps and Desktops vers leur appareil.

> **Remarque :**
>
> Les stratégies de transfert de fichiers s'appliquent uniquement à l'application Citrix Workspace pour HTML5 et à l'application Citrix Workspace pour Chrome OS.

### Utiliser les écritures asynchrones

Ce paramètre active ou désactive les écritures asynchrones sur disque.

Par défaut, les écritures asynchrones sont désactivées.

Les écritures asynchrones sur disque peuvent accélérer la vitesse de transfert et d'écriture de fichiers sur les disques clients via des réseaux étendus, généralement caractérisés par une bande passante relativement élevée et une forte latence. Toutefois, en présence d'une erreur de connexion ou de disque, il est possible que le ou les fichiers clients en cours d'écriture se retrouvent dans un état indéfini. Si cet état indéfini se produit, une fenêtre contextuelle indique à l'utilisateur les fichiers affectés. L'utilisateur peut alors prendre une mesure corrective, par exemple en redémarrant un transfert de fichiers interrompu lors de la reconnexion ou une fois l'erreur de disque corrigée.

Citrix recommande d'activer les écritures asynchrones sur disque uniquement pour les utilisateurs nécessitant une connectivité à distance avec accès rapide aux fichiers. Et qui peuvent facilement récupérer des fichiers ou des données perdus en cas de panne de connexion ou de disque.

Lorsque que vous ajoutez ce paramètre à une stratégie, vérifiez que le paramètre **Redirection de lecteur client** est présent et défini sur Autorisé. Si ce paramètre est désactivé, aucune écriture asynchrone n'aura lieu.

## Paramètres de stratégie Graphiques

June 27, 2024

La section **Graphiques** contient des paramètres de stratégie permettant de contrôler le traitement des images dans les sessions utilisateur.

### Autoriser la compression visuelle sans perte

Ce paramètre permet d'utiliser une compression visuellement sans perte au lieu d'une compression vraie sans perte pour l'affichage des graphiques. La compression visuellement sans perte améliore les performances par rapport à la compression vraie sans perte, mais engendre une perte mineure qui ne peut être remarquée à l'œil nu. Ce paramètre change la manière dont les valeurs du paramètre Qualité visuelle sont utilisées.

Par défaut, ce paramètre est désactivé.

### Indicateur d'état des graphiques

Ce paramètre configure l'indicateur d'état des graphiques à exécuter dans la session utilisateur. Cet outil permet à l'utilisateur de voir des informations sur le mode graphique actif. Ces informations comprennent des détails sur le codec vidéo, le codage matériel, la qualité d'image et les moniteurs utilisés pour la session. Avec l'indicateur d'état des graphiques, l'utilisateur peut également activer ou désactiver le mode Pixel parfait.

Les versions Citrix Virtual Apps and Desktops 2103 et ultérieures incluent un curseur de qualité d'image pour aider l'utilisateur à trouver le bon équilibre entre qualité d'image et interactivité.

Les versions Citrix Virtual Apps and Desktops 2109 et ultérieures incluent des fonctionnalités permettant de configurer une disposition d'affichage virtuel via une interface utilisateur lancée à l'aide de l'indicateur d'état des graphiques.

L'indicateur d'état des graphiques remplace l'outil Indicateur sans perte des versions précédentes. Cette stratégie active l'indicateur sans perte pour Citrix Virtual Apps and Desktops versions 7.16 à 1809.

### Partage d'écran

Ce paramètre permet aux utilisateurs de partager leurs sessions, y compris le contenu de l'écran, les claviers et les souris, avec d'autres utilisateurs.

Par défaut, ce paramètre est désactivé.

Le VDA tente d'utiliser les ports de la plage de ports TCP pour échanger des données, en commençant par le port le plus bas et en utilisant un numéro de port croissant à chaque connexion ultérieure. Le port gère le trafic entrant et sortant.

Par défaut, la plage de ports TCP est définie sur 52525-52625.

Le port utilisé pour le partage d'écran doit être ajouté à la liste des exceptions du pare-feu. Cette option s'affiche sous la forme d'une case à cocher lors de l'installation du VDA. Par défaut, cette option n'est pas cochée.

### Limite de mémoire d'affichage

Ce paramètre spécifie la taille maximale de la mémoire tampon vidéo (en kilo-octets) pour la session.

Par défaut, la limite de mémoire d'affichage est de 65,536 kilo-octets.

Spécifie la taille maximale de la mémoire tampon vidéo (en kilo-octets) pour la session. Spécifiez une taille en kilo-octets comprise entre 128 et 4 194 303. La valeur maximale de 4 194 303 ne limite pas la mémoire d'affichage. Par défaut, la mémoire d'affichage est de 65,536 kilo-octets. Les connexions utilisant un nombre de couleurs et une résolution élevés nécessitent plus de mémoire. En mode graphique d'ancienne génération, si la limite de mémoire est atteinte, l'affichage se dégrade en fonction du paramètre « Préférence de dégradation du mode d'affichage ».

Pour les connexions nécessitant un nombre de couleurs et une résolution élevés, augmentez la limite. Calculez la mémoire maximale requise à l'aide de cette équation :

Quantité de mémoire en octets = (nombre-de-couleur-en-bits-par-pixel)/8) x (résolution-verticale-en-pixels) x (résolution-horizontale-en-pixels).

Par exemple, imaginez un scénario avec un nombre de couleurs de 32, une résolution verticale de 600 et une résolution horizontale de 800. Dans ce cas, la mémoire maximale requise est (32/8) x (600) x (800) = 1920 000 octets, ce qui limite la mémoire d'affichage à 1 920 Ko.

Des nombres de couleurs autres que 32 bits sont uniquement disponibles si la stratégie de mode graphique d'ancienne génération est activée.

HDX alloue uniquement la quantité de mémoire d'affichage nécessaire pour chaque session. Donc, si seuls certains utilisateurs ont besoin de plus que la valeur par défaut, il n'existe aucun impact négatif sur la capacité à monter en charge par l'augmentation de la limite de mémoire d'affichage.

### Préférence de dégradation du mode d'affichage

> **Remarque :**
>
> Pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre spécifie que le nombre de couleurs ou la résolution se dégrade en premier lorsque la limite de mémoire d'affichage de la session est atteinte.

Par défaut, le nombre de couleurs se dégrade en premier.

Lorsque la limite de mémoire de la session est atteinte, vous pouvez réduire la qualité des images affichées. Vous pouvez réduire cette qualité en indiquant si le nombre de couleurs ou la résolution se dégrade en premier. Lorsque le nombre de couleurs se dégrade en premier, les images affichées utilisent moins de couleurs. Lorsque la résolution se dégrade en premier, les images affichées utilisent moins de pixels par pouce.

Pour avertir les utilisateurs lorsque le nombre de couleurs ou la résolution se dégrade, configurez le paramètre Notifier l'utilisateur lorsque le mode d'affichage se dégrade.

### Aperçu de fenêtres dynamiques

Ce paramètre active ou désactive l'affichage des fenêtres transparentes dans :

- Flip-
- Flip 3D
- Aperçu de la barre des tâches
- Windows Peek

| Option d'aperçu de Windows Aero | Description |
|---|---|
| Aperçu de la barre des tâches | Lorsque l'utilisateur place le pointeur de la souris sur l'icône de barre des tâches d'une fenêtre, une image de cette fenêtre s'affiche au-dessus de la barre des tâches. |
| Windows Peek | Lorsque l'utilisateur place le pointeur de la souris sur l'image d'un aperçu de la barre des tâches, une image plein écran de cette fenêtre s'affiche. |
| Flip | Lorsque l'utilisateur appuie sur ALT+TAB, des petites icônes d'aperçu s'affichent pour chaque fenêtre ouverte. |
| Flip 3D | Lorsque l'utilisateur appuie sur la touche Windows+TAB, des grandes images des fenêtres ouvertes s'affichent en cascade sur l'écran. |

Ce paramètre est activé par défaut.

### Mise en cache d'image

> **Remarque :**
>
> Pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre active ou désactive la mise en cache et la récupération de sections d'images dans les sessions. La mise en cache des images dans des sections et la récupération de ces sections permettent d'obtenir les résultats suivants :

- Défilement plus fluide sur la machine utilisateur
- Réduction de la quantité de données transmises via le réseau sur la machine utilisateur
- Réduction du traitement requis sur la machine utilisateur

Le paramètre de mise en cache des images est activé par défaut.

> **Remarque :**
>
> Le paramètre de mise en cache d'image contrôle la façon dont les images sont placées dans le cache et récupérées. Ce paramètre ne contrôle pas la mise en cache des images. Les images sont placées dans le cache si le paramètre Mode graphique d'ancienne génération est activé.

### Mode graphique d'ancienne génération : non pris en charge. Pour la rétrocompatibilité uniquement

> **Important :**
>
> Nous ne prenons pas en charge le mode graphique d'ancienne génération et la Redirection de composition du Bureau (DCR) dans cette version. Cette stratégie est fournie uniquement pour la rétrocompatibilité lors de l'utilisation de XenApp 7.15 LTSR, XenDesktop 7.15 LTSR et les versions de VDA précédentes avec Windows 7 et Windows 2008 R2.

Ce paramètre désactive l'expérience graphique enrichie. Utilisez ce paramètre pour revenir à l'expérience graphique d'ancienne génération, ce qui réduit la consommation de bande passante sur un réseau étendu ou une connexion mobile. Les réductions apportées à la consommation de bande passante introduites dans XenApp et XenDesktop 7.13 rendent ce mode obsolète.

Par défaut, ce paramètre est désactivé et les utilisateurs se voient offrir une expérience graphique enrichie.

Le mode graphique d'ancienne génération est pris en charge sur les systèmes suivants :

- Windows 7
- VDA Windows Server 2008 R2

Le mode graphique d'ancienne génération n'est pas pris en charge sur les systèmes suivants :

- Windows 8.x et 10
- Windows Server 2012, 2012 R2 et 2016

Consultez l'article CTX202687 pour de plus amples informations sur l'optimisation des modes graphiques et sur les stratégies dans XenApp et XenDesktop 7.6 FP3 ou version supérieure.

### Nombre de couleurs maximal autorisé

> **Remarque :**
>
> Pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre spécifie le nombre maximal de couleurs autorisé pour une session.

Par défaut, le nombre maximal de couleurs autorisé est de 32 bits par pixel.

Ce paramètre s'applique uniquement aux pilotes et aux connexions Thinwire. Il ne s'applique pas aux VDA dont le pilote d'affichage principal n'est pas ThinWire. Ces VDA sont des VDA qui utilisent un pilote Windows Display Driver Model (WDDM) comme pilote d'affichage principal. Pour les VDA avec OS mono-session utilisant un pilote WDDM en tant que pilote d'écran principal, tel que Windows 8, ce paramètre n'a aucun effet. Pour les VDA avec OS multi-session Windows utilisant un pilote WDDM, tel que Windows Server 2012 R2, ce paramètre peut empêcher les utilisateurs de se connecter au VDA.

Plus le nombre de couleurs est élevé, plus la mémoire requise est importante. Pour dégrader le nombre de couleurs lorsque la limite de mémoire est atteinte, configurez le paramètre **Préférence de dégradation du mode d'affichage**. Lorsque le nombre de couleurs se dégrade, les images affichées utilisent moins de couleurs.

### Notifier l'utilisateur lorsque le mode d'affichage se dégrade

> **Remarque :**
>
> Pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre permet d'afficher une brève explication pour l'utilisateur lorsque le nombre de couleurs ou la résolution se dégrade.

Par défaut, la notification des utilisateurs est désactivée.

### Optimiser pour la charge des graphiques 3D

Ce paramètre configure les paramètres par défaut appropriés qui conviennent le mieux aux charges de travail exigeant d'importantes ressources graphiques. Activez ce paramètre pour les utilisateurs dont la charge de travail utilise des applications exigeant d'importantes ressources graphiques. Appliquez cette stratégie uniquement dans les cas où un processeur graphique est disponible pour la session. Tous les autres paramètres qui remplacent explicitement les paramètres par défaut définis par cette stratégie sont prioritaires.

Par défaut, l'optimisation pour la charge des graphiques 3D est désactivée.

### Mise en file d'attente et suppression

> **Remarque :**
>
> Pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre permet d'ignorer toute image en file d'attente qui est remplacée par une autre image.

Par défaut, la mise en file d'attente et le ballotage sont activés.

Ce paramètre améliore le temps de réponse lorsque des graphiques sont envoyés à la machine utilisateur. La configuration de ce paramètre peut provoquer une animation hachée due à des trames ignorées.

### Utiliser codec vidéo pour la compression

Permet d'utiliser un codec vidéo pour compresser les graphiques lorsque le décodage vidéo est disponible sur le poste client. Lorsque **Pour l'écran entier** est sélectionné, le codec vidéo est appliqué en tant que codec par défaut pour tout. Lorsque **Pour les zones changeant constamment** est sélectionné, le codec vidéo est utilisé pour les zones changeant constamment sur l'écran, les autres données continuent à utiliser la compression d'image fixe et la mise en cache des bitmaps Si le décodage vidéo n'est pas disponible sur le point de terminaison ou que vous avez spécifié **Ne pas utiliser de codec vidéo**, une combinaison de compression d'image fixe et de mise en cache des bitmaps est utilisée. Lorsque l'option **Utiliser au choix** est sélectionnée, le système se base sur plusieurs facteurs pour effectuer un choix. Les résultats peuvent varier en fonction des versions car la méthode de sélection est améliorée.

Sélectionnez l'option **Utiliser au choix** pour permettre au système de choisir les paramètres qui conviennent le mieux au scénario actuel.

Sélectionnez l'option **Pour l'écran entier** pour optimiser l'expérience utilisateur et la bande passante, particulièrement dans les cas dans lesquels le rendu vidéo sur le serveur et les graphiques 3D sont fortement sollicités.

Sélectionnez l'option **Pour les zones changeant constamment** pour optimiser les performances vidéo, particulièrement en cas de faible bande passante, tout en conservant la capacité à monter en charge pour le contenu statique et changeant lentement. Ce paramètre est pris en charge dans les déploiements comportant plusieurs moniteurs.

Sélectionnez l'option **Ne pas utiliser de codec vidéo** pour optimiser la charge d'UC du serveur et pour les scénarios avec peu de rendu vidéo sur le serveur ou ne faisant pas appel à beaucoup d'applications exigeant d'importantes ressources graphiques.

La valeur par défaut est **Utiliser au choix**.

### Utiliser le codage matériel pour la vidéo

Ce paramètre permet d'utiliser du matériel graphique, si disponible, pour compresser les éléments d'écran avec un codec vidéo. Si ce matériel n'est pas disponible, le VDA utilise le codage basé sur l'UC avec le codec vidéo logiciel.

L'option par défaut pour ce paramètre de stratégie est **Activé**.

Les moniteurs multiples sont pris en charge.

Toute application Citrix Workspace qui prend en charge le décodage vidéo peut être utilisée avec le codage matériel.

#### NVIDIA

Pour les GPU NVIDIA GRID, le codage matériel est pris en charge avec les VDA pour OS multi-session et OS mono-session.

Les GPU NVIDIA doivent prendre en charge le codage matériel NVENC. Voir SDK codec vidéo NVIDIA pour une liste des processeurs graphiques pris en charge.

NVIDIA GRID requiert une version de pilote 3.1 ou supérieure. NVIDIA Quadro requiert une version de pilote 362.56 ou supérieure. Citrix recommande des pilotes NVIDIA version R361.

Le texte sans perte n'est pas compatible avec le codage matériel NVENC. Si vous avez activé le texte sans perte, le texte sans perte a priorité sur le codage matériel NVENC.

L'utilisation sélective du codec de matériel H.264 pour les zones changeant constamment est prise en charge.

La compression visuelle sans perte (YUV 4:4:4) est prise en charge. La compression visuelle sans perte (paramètre de stratégie graphique, Autoriser la compression visuelle sans perte) requiert l'application Citrix Workspace 1808 ou version supérieure ou Citrix Receiver pour Windows version 4.5 ou version supérieure.

#### Intel

Pour les processeurs graphiques Intel Iris Pro, le codage matériel est pris en charge avec les VDA pour OS mono-session et les VDA pour OS multi-session.

Les processeurs graphiques Intel Iris Pro de la famille des processeurs Intel Broadwell et plus récents sont pris en charge. Intel Remote Displays SDK version 1.0 est requis et peut être téléchargé à partir du site Web Intel : SDK affichages distants.

Le texte sans perte est pris en charge uniquement lorsque la stratégie Codec vidéo est définie pour l'intégralité de l'écran et que la stratégie **Optimiser pour la charge des graphiques 3D** est désactivée.

La compression visuelle sans perte (YUV 4:4:4) n'est pas prise en charge.

Le codeur Intel fournit une expérience utilisateur de bonne qualité pour jusqu'à huit sessions de codage (par exemple, un utilisateur utilisant huit moniteurs ou huit utilisateurs utilisant un moniteur). Si plus de huit sessions de codage sont requises, vérifiez le nombre de moniteurs auxquels la machine virtuelle se connecte. Afin de conserver une expérience utilisateur optimale, l'administrateur choisit de configurer ce paramètre de stratégie par utilisateur ou par machine.

#### AMD

Pour AMD, le codage matériel est pris en charge avec les VDA pour OS mono-session.

Les GPU AMD doivent prendre en charge le SDK RapidFire. Par exemple, les GPU AMD Radeon Pro ou FirePro.

Pour que le codage fonctionne, installez les derniers pilotes AMD. Vous pouvez télécharger ces pilotes à partir de https://www.amd.com/en/support.

Le texte sans perte n'est pas compatible avec le codage matériel AMD. Si vous avez activé le texte sans perte, celui-ci a priorité sur le codage matériel AMD.

L'utilisation sélective du codec de matériel H.264 pour les zones changeant constamment est prise en charge.

## Paramètres de stratégie Mise en cache

June 27, 2024

Cette section contient des paramètres de stratégie qui vous permettent de mettre en cache des données d'image sur les machines utilisateur lorsque les connexions clientes sont limitées en bande passante.

### Seuil de cache permanent

**Remarque :** Pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie **Mode graphique d'ancienne génération** est activé.

Ce paramètre met en cache les bitmaps sur le disque dur de la machine utilisateur et permet ainsi la réutilisation d'images volumineuses fréquemment utilisées lors de sessions précédentes.

Par défaut, le seuil est de 3000000 kilobits par seconde.

La valeur de seuil représente le point en dessous duquel la fonctionnalité de cache permanent prend effet. Par exemple, concernant la valeur par défaut, les images bitmaps sont cachées sur le disque dur de la machine utilisateur lorsque la bande passante se trouve en dessous de 3000000 bps.

## Paramètres de stratégie Framehawk

June 27, 2024

> **Important :**
>
> À partir de Citrix Virtual Apps and Desktops 7 1903, Framehawk n'est plus pris en charge. Utilisez Thinwire avec le transport adaptatif activé.

La section **Framehawk** contient des paramètres de stratégie permettant d'activer et de configurer le canal d'affichage Framehawk sur le serveur.

### Canal d'affichage Framehawk

Lorsque cette option est activée, le serveur tente d'utiliser le canal d'affichage Framehawk pour les graphiques et la saisie à distance. Ce canal d'affichage utilise UDP pour offrir une meilleure expérience utilisateur sur les réseaux à perte et à latence élevées. Cependant, il peut également utiliser davantage de ressources serveur et de bande passante que les autres modes graphiques.

Par défaut, le canal d'affichage Framehawk est désactivé.

### Plage de ports du canal d'affichage Framehawk

Ce paramètre spécifie la plage de numéros de ports UDP que le VDA peut utiliser pour échanger des données de canal d'affichage Framehawk avec la machine utilisateur. Les numéros de port se présentent sous la forme *numéro de port le plus bas ou numéro de port le plus élevé*. Le VDA tente d'utiliser chaque port, en commençant par le numéro de port le plus bas et en remontant pour chaque tentative. Le port gère le trafic entrant et sortant.

Par défaut, la plage de ports est 3224,3324.

# Paramètres de stratégie Persistance

June 27, 2024

La section **Persistance** contient les paramètres de stratégie pour gérer les messages de persistance ICA.

### Délai d'expiration de persistance ICA

Ce paramètre spécifie le nombre de secondes entre les messages de persistance ICA successifs.

Par défaut, l'intervalle entre les messages de persistance est de 60 secondes.

Spécifiez l'intervalle (entre 1 et 3600 secondes) à utiliser pour envoyer des messages de persistance ICA. Ne configurez pas ce paramètre si votre logiciel de contrôle de réseau est responsable de la fermeture des connexions inactives.

### Messages de persistance ICA

Ce paramètre active ou désactive l'envoi périodique de messages de persistance ICA.

Par défaut, aucun message de persistance n'est envoyé.

L'activation de ce paramètre empêche la déconnexion des connexions interrompues. Si le serveur ne détecte pas d'activité, ce paramètre empêche les services Bureau à distance de déconnecter la session. Le serveur envoie des messages de persistance à quelques secondes d'intervalle pour détecter si la session est active. Si la session n'est plus active, le serveur marque la session en tant que déconnectée.

Cependant, la persistance ICA ne fonctionne pas si vous utilisez la fiabilité de session. Ne configurez la persistance ICA que pour les connexions qui n'utilisent pas la fiabilité de session.

Paramètres de stratégie liés : Connexions de fiabilité de session.

# Paramètres de stratégie Local App Access

June 27, 2024

La section **Local App Access** contient des paramètres de stratégie qui gèrent les applications des utilisateurs installées localement avec les applications hébergées. Ces paramètres de stratégie gèrent l'intégration dans un environnement de bureau hébergé.

### Autoriser Local App Access

Ce paramètre autorise ou empêche l'intégration des applications installées localement avec les applications hébergées. Ces paramètres de stratégie gèrent l'intégration dans un environnement de bureau hébergé.

Lorsqu'un utilisateur démarre une application installée localement, l'application semble être exécutée dans leur bureau virtuel, même si elle est exécutée localement.

Si vous définissez le paramètre de stratégie **Autoriser Local App Access** sur **Activé**, la redirection de contenu du navigateur n'est pas prise en charge et l'état de la batterie de la zone de notification côté client n'apparaît pas dans les sessions de bureau.

Par défaut, **Autoriser Local App Access** est désactivé.

### Liste de blocage de redirection d'adresse URL

Ce paramètre spécifie les sites Web qui sont redirigés vers et démarrés dans le navigateur Web local. Ces sites Web peuvent être les suivants :

- Sites Web nécessitant des informations locales, tels que msn.com ou newsgoogle.com
- Sites Web avec du contenu multimédia enrichi qui s'affiche mieux sur la machine utilisateur.

Par défaut, aucun site n'est spécifié.

### Liste d'autorisation de redirection d'adresse URL

Ce paramètre spécifie les sites Web qui sont restitués dans l'environnement dans lequel elles sont démarrées.

Par défaut, aucun site n'est spécifié.

## Paramètres de stratégie Expérience mobile

June 27, 2024

La section **Experience Mobile** contient des paramètres de stratégie destinés à la gestion de Citrix Mobility Pack.

### Affichage automatique du clavier

Ce paramètre active ou désactive l'affichage automatique du clavier sur les écrans des appareils mobiles.

Par défaut, l'affichage automatique du clavier est désactivé.

### Démarrer un bureau tactile

Ce paramètre est désactivé et n'est pas disponible pour les machines Windows 10 ou Windows Server 2016.

Ce paramètre détermine le comportement global de l'interface de l'application Citrix Workspace. Ce paramètre autorise ou interdit une interface tactile optimisée pour les tablettes.

Par défaut, une interface tactile est utilisée.

Pour n'utiliser que l'interface Windows, définissez cette stratégie sur Interdit.

### Contrôler à distance les zones de liste déroulantes

Ce paramètre détermine les types de zones de liste déroulante que vous pouvez afficher dans les sessions sur les appareils mobiles. Pour afficher la commande de zone combinée d'appareil native, définissez ce paramètre de stratégie sur Autorisé. Lorsque ce paramètre est autorisé, un utilisateur peut modifier un paramètre de session de l'application Citrix Workspace pour iOS afin d'utiliser la zone combinée Windows.

Par défaut, la fonctionnalité **Contrôler la zone combinée** est interdite.

## Paramètres de stratégie multimédia

June 27, 2024

La section **Multimédia** contient les paramètres de stratégie permettant de gérer les données audio et vidéo HTML5 et Windows livrées en streaming dans les sessions utilisateur.

> **Avertissement**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de

> votre registre avant de le modifier.

### Stratégies multimédia

Par défaut, toutes les stratégies multimédia définies sur le Delivery Controller sont stockées dans ces registres :

Stratégies machine :

HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies

Stratégies utilisateur :

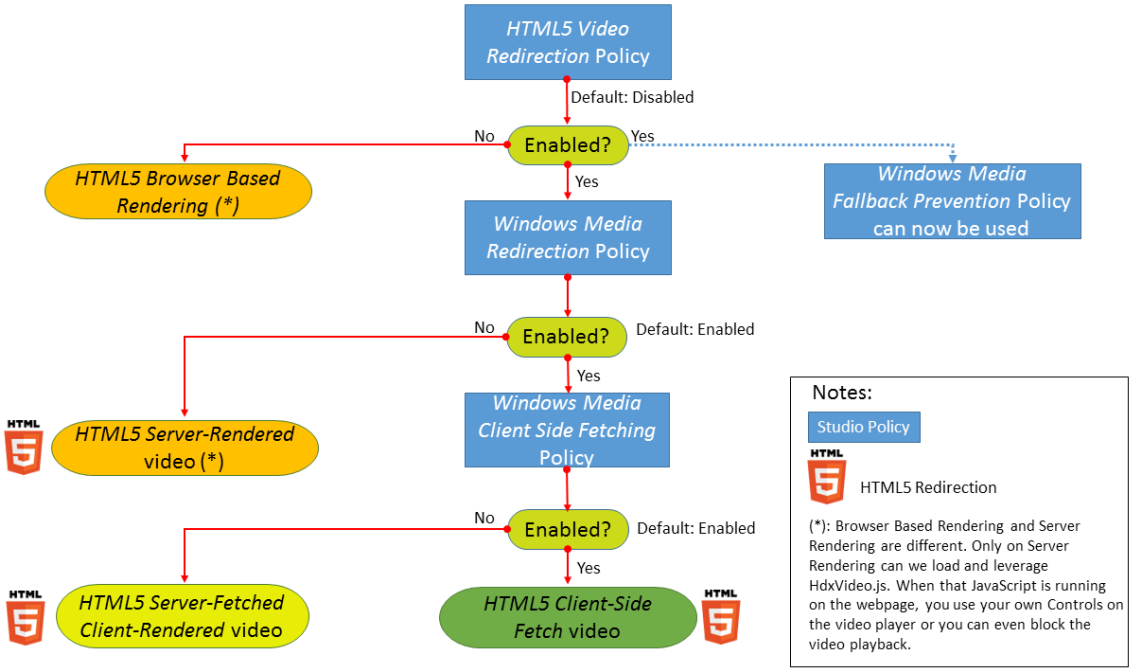
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{User Session ID}\User\MultimediaPolicies

Pour trouver l'ID de session utilisateur actuel, exécutez la commande **qwinsta** sur la ligne de commande Windows.

### Redirection vidéo HTML5

Contrôle et optimise la manière dont les serveurs Citrix Virtual Apps and Desktops mettent à disposition le contenu Web multimédia HTML5 pour les utilisateurs.

Par défaut, ce paramètre est désactivé.




Dans cette version, cette fonctionnalité est disponible pour les pages Web contrôlées uniquement. Elle requiert l'ajout de JavaScript dans les pages Web sur lesquelles le contenu multimédia HTML5 est disponible, par exemple, des vidéos sur un site de formation interne.

Pour configurer la redirection vidéo HTML5 :

1. Copiez le fichier **HdxVideo.js** depuis %Program Files%/Citrix/ICA Service/HTML5 Video Redirection sur l'installation du VDA vers votre page Web interne.
2. Insérez cette ligne dans votre page Web (si votre page Web dispose d'autres scripts, incluez **HdxVideo.js** avant ces scripts) :
   ```
   <script src="HdxVideo.js"type="text/javascript"\></script>
   ```

**Remarque :** si HdxVideo.js ne figure pas dans le même emplacement que votre page Web, utilisez l'attribut **src** pour définir le chemin d'accès complet vers ce dernier.

Imaginez que le code JavaScript n'est pas ajouté à vos pages Web contrôlées et que l'utilisateur lit une vidéo HTML5. Dans ce cas, Citrix Virtual Apps and Desktops utilise par défaut le rendu côté serveur.

La ***redirection Windows Media*** doit être autorisée pour que la redirection vidéo HTML5 fonctionne. Cette stratégie est obligatoire pour la récupération client avec restitution client et nécessaire pour la récupération côté client. La récupération côté client nécessite également que la *récupération de contenu Windows Media côté client* soit autorisée.

Microsoft Edge ne prend pas en charge cette fonctionnalité.

HdxVideo.js remplace les contrôles du lecteur HTML5 du navigateur avec les siens. Pour vérifier que la stratégie de redirection vidéo HTML5 est appliquée sur un site Web donné, comparez les contrôles du lecteur à un scénario où la stratégie **Redirection vidéo HTML5** est interdite :

(Contrôles personnalisés Citrix lorsque la stratégie est autorisée)

(Contrôles de page Web natifs lorsque la stratégie est interdite ou non configurée)


Les commandes de vidéo suivantes sont prises en charge :

- lecture
- suspendre
- recherche
- répétition
- Audio
- plein écran

Vous pouvez afficher une page de test de redirection vidéo HTML5 sur.

#### TLS, redirection vidéo HTML5 et redirection du contenu du navigateur

Vous pouvez utiliser la redirection vidéo HTML5 pour :

- Rediriger des vidéos depuis des sites HTTPS
- Ou
- Rediriger le contenu de navigateur pour rediriger l'ensemble du site

Le code JavaScript injecté sur ces sites Web doit établir une connexion TLS avec le service de redirection vidéo Citrix HDX HTML5 (WebSocketService.exe) en cours d'exécution sur le VDA. Le service de redirection vidéo Citrix HDX HTML5 dans le magasin de certificats sur le VDA génère deux certificats personnalisés pour :

- Réaliser la redirection vidéo
- Préserver l'intégrité TLS de la page Web

HdxVideo.js utilise Secure WebSockets pour communiquer avec WebSocketService.exe en cours d'exécution sur le VDA. Ce processus s'exécute en tant que compte du système local et effectue le mappage de session utilisateur et d'arrêt SSL.

WebSocketService.exe écoute le port 9001 127.0.0.1.

### Limiter la qualité vidéo

Ce paramètre s'applique uniquement à Windows Media et non à HTML5. Vous devez activer **Optimisation pour la redirection multimédia Windows Media sur un réseau étendu**.

Ce paramètre spécifie le niveau de qualité vidéo maximum autorisé pour une connexion HDX. Une fois configurée, la qualité vidéo maximale est limitée à la valeur spécifiée, en assurant que la qualité de service (QoS) multimédia est conservée dans un environnement.

Ce paramètre n'est pas configuré par défaut.

Pour limiter le niveau de qualité vidéo maximum autorisé, choisissez l'une des options suivantes :

- 1080p/8,5 Mbits/s
- 720p/4 Mbits/s
- 480p/720 Kbits/s
- 380p/400 Kbits/s
- 240p/200 Kbits/s

La lecture simultanée de plusieurs vidéos sur le même serveur utilise une quantité importante de ressources et peut avoir un impact sur l'extensibilité du serveur.

### Redirection de Microsoft Teams

Ce paramètre permet l'optimisation de Microsoft Teams, basée sur la technologie HDX.

Si cette stratégie est activée et que vous utilisez une version prise en charge de l'application Citrix Workspace, cette clé de Registre est définie sur **1** sur le VDA. L'application Microsoft Teams lit la clé à charger en mode VDI.
Veuillez noter qu'il n'est pas nécessaire de définir la clé de Registre manuellement.

HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream

Nom : MSTeamsRedirSupport

Valeur : DWORD (1 - activé, 0 - désactivé)

> **Remarque :**
>
> Supposons que vous utilisez des VDA version 1906.2 ou ultérieure avec des versions plus anciennes du Controller, pour lesquelles la stratégie n'est pas disponible dans Web Studio. La version 7.15 est un exemple d'ancienne version du contrôleur. Dans ce cas, l'optimisation HDX est activée par défaut sur le VDA. Si la version de l'application Workspace est 1907 ou supérieure, Microsoft Teams démarre en mode optimisé. Pour plus d'informations sur les mises en garde lors du mélange de contrôleurs LTSR 7.15 et de VDA CR, consultez l'article du Centre de connaissances CTX205549.
>
> Dans ce cas, pour désactiver la fonctionnalité pour des utilisateurs spécifiques, vous pouvez remplacer le paramètre de registre. Remplacez les paramètres de Registre à l'aide d'une stratégie de groupe pour appliquer un script d'ouverture de session à l'unité d'organisation de l'utilisateur.

Par défaut, la redirection Microsoft Teams est activée.

### Conférences multimédia

Ce paramètre autorise ou empêche l'utilisation de la technologie de redirection de webcam optimisée par les applications de vidéoconférence.

Par défaut, la prise en charge de la visioconférence est activée.

Lors de l'ajout de ce paramètre à une stratégie, vérifiez que le paramètre **Redirection Windows Media** est présent et défini sur **Autorisé** (valeur par défaut).

Lorsque vous utilisez les fonctions de **conférence multimédia**, assurez-vous que les conditions suivantes sont remplies :

- Les pilotes fournis par le constructeur pour la webcam utilisée pour les conférences multimédia sont installés sur le client.

- Connectez la webcam à la machine cliente avant de démarrer une session de visioconférence. Le serveur n'utilise qu'une seule webcam installée à la fois. Si plusieurs webcams sont installées sur la machine cliente, le serveur tente d'utiliser chacune d'elles successivement. Cette tentative se poursuit jusqu'à ce qu'il réussisse à créer une session de visioconférence

Cette stratégie n'est pas nécessaire lors de la redirection de la webcam à l'aide de la redirection USB générique. Dans ce cas, installez les pilotes de webcam sur le VDA.

### Optimisation de la redirection multimédia de Windows Media sur un réseau étendu

Ce paramètre s'applique uniquement à Windows Media et non à HTML5. Avec ce paramètre, vous pouvez :

- Transcoder le contenu multimédia en temps réel
- Diffuser des médias audio et vidéo vers des appareils mobiles via des réseaux dégradés
- Améliorer l'expérience utilisateur en améliorant la façon dont le contenu Windows Media est diffusé sur un réseau étendu

Par défaut, la mise à disposition du contenu Windows Media sur le réseau étendu est optimisée.

Lors de l'ajout de ce paramètre à une stratégie, vérifiez que le paramètre **Redirection Windows Media** est présent et défini sur **Autorisé**.

Lorsque ce paramètre est activé, le transcodage multimédia en temps réel est déployé automatiquement lorsque nécessaire pour activer la livraison en streaming de contenu multimédia. Vous fournissez également une expérience utilisateur fluide, même dans des conditions réseau extrêmes.

### Utiliser GPU pour l'optimisation de la redirection multimédia Windows Media sur un réseau étendu

Ce paramètre s'applique uniquement à Windows Media et active le transcodage multimédia en temps réel qui doit être effectué dans l'unité de traitement graphique (GPU) sur le Virtual Delivery Agent (VDA). Il améliore l'extensibilité du serveur. Le transcodage sur l'unité de traitement graphique (GPU) n'est disponible que si le VDA possède une unité de traitement graphique pour l'accélération matérielle. Sinon, le transcodage retourne à l'UC.

**Remarque :** le transcodage GPU est pris en charge uniquement sur les GPU NVIDIA.

Par défaut, l'utilisation du GPU sur le VDA pour optimiser la mise à disposition de contenu Windows Media sur le réseau étendu est interdite.

Lorsque vous ajoutez ce paramètre à une stratégie, assurez-vous que les paramètres suivants sont présents et définis sur Autorisé :

- **Redirection Windows Media**
- **Paramètres Optimisation de la redirection multimédia de Windows Media sur un réseau étendu**

### Prévention du retour à Windows Media

Ce paramètre s'applique à la redirection du contenu du navigateur, HTML5 et Windows Media. Pour qu'il fonctionne avec HTML5, définissez la stratégie **Redirection vidéo HTML5** sur **Autorisé**.

Les administrateurs peuvent utiliser le paramètre de **prévention du retour à Windows Media** pour spécifier la méthode qui est utilisée pour livrer en streaming les contenus aux utilisateurs.

Ce paramètre n'est pas configuré par défaut. Lorsque le paramètre est défini sur Non configuré, le comportement est le même que **Lire tout le contenu**.

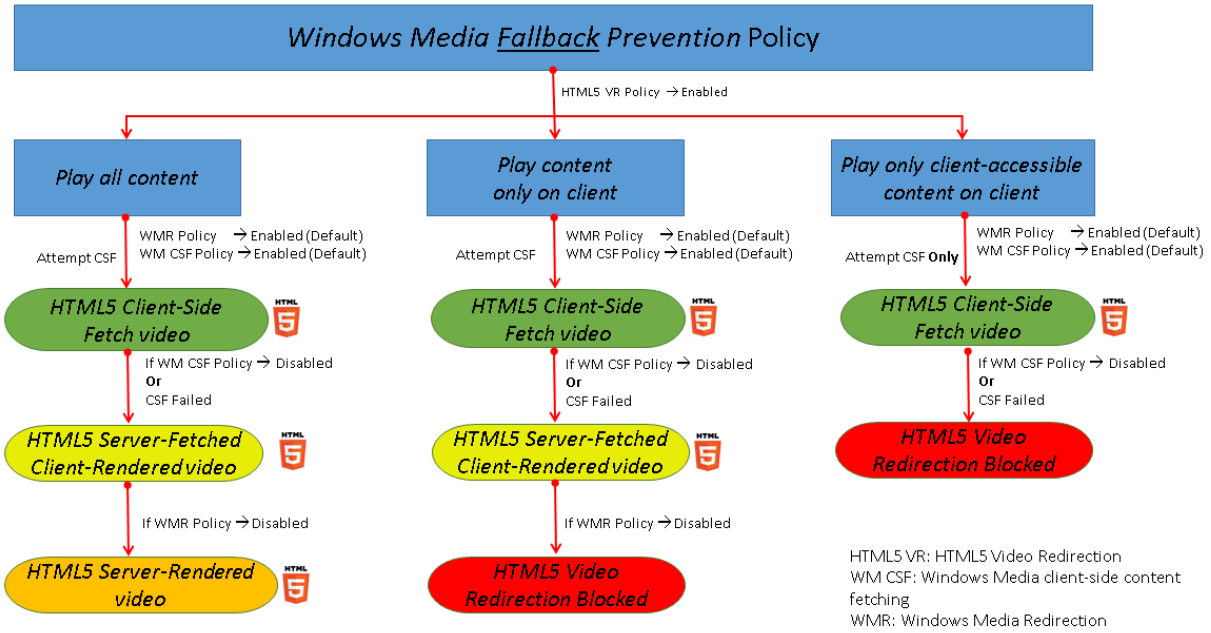
Pour contrôler ce paramètre, choisissez l'une des options suivantes :

- **Lire tout le contenu**. Tentative de récupération de contenu côté client, puis Redirection Windows Media. En cas d'échec, lit le contenu sur le serveur.
- **Lire tout le contenu uniquement sur le client**. Tentative de récupération côté client, puis Redirection Windows Media. En cas d'échec, le contenu n'est pas lu.
- **Lire uniquement le contenu accessible par le client sur le client**. Tentative de récupération côté client uniquement. En cas d'échec, le contenu n'est pas lu.

Lorsque le contenu ne fonctionne pas, le message d'erreur suivant s'affiche (pendant 5 secondes) dans la fenêtre du lecteur :

```
"Company has blocked video because of lack of resources"
```




La durée de ce message d'erreur peut être personnalisée avec la clé de registre suivante sur le VDA. Si l'entrée de registre n'existe pas, la durée par défaut est de 5 secondes.

Le chemin d'accès au Registre varie en fonction de l'architecture du VDA :

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

Ou

\HKLM\SOFTWARE\Citrix\HdxMediastream

Clé de registre :

Nom : VideoLoadManagementErrDuration

Type : DWORD

Plage : 1 - jusqu'à la limite DWORD (par défaut = 5)

Unité : secondes

### Récupération de contenu Windows Media côté client

Ce paramètre s'applique à HTML5 et à Windows Media. Le paramètre permet aux machines utilisateur de livrer en streaming des fichiers multimédia directement à partir du fournisseur source sur Internet ou Intranet, plutôt qu'au travers du serveur hôte XenApp ou XenDesktop.

Par défaut, ce paramètre est **autorisé**. L'autorisation de ce paramètre améliore l'utilisation du réseau et l'évolutivité du serveur. Cette amélioration est obtenue en déplaçant tout traitement sur le média depuis le serveur hôte vers la machine utilisateur. Elle supprime également le besoin d'installer

une infrastructure multimédia avancée tels que Microsoft DirectShow ou Media Foundation sur la machine utilisateur. La machine utilisateur nécessite la possibilité de lire un fichier à partir d'une adresse URL.

Lors de l'ajout de ce paramètre à une stratégie, vérifiez que le paramètre **Redirection Windows Media** est présent et défini sur **Autorisé**. Si **Redirection Windows Media** est désactivée, le streaming des fichiers multimédias vers la machine utilisateur directement à partir du fournisseur source est également désactivé.

### Redirection Windows Media

Ce paramètre s'applique à HTML5 et Windows Media et permet de contrôler et d'optimiser la façon dont les serveurs livrent en streaming des données audio et vidéo auprès des utilisateurs.

Par défaut, ce paramètre est **autorisé**. Pour HTML5, ce paramètre ne prend pas effet si la stratégie **Redirection vidéo HTML5** est définie sur **Interdit**.

L'activation de ce paramètre améliore la qualité de l'audio et de la vidéo restitués depuis le serveur à un niveau comparable à celui obtenu avec de l'audio et de la vidéo exécutés localement sur une machine utilisateur. le serveur livre en streaming du contenu multimédia vers le client au format compressé d'origine et permet à la machine utilisateur de décompresser et de restituer le contenu multimédia.

La redirection Windows Media optimise les fichiers multimédia encodés à l'aide de codecs conformes aux normes DirectShow, DirectX Media Objects (DMO) et Media Foundation standard de Microsoft. Pour lire un fichier multimédia donné, la machine utilisateur doit disposer d'un codec compatible avec le format d'encodage du fichier multimédia.

Par défaut, l'audio est désactivé sur l'application Citrix Workspace. Pour permettre aux utilisateurs d'exécuter des applications multimédia dans les sessions ICA, activez l'audio ou accordez aux utilisateurs l'autorisation de l'activer dans leur interface application Citrix Workspace.

Sélectionnez uniquement **Interdit** si la qualité obtenue avec la redirection Windows Media semble inférieure à celle obtenue à l'aide de la compression ICA de base et des réglages audio standard. Cette situation est rare mais possible dans le cas de conditions où la bande passante est faible, par exemple, si le contenu multimédia dispose d'une faible fréquence de trames clés.

### Taille de tampon de redirection Windows Media

Ce paramètre est hérité et ne s'applique pas à HTML5.

Ce paramètre spécifie une taille de tampon de 1 à 10 secondes pour l'accélération multimédia.

Par défaut, la taille du tampon est de 5 secondes.

### Utilisation de la taille de tampon de redirection Windows Media

Ce paramètre est hérité et ne s'applique pas à HTML5.

Ce paramètre active ou désactive l'utilisation de la taille de tampon définie par le paramètre **Taille de tampon de redirection Windows Media**.

Par défaut, la taille du tampon spécifiée n'est pas utilisée.

Si ce paramètre est désactivé ou si le paramètre **Taille de tampon de redirection Windows Media** n'est pas configuré, le serveur utilise la valeur de taille de tampon par défaut (5 secondes).

## Paramètres de stratégie Connexions Multi-Stream

June 27, 2024

La section **Connexions Multi-Stream** contient des paramètres de stratégie destinés à gérer la hiérarchisation de la qualité de service pour les multiples connexions ICA dans une session.

> **Remarque :**
>
> La découverte MTU n'est pas prise en charge si la stratégie Connexions Multi-Stream est activée.

### Audio sur UDP

Ce paramètre autorise ou empêche l'audio via UDP sur le serveur.

Par défaut, l'audio sur UDP est autorisé sur le serveur.

Lorsqu'il est activé, ce paramètre s'ouvre un port UDP sur le serveur pour prendre en charge toutes les connexions configurées pour utiliser le transport en temps réel Audio sur UDP.

### Plage de port UDP audio

Ce paramètre spécifie la plage de numéros de ports (numéro de port le plus bas, numéro de port le plus élevé) utilisés par Virtual Delivery Agent(VDA). Cette spécification permet d'échanger des données de paquets audio avec la machine utilisateur. Le VDA tente d'utiliser chaque paire de ports UDP pour échanger des données avec la machine utilisateur, en commençant par le plus bas et en incrémentant de deux pour chaque tentative ultérieure. Chaque port gère le trafic entrant et sortant.

Par défaut, cette plage est réglée sur 16500,16509.

### Stratégie Multi-Port

Ce paramètre spécifie les ports TCP à utiliser pour le trafic ICA et établit la priorité réseau pour chaque port.

Par défaut, le port principal (2598) a une priorité élevée.

Lorsque vous configurez des ports, vous pouvez leur attribuer les priorités suivantes :

- **Très élevée :** réservée aux activités en temps réel, telles que les conférences Web (avec web-cam).
- **Élevée :** réservée aux éléments interactifs, tels que l'écran, le clavier et la souris.
- **Moyenne :** réservée aux processus de masse, tels que le mappage des lecteurs clients.
- **Faible :** réservée aux activités d'arrière-plan, telles que l'impression.

Chaque port doit disposer d'une priorité unique. À titre d'exemple, vous ne pouvez pas attribuer une priorité Très élevé au port 1 CGP et au port 3 CGP.

Pour n'attribuer aucune priorité à un port, définissez le numéro de port sur 0. Vous ne pouvez ni supprimer le port principal, ni modifier son niveau de priorité.

Redémarrez le serveur après avoir configuré ce paramètre. Ce paramètre ne s'applique que lorsque le paramètre de stratégie **Paramètre Ordinateur Multi-Stream** est activé.

### Paramètre Ordinateur Multi-Stream

Ce paramètre active ou désactive la fonctionnalité Multi-Stream sur le serveur.

Par défaut, Multi-Stream est désactivée. Configurez le paramètre de stratégie d'ordinateur Multi-Stream si vous utilisez Citrix SD-WAN ou des routeurs tiers pour obtenir la qualité de service souhaitée.

Si Multi-Stream est activé, la découverte MTU, une fonctionnalité de transport adaptatif, n'est pas prise en charge.

Une fois ce paramètre configuré, redémarrez le serveur pour que les modifications prennent effet.

> **Important :**
>
> L'utilisation de ce paramètre de stratégie en conjonction avec les paramètres de stratégie de limite de bande passante (Limite de bande passante de session générale) peut produire des résultats inattendus. Lors de l'inclusion de ce paramètre dans une stratégie, assurez-vous que les paramètres de limite de bande passante ne sont pas inclus.

### Paramètre Utilisateur Multi-Stream

Ce paramètre active ou désactive la fonctionnalité Multi-Stream sur la machine utilisateur.

Par défaut, Multi-Stream est désactivé pour tous les utilisateurs. Configurez le paramètre utilisateur Multi-Stream si vous utilisez Citrix SD-WAN ou des routeurs tiers pour atteindre la qualité de service souhaitée.

Ce paramètre ne s'applique que sur les hôtes sur lesquels le paramètre de stratégie **Paramètre Ordinateur Multi-Stream** est activé.

> **Important :**
>
> L'utilisation de ce paramètre de stratégie en conjonction avec les paramètres de stratégie de limite de bande passante (Limite de bande passante de session générale) peut produire des résultats inattendus. Lors de l'inclusion de ce paramètre dans une stratégie, assurez-vous que les paramètres de limite de bande passante ne sont pas inclus.

### Paramètres d'attribution de canaux virtuels Multi-Stream

Ce paramètre spécifie le flux ICA auquel les canaux virtuels sont affectés lors de l'utilisation de Multi-Stream.

Si vous ne configurez pas ces paramètres, les canaux virtuels sont conservés dans leur flux par défaut. Pour affecter un canal virtuel à un flux ICA, sélectionnez le numéro de flux souhaité (0, 1, 2, 3) dans la liste **Numéro de flux** en regard du nom du canal virtuel.

Si un canal virtuel personnalisé est utilisé dans l'environnement, cliquez sur **Ajouter**, spécifiez le nom du canal virtuel dans la zone de texte sous **Canaux virtuels** et sélectionnez le numéro de flux souhaité dans la liste **Numéro de flux** en regard de celui-ci. Le nom que vous spécifiez doit être le nom réel du canal virtuel et non un nom convivial. Par exemple, CTXSBR au lieu de Citrix Browser Acceleration.

Ces paramètres ne prennent effet que lorsque vous avez activé le paramètre Ordinateur Multi-Stream.

Par défaut, les canaux virtuels et leurs attributions de flux sont :

- AppFlow : 2
- Audio : 0
- Redirection du contenu du navigateur : 2
- Mappage de port COM client : 3
- Mappage des lecteurs clients : 2
- Mappage d'imprimante client : 3
- Presse-papiers : 2

- CTXDND : 1 (**Remarque :** prend en charge le glisser-déposer de fichiers entre une session Citrix et un point de terminaison local.)
- Plug-in DVC (nom VC statique généré automatiquement à partir du nom convivial du plug-in DVC, ou assigné par l'administrateur) : 2
- Surveillance de l'expérience utilisateur final : 1
- Transfert de fichiers (Receiver HTML5) : 2
- Transfert de données générique : 2
- Contrôle ICA : 1
- Éditeur de méthode d'entrée : 1
- Mappage d'imprimantes clientes d'ancienne génération (COM1) : 1, 3
- Mappage d'imprimantes clientes d'ancienne génération (COM2) : 2, 3
- Mappage d'imprimantes clientes d'ancienne génération (LPT1) : 1, 3
- Mappage d'imprimantes clientes d'ancienne génération (LPT2) : 2, 3
- Gestion des licences : 1
- Redirection de Microsoft Teams/WebRTC : 1
- Receiver mobile : 1
- MultiTouch : 1
- Réacheminement de port : 2
- RAVE (extensions audio and vidéo à distance) : 2
- Transparent (Intégration de fenêtre transparente) : 1
- Capteur et emplacement : 1
- Carte à puce : 1
- Graphiques Thinwire : 1
- Intégration de l'interface utilisateur transparente/état de la connexion : 2
- Redirection TWAIN : 2
- USB : 2
- Police et clavier à latence nulle : 2
- Canal de données à latence nulle : 2

Pour plus d'informations sur les attributions et les priorités des canaux virtuels, consultez l'article CTX131001 du centre de connaissances.

## Paramètres de stratégie de redirection de port

June 27, 2024

La section **Redirection de port** contient les paramètres de stratégie pour le mappage des ports LPT et COM clients.

Pour les versions du Virtual Delivery Agent **antérieures à la version 7.0**, utilisez les paramètres de stratégie suivants pour configurer la redirection de port. Pour les versions VDA de **7.0 à 7.8**, configurez ces paramètres à l'aide du registre ; consultez la section Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre. Pour la version **7.9** du VDA, utilisez les paramètres de stratégie suivants.

### Connecter automatiquement les ports COM du client

Ce paramètre active ou désactive la connexion automatique des ports COM sur les machines utilisateur lorsque les utilisateurs ouvrent une session sur un site.

Par défaut, les ports COM du client ne sont pas automatiquement connectés.

### Connecter automatiquement les ports LPT du client

Ce paramètre active ou désactive la connexion automatique des ports LPT sur les machines utilisateur lorsque les utilisateurs ouvrent une session sur un site.

Par défaut, les ports LPT du client ne sont pas automatiquement connectés.

### Redirection de port COM client

Ce paramètre autorise ou empêche l'accès aux ports COM sur la machine utilisateur.

Par défaut, la redirection des ports COM est interdite.

Les paramètres de stratégie suivants sont associés :

- Limite de bande passante de redirection de port COM
- Pourcentage de limite de bande passante de redirection du port COM

### Redirection de port LPT client

Ce paramètre autorise ou empêche l'accès aux ports LPT sur la machine utilisateur.

Par défaut, la redirection des ports LPT est interdite.

Les ports LPT sont uniquement utilisés par les applications d'ancienne génération qui leur envoient les tâches d'impression. Ces ports ne sont pas utilisés par les applications d'ancienne génération qui envoient les tâches d'impression aux objets d'impression sur la machine utilisateur La plupart des applications peuvent désormais envoyer des tâches d'impression aux objets d'imprimante. Ce paramètre de stratégie est uniquement nécessaire pour les serveurs hébergeant des applications d'ancienne génération qui impriment sur des ports LPT.

Veuillez noter que bien que la redirection des ports COM clients soit bi-directionnelle, la redirection des ports LPT est en sortie uniquement et limitée à \\client\LPT1 et \\client\LPT2 dans une session ICA.

Les paramètres de stratégie suivants sont associés :

- Limite de bande passante pour la redirection du port LPT
- Pourcentage de limite de bande passante de redirection du port LPT

## Paramètres de stratégie Impression

June 27, 2024

La section Impression contient les paramètres de stratégie qui permettent de gérer l'impression cliente.

### Redirection d'imprimante cliente

Ce paramètre contrôle si les imprimantes clientes sont mappées sur un serveur lorsqu'un utilisateur ouvre une session.

Par défaut, le mappage des imprimantes clientes est autorisé. Si ce paramètre est désactivé, l'imprimante PDF pour la session n'est pas créée automatiquement.

Paramètres de stratégie liés : créer automatiquement des imprimantes clientes

### Imprimante par défaut

Ce paramètre spécifie la façon dont l'imprimante par défaut est définie sur la machine utilisateur dans une session.

Par défaut, l'imprimante actuelle de l'utilisateur est utilisée comme imprimante par défaut pour la session.

Pour utiliser le paramètre de profil utilisateur des services Bureau à distance ou Windows courant pour l'imprimante par défaut, sélectionnez Ne pas ajuster l'imprimante par défaut de l'utilisateur. Si vous choisissez cette option, l'imprimante par défaut n'est pas enregistrée dans le profil et elle ne change pas selon les propriétés des autres sessions ou du client. L'imprimante par défaut d'une session est la première imprimante créée automatiquement dans la session, à savoir :

- La première imprimante ajoutée localement au serveur Windows dans **Panneau de configuration > Périphériques** et **Imprimantes**.

- La première imprimante créée automatiquement, si aucune imprimante n'a été ajoutée localement sur le serveur.

Vous pouvez utiliser cette option pour présenter l'imprimante la plus proche aux utilisateurs par le biais des paramètres de profil (fonctionnalité connue sous le nom d'impression de proximité).

### Attributions d'imprimantes

Ce paramètre permet d'offrir une alternative aux paramètres Imprimante par défaut et Imprimantes de session. Utilisez les paramètres Imprimante par défaut et Imprimantes de session pour configurer les comportements d'un site, d'un groupe important ou d'une unité d'organisation. Utilisez le paramètre **Attributions d'imprimantes** pour attribuer un groupe important d'imprimantes à plusieurs utilisateurs.

Ce paramètre spécifie la façon dont l'imprimante par défaut des machines utilisateur répertoriées est établie dans une session.

Par défaut, l'imprimante actuelle de l'utilisateur est utilisée comme imprimante par défaut pour la session.

Ce paramètre spécifie de créer automatiquement les imprimantes réseau dans une session pour chaque machine utilisateur. Par défaut, aucune imprimante n'est spécifiée.

- Lors de la définition de la valeur d'imprimante par défaut :

  Pour utiliser l'imprimante par défaut courante pour la machine utilisateur, sélectionnez Ne pas ajuster.

  Pour utiliser le paramètre de profil utilisateur des services Bureau à distance ou Windows courant pour l'imprimante par défaut, sélectionnez Ne pas régler. Si vous choisissez cette option, l'imprimante par défaut n'est pas enregistrée dans le profil et elle ne change pas selon les propriétés des autres sessions ou du client. L'imprimante par défaut d'une session est la première imprimante créée automatiquement dans la session, à savoir :

  - La première imprimante ajoutée localement au serveur Windows dans **Panneau de configuration > Périphériques** et imprimantes.
  - La première imprimante créée automatiquement, si aucune imprimante n'a été ajoutée localement sur le serveur.

- Lors de la définition de la valeur des imprimantes de session : pour ajouter des imprimantes, entrez le chemin UNC de l'imprimante que vous souhaitez créer automatiquement. Après avoir ajouté l'imprimante, vous pouvez appliquer les paramètres personnalisés pour la session courante lors de chaque ouverture de session.

### Préférence de journalisation des événements de création automatique des imprimantes

Ce paramètre spécifie les événements journalisés pendant le processus de création automatique de l'imprimante. Vous pouvez choisir de ne journaliser ni les erreurs ni les avertissements, uniquement les erreurs, ou les erreurs et les avertissements.

Par défaut, les erreurs et les avertissements sont journalisés.

Un exemple d'avertissement est un événement au cours duquel le pilote natif d'une imprimante n'a pas pu être installé ; c'est le pilote d'impression universelle qui a été installé à la place. Pour utiliser le pilote d'impression universelle dans ce scénario, configurez le paramètre Utilisation du pilote d'impression universelle sur l'option Utiliser l'impression universelle uniquement ou Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible.

### Imprimantes de session

Ce paramètre spécifie de créer automatiquement les imprimantes réseau dans une session. Dans la session ICA/HDX, le service Citrix Print Manager(CpSvc.exe) crée une connexion d'imprimante réseau pendant l'ouverture de session pour chaque imprimante réseau spécifiée dans le paramètre de stratégie **Imprimante de session**. Il supprime les imprimantes pendant la fermeture de la session. Par défaut, aucune imprimante n'est spécifiée.

Dans le paramètre de stratégie **d'imprimante de session**, les imprimantes réseau peuvent résider sur un serveur d'impression Windows ou un serveur d'impression universelle Citrix.

- **Serveur d'impression Windows :** partage une ou plusieurs imprimantes réseau. Il dispose également des pilotes d'imprimante natifs requis pour utiliser les imprimantes réseau.
- **Serveur d'impression universelle :** serveur d'impression Windows sur lequel le logiciel Serveur d'impression universelle Citrix a été installé.

Lors de l'utilisation d'un serveur d'impression Windows, le service Citrix Print Manager crée l'imprimante réseau à l'aide de pilotes d'imprimante natifs. Les pilotes d'imprimante natifs doivent être installés sur le serveur Citrix Virtual Apps.

Lors de l'utilisation d'un serveur d'impression universelle Citrix, le service Citrix Print Manager crée les connexions d'imprimante réseau à l'aide des pilotes d'imprimante natifs, Citrix Universal Printer Driver ou Citrix Universal XPS Printer Driver. Le pilote que vous utilisez est contrôlé par le paramètre de stratégie Utilisation du pilote d'impression universelle.

Tous les pilotes d'imprimante Windows correspondent actuellement à la version v3 ou v4 du pilote. Pour plus d'informations, consultez Prise en charge des architectures de pilotes d'imprimante Microsoft V3 et V4.

Pour ajouter des imprimantes de session et vérifier si elles apparaissent dans les sessions, procédez comme suit :

1. Connectez-vous à Web Studio, sélectionnez **Stratégies** dans le volet de gauche, puis cliquez sur l'onglet **Stratégies**.
2. Activez la stratégie **Imprimantes de session**.
3. Dans la stratégie, ajoutez l'imprimante de session. Pour ajouter des imprimantes, entrez le chemin UNC de l'imprimante que vous souhaitez créer automatiquement. Après avoir ajouté l'imprimante, vous pouvez appliquer les paramètres personnalisés pour la session courante lors de chaque ouverture de session. L'imprimante de session doit s'afficher dans la liste.
4. Une fois la stratégie définie, l'application publiée peut ne pas afficher les imprimantes de session. Ce problème peut se produire car le pilote d'imprimante n'est pas présent sur le serveur Citrix Virtual Apps ou la stratégie a été créée mais non activée.

   > **Remarque :**
   >
   > Si une imprimante de session a besoin d'un pilote d'imprimante natif et que ce dernier n'est pas installé sur le VDA, l'imprimante de session peut ne pas être créée dans la session.

5. Démarrez le bureau publié et ajoutez manuellement l'imprimante de session dans **Périphériques et imprimantes > Panneau de configuration**.
6. En cas d'échec, examinez la communication entre le serveur Citrix Virtual Apps et le serveur d'impression. Envisagez d'exécuter un test avec RDP.

### Attendre la création d'imprimantes

Utilisez la stratégie sur le Delivery Controller pour activer la fonctionnalité sur les Citrix Virtual Desktops.

**Attendre la création d'imprimantes (bureau de serveur) :**

Ce paramètre autorise l'application d'un délai lors de la connexion à une session de sorte à autoriser la création automatique des imprimantes redirigées par le client.

Par défaut, aucun délai de connexion n'intervient.

**Attendez la création d'imprimantes (Citrix Virtual Apps) :**

L'exécution de l'applet de commande PowerShell suivante retarde la connexion aux applications virtuelles exécutées sur des hôtes multisessions afin que les imprimantes redirigées vers le client puissent être créées automatiquement avant l'ouverture de l'application.

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation
$true
```

Par défaut, aucun délai de connexion n'intervient.

## Paramètres de stratégie d'imprimantes clientes

June 27, 2024

La section **Imprimantes clientes** contient les paramètres de stratégie des imprimantes clientes, notamment les paramètres relatifs à la création automatique d'imprimantes clientes, à la rétention des propriétés d'imprimante et à la connexion aux serveurs d'impression.

### Créer automatiquement les imprimantes clientes

Ce paramètre spécifie les imprimantes clientes créées automatiquement. Il remplace les paramètres par défaut de création automatique d'imprimantes clientes.

Par défaut, toutes les imprimantes clientes sont créées automatiquement.

Ce paramètre n'entre en vigueur que si le paramètre **Redirection d'imprimante cliente** est présent et est défini sur **Autorisé**.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- **Créer automatiquement toutes les imprimantes clientes** crée automatiquement toutes les imprimantes clientes sur une machine utilisateur.
- **Ne créer automatiquement que l'imprimante par défaut du client** ne crée automatiquement que l'imprimante sélectionnée comme imprimante par défaut sur la machine utilisateur.
- **Ne créer automatiquement que les imprimantes clientes locales (non réseau)** ne crée automatiquement que les imprimantes directement connectées à la machine utilisateur via un port LPT, COM, USB, TCP/IP ou un autre port local.
- **Ne pas créer les imprimantes clientes automatiquement** désactive la création automatique pour toutes les imprimantes clientes lorsque les utilisateurs ouvrent une session. Avec cette option, les paramètres des services Bureau à distance (RDS) liés à la création automatique d'imprimantes clientes remplacent ce paramètre dans les stratégies de priorité inférieure.

### Créer automatiquement l'imprimante universelle générique

Ce paramètre active ou désactive la création automatique de l'objet d'impression générique de l'imprimante universelle Citrix pour les sessions. Ces sessions incluent uniquement les sessions où une machine utilisateur compatible avec l'impression universelle est en cours d'utilisation.

Par défaut, l'objet Imprimante universelle générique n'est pas créé automatiquement.

Les paramètres de stratégie suivants sont associés :

- Utilisation du pilote d'impression universelle
- Préférence de pilote universel

### Créer automatiquement l'imprimante universelle PDF

Ce paramètre active ou désactive la création automatique de l'imprimante PDF Citrix pour les sessions utilisant :

- Application Citrix Workspace pour Windows (à partir de VDA 7.19)
- Application Citrix Workspace pour HTML5
- Application Citrix Workspace pour Chrome

Par défaut, l'imprimante PDF Citrix n'est pas créée automatiquement.

### Noms des imprimantes clientes

Ce paramètre permet de sélectionner la convention d'appellation pour les imprimantes clientes créées automatiquement.

Par défaut, les noms d'imprimante standard sont utilisés.

Sélectionnez **Noms d'imprimantes standards** pour utiliser des noms d'imprimante tels que « HPLaserJet 4 sur nom du client dans la session 3 »

Sélectionnez **Noms d'imprimantes d'ancienne génération** pour utiliser les anciens noms d'imprimantes clientes et pour préserver la rétrocompatibilité avec les noms d'imprimantes hérités tels que présents dans les versions XenDesktop du produit. Vous pouvez utiliser cette option avec les versions actuelles de Citrix Virtual Apps and Desktops du produit. Un exemple de nom d'imprimante d'ancienne génération est « Client/nomclient#/HPLaserJet 4 ». Cette option est moins sécurisée.

Lorsque vous utilisez l'imprimante PDF Citrix dans une session lancée à partir de l'application Citrix Workspace pour HTML5, définissez le paramètre **Noms des imprimantes clientes** comme paramètre par défaut ou sélectionnez **Noms d'imprimantes standards**. Si vous sélectionnez **Noms d'imprimantes d'ancienne génération**, l'application Citrix Workspace pour HTML5 ne prend pas en charge l'option Imprimante PDF Citrix.

### Diriger les connexions vers les serveurs d'impression

Ce paramètre permet d'activer ou de désactiver les connexions directes à partir du bureau virtuel ou du serveur hébergeant les applications vers un serveur d'impression pour les imprimantes clientes. Ici, les imprimantes clientes sont hébergées sur un partage réseau accessible.

Par défaut, les connexions directes sont activées.

Activez les connexions directes si le serveur d'impression réseau n'est pas sur un réseau étendu à partir du bureau virtuel ou du serveur hébergeant les applications. Les communications directes donnent lieu à des impressions plus rapides lorsque le serveur d'impression réseau et le bureau virtuel ou le serveur hébergeant les applications sont sur le même réseau local.

Vous pouvez désactiver les connexions directes si le réseau se trouve à l'autre extrémité d'un réseau étendu, s'il est soumis à une latence élevée ou s'il dispose d'une bande passante réduite. Les tâches d'impression sont acheminées via la machine utilisateur, puis redirigées vers le serveur d'impression réseau. Les données envoyées à la machine utilisateur sont compressées. Les transmissions de données sur le réseau étendu nécessitent donc moins de bande passante.

Si deux imprimantes réseau ont le même nom, l'imprimante située sur le même réseau que la machine utilisateur est utilisée.

### Mappage et compatibilité du pilote d'imprimante

Ce paramètre spécifie les règles de remplacement de pilotes pour les imprimantes créées automatiquement.

Ce paramètre est configuré pour exclure Microsoft OneNote et XPS Document Writer dans la liste d'imprimantes clientes créées automatiquement.

Lorsque vous définissez ces règles de remplacement, vous pouvez autoriser ou empêcher la création d'imprimantes avec le pilote spécifié. En outre, vous pouvez autoriser les imprimantes créées à utiliser uniquement les pilotes d'imprimantes universels. Le remplacement de pilote annule (ou mappe) le nom de pilote d'imprimante fourni par le client, en le remplaçant par un pilote équivalent sur le serveur. Cela permet à des applications exécutées sur le serveur d'accéder à des imprimantes clientes qui ont les mêmes pilotes que le serveur mais sous des noms de pilote différents.

Vous pouvez effectuer les opérations suivantes :

- Ajouter un mappage d'imprimante
- Modifier un mappage existant
- Remplacer les paramètres personnalisés pour un mappage
- Supprimer un mappage
- Modifier l'ordre des entrées de pilotes dans la liste

Lors de l'ajout d'un mappage, entrez le nom de pilote de l'imprimante cliente, puis sélectionnez le pilote serveur que vous souhaitez remplacer.

### Rétention des propriétés de l'imprimante

Ce paramètre indique si les propriétés d'imprimante sont stockées et précise l'emplacement de stockage.

Par défaut, le système détermine si les propriétés d'imprimante doivent être stockées sur la machine utilisateur, le cas échéant, ou dans le profil utilisateur.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Enregistrées uniquement sur la machine cliente est une option destinée aux machines utilisateur qui possèdent un profil obligatoire ou itinérant qui n'est pas enregistré.
- Conservées uniquement dans le profil d'utilisateur est une option destinée aux machines utilisateur soumises à des contraintes de bande passante (cette option permet de réduire le trafic réseau) et de temps d'ouverture de session ou si des utilisateurs utilisent des plug-ins d'ancienne génération. Cette option stocke les propriétés d'imprimante dans le profil utilisateur sur le serveur et empêche tout échange des propriétés avec la machine cliente. Cette option ne s'applique qu'en cas d'utilisation d'un profil itinérant des services Bureau à distance (RDS).
- Le paramètre Contenu dans le profil uniquement si non enregistré sur le client permet au système de déterminer l'emplacement de stockage des propriétés d'imprimante. Les propriétés d'imprimante sont stockées sur la machine cliente, le cas échéant, ou dans le profil utilisateur. Bien que cette option soit la plus souple, elle peut aussi entraîner un ralentissement à l'ouverture de session et utiliser davantage de bande passante pour les vérifications du système.
- Ne pas conserver les propriétés des imprimantes empêche le stockage des propriétés de l'imprimante.

### Imprimantes clientes conservées et restaurées

Ce paramètre permet d'activer ou de désactiver la rétention et la recréation d'imprimantes sur la machine utilisateur. Par défaut, les imprimantes clientes sont conservées automatiquement et restaurées automatiquement.

Les imprimantes conservées sont des imprimantes créées par l'utilisateur qui sont recréées, ou rappelées, au début de la session suivante. Lorsque Citrix Virtual Apps recrée une imprimante conservée, il tient compte de tous les paramètres de stratégie, à l'exception du paramètre **Créer automatiquement des imprimantes clientes**.

Les imprimantes restaurées sont des imprimantes entièrement personnalisées par un administrateur, dans un état enregistré qui est connecté en permanence au port d'un client.

### Pilote universel d'impression PDF Citrix

Le pilote d'imprimante universelle PDF Citrix permet aux utilisateurs d'imprimer les documents ouverts avec des applications hébergées ou des applications exécutées sur des bureaux virtuels mis à disposition par Citrix Virtual Apps and Desktops. Lorsqu'un utilisateur sélectionne l'option **Imprimante PDF Citrix**, le pilote convertit le fichier au format PDF et transfère le PDF sur l'appareil local. Le PDF est ouvert à des fins d'affichage et d'impression à partir d'une imprimante connectée localement. PDF est l'un des formats pris en charge par l'impression universelle Citrix (en plus de EMF et XPS).
L'imprimante PDF peut être activée, configurée et définie comme imprimante par défaut à l'aide de la stratégie Citrix. L'option **Imprimante PDF Citrix** est disponible pour les utilisateurs de l'application Citrix Workspace pour Windows, Chrome et HTML5.

> **Remarque :**
>
> Une visionneuse PDF est requise pour les points de terminaison Windows. Le client doit avoir une application avec association de type de fichier enregistrée sous Windows pour ouvrir les fichiers PDF.

## Paramètres de stratégie Pilotes

June 27, 2024

La section **Pilotes** contient des paramètres de stratégie relatifs aux pilotes d'imprimante.

### Installation automatique de pilotes d'imprimante fournis par défaut

> **Remarque**
>
> Cette stratégie ne prend pas en charge les VDA dans cette version.

Ce paramètre active ou désactive l'installation automatique des pilotes d'imprimante à partir des éléments suivants :

- Ensemble de pilotes Windows intégrés
- Packs de pilotes installés sur l'hôte à l'aide de `pnputil.exe /a`

Par défaut, ces pilotes sont installés selon vos besoins.

### Préférence de pilote universel

Ce paramètre spécifie l'ordre dans lequel les pilotes d'imprimante universels sont utilisés, en commençant par la première entrée de la liste.

Par défaut, l'ordre de préférence est le suivant :

- EMF
- XPS
- PCL5c
- PCL4
- PS

Vous pouvez ajouter, modifier ou supprimer des pilotes et changer leur ordre dans la liste.

### Utilisation du pilote d'impression universelle

Ce paramètre spécifie à quel moment utiliser l'impression universelle.

Par défaut, l'impression universelle n'est utilisée que si le pilote demandé n'est pas disponible.

L'impression universelle utilise des pilotes d'imprimante génériques au lieu de pilotes spécifiques au modèle standard, simplifiant potentiellement la charge de gestion des pilotes sur les ordinateurs hôtes. La disponibilité des pilotes d'impression universels dépend des capacités de la machine utilisateur, de l'hôte et du logiciel du serveur d'impression. Dans certaines configurations, il se peut que l'impression universelle ne soit pas disponible.

Lorsque vous ajoutez ce paramètre à une stratégie, sélectionnez une option dans le tableau suivant :

| Option | Description |
|---|---|
| **Utiliser uniquement les pilotes spécifiques au modèle de l'imprimante** | Spécifie que l'imprimante cliente utilise uniquement les pilotes spécifiques au modèle standard créés automatiquement lors de la connexion. Si le pilote requis n'est pas disponible, l'imprimante cliente ne peut pas être créée automatiquement. |
| **Utiliser l'impression universelle uniquement** | Spécifie qu'aucun pilote spécifique au modèle standard n'est utilisé. Seuls les pilotes d'impression universelle sont utilisés pour créer des imprimantes. |

| Option | Description |
| --- | --- |
| **Utiliser l'impression universelle uniquement si le pilote requis n'est pas disponible** | Utilise les pilotes spécifiques au modèle standard pour la création d'imprimantes s'ils sont disponibles. Si le pilote n'est pas disponible sur le serveur, l'imprimante cliente est automatiquement créée à l'aide du pilote d'imprimante universelle approprié. |
| **Utiliser les pilotes spécifiques au modèle d'imprimante uniquement si impression universelle non dispo** | Utilise le pilote d'impression universelle s'il est disponible. Si le pilote n'est pas disponible sur le serveur, l'imprimante cliente est automatiquement créée à l'aide du pilote spécifique au modèle standard approprié. |

## Paramètres de stratégie Serveur d'impression universelle

June 27, 2024

La section **Serveur d'impression universelle** contient les paramètres de stratégie permettant de gérer le Serveur d'impression universelle.

### Suite de chiffrement SSL

Ce paramètre spécifie l'ensemble des suites de chiffrement SSL/TLS utilisées par le client d'impression universelle pour les connexions CGP (flux de données d'impression crypté).

Pour contrôler le package de suite de chiffrement utilisé par le client d'impression universelle pour les connexions HTTPS/SOAP (service Web d'impression chiffrée), consultez [SCHANNEL].

Valeur par défaut : ALL

Ce paramètre a les valeurs suivantes : ALL, COM ou GOV.

Les suites de chiffrement correspondant à chaque valeur sont les suivantes :

**ALL :**

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

TLS_ECDHE_RSA_AES128_CBC_SHA

**COM :**

TLS_ECDHE_RSA_AES128_CBC_SHA

**GOV :**

TLS_ECDHE_RSA_AES256_GCM_SHA384

TLS_ECDHE_RSA_AES256_CBC_SHA384

### Mode de conformité SSL

Ce paramètre spécifie le niveau de conformité avec la norme NIST Special Publication 800-52 utilisée par le client d'impression universelle pour les connexions CGP (flux de données d'impression crypté).

Valeur par défaut : None.

Ce paramètre a les valeurs suivantes :

**Aucun.**

Les connexions CGP utilisent le mode de conformité par défaut.

**SP800-52.**

Les connexions CGP utilisent le mode de conformité NIST Special Publication 800-52.

### SSL activé

Ce paramètre spécifie si SSL/TLS est utilisé par le client d'impression universelle pour les opérations suivantes :

- Connexions de flux de données d'impression (CGP)
- Connexions aux services Web (HTTP/SOAP)

Lorsque vous définissez **Activer le serveur d'impression universelle** sur **Activé avec retour à l'impression distante native de Windows**, les connexions de secours sont effectuées par le fournisseur d'impression réseau Microsoft Windows. Ce paramètre n'affecte pas ces connexions de secours.

Valeur par défaut : Désactivé

Ce paramètre a les valeurs suivantes :

**Activé.**

Le client d'impression universelle utilise SSL/TLS pour se connecter au serveur d'impression universelle.

**Désactivé.**

Le client d'impression universelle utilise SSL/TLS pour se connecter au serveur d'impression universelle.

### Mode FIPS SSL

Ce paramètre spécifie si le module cryptographique SSL/TLS utilisé par le client d'impression universelle pour les connexions CGP s'exécute en mode FIPS.

Valeur par défaut : Désactivé

Ce paramètre a les valeurs suivantes :

**Activé.**

Le mode FIPS est activé.

**Désactivé.**

Le mode FIPS est désactivé.

### Version du protocole SSL

Ce paramètre spécifie la version du protocole SSL/TLS utilisée par le client d'impression universelle.

Valeur par défaut : ALL

Ce paramètre a les valeurs suivantes :

**ALL.**

Utilisez les versions 1.0, 1.1 ou 1.2 de TLS.

**TLSv1.**

Utilisez la version 1.0 de TLS.

**TLSv1.1.**

Utilisez la version 1.1 de TLS.

**TLSv1.2.**

Utilisez la version 1.2 de TLS.

### Port (CGP) du flux de données d'impression crypté du serveur d'impression universelle SSL

Ce paramètre spécifie le numéro de port TCP du port CGP. Ce port reçoit les données des travaux d'impression.

Valeur par défaut : 443

### Port (HTTP/SOAP) du service Web crypté du serveur d'impression universelle SSL

Ce paramètre spécifie le numéro de port TCP du port HTTPS/SOAP (service Web crypté du serveur d'impression universelle). Ce port reçoit les données des commandes d'impression.

Valeur par défaut : 8443

### Activer le serveur d'impression universelle

Cette stratégie active ou désactive l'utilisation du serveur d'impression universelle Citrix (UPS). Appliquez ce paramètre de stratégie aux unités organisationnelles (UO) qui incluent les applications de bureau virtuel ou d'hébergement de serveurs. Ces paramètres de stratégie incluent des options de secours pour autoriser les connexions aux serveurs d'impression à l'aide du service d'impression à distance Windows natif au cas où le composant Citrix UPS n'est pas installé ou n'est pas disponible sur le serveur d'impression demandé. Les modifications apportées à cette stratégie ne s'appliquent qu'après le redémarrage du VDA.

Par défaut, le serveur d'impression universelle est désactivé.

Lorsque vous ajoutez ce paramètre à une stratégie, sélectionnez l'une des options suivantes :

- **Activé avec retour à l'impression distante native de Windows** : le serveur d'impression universelle assure le service des connexions d'imprimante réseau, si possible. Si le serveur d'impression universelle n'est pas disponible, le fournisseur d'impression Windows est utilisé. Le fournisseur d'impression Windows continue de gérer toutes les imprimantes créées précédemment avec le fournisseur d'impression Windows.
- **Activé avec aucun retour à l'impression distante native de Windows** : le serveur d'impression universelle assure exclusivement les connexions d'imprimante réseau. Si le serveur d'impression universelle n'est pas disponible, la connexion de l'imprimante réseau échoue. Ce paramètre désactive de manière effective l'impression réseau au travers du fournisseur d'impression Windows. Les imprimantes créées précédemment avec le fournisseur d'impression Windows ne sont pas créées tant qu'une stratégie contenant ce paramètre est active.
- **Désactivé** : la fonctionnalité Serveur d'impression universelle est désactivée. Aucune tentative de connexion avec le serveur d'impression universelle n'est effectuée lors de la connexion à une imprimante réseau avec un nom UNC. Les connexions aux imprimantes distantes continuent d'utiliser l'outil d'impression à distance Windows natif.

### Port (CGP) du flux de données d'impression du serveur d'impression universelle

Ce paramètre spécifie le numéro de port TCP utilisé par l'écouteur CGP (Common Gateway Protocol) du flux de données d'impression Serveur d'impression universelle. Appliquez ce paramètre de stratégie uniquement aux unités d'organisation contenant le serveur d'impression.

Le numéro port est défini par défaut sur 7229.

Les numéros de port valides doivent se trouver dans une plage de 1 à 65535.

### Limite de bande passante d'entrée du flux d'impression du serveur d'impression universelle (Kbits/s)

Ce paramètre spécifie la limite supérieure (en kilobits par seconde) du taux de transfert des données d'impression. Le taux de transfert est calculé pour les données d'impression mises à disposition depuis chaque tâche d'impression vers le serveur d'impression universelle à l'aide de CGP. Appliquez ce paramètre de stratégie aux unités d'organisation contenant le bureau virtuel ou le serveur hébergeant les applications.

Par défaut, la valeur est 0, qui ne spécifie aucune limite supérieure.

### Port (HTTP/SOAP) du service Web du serveur d'impression universelle

Ce paramètre spécifie le numéro de port TCP utilisé par l'écouteur du service Web Serveur d'impression universelle pour les requêtes (HTTP/SOAP). Le serveur d'impression universelle est un composant facultatif qui permet l'utilisation des pilotes d'impression universelle Citrix dans les scénarios d'impression réseau.

Lorsque le serveur d'impression universelle est utilisé, les commandes d'impression sont envoyées depuis les hôtes Citrix Virtual Apps and Desktops vers le serveur d'impression universelle via SOAP sur HTTP. Ce paramètre modifie le port TCP par défaut sur lequel le serveur d'impression universelle écoute les requêtes HTTP/SOAP entrantes.

Vous devez configurer le port HTTP du serveur d'impression et de l'hôte de façon identique. Si les ports ne sont pas configurés de manière identique, le logiciel de l'hôte ne se connecte pas au serveur d'impression universelle. Ce paramètre modifie le VDA sur Citrix Virtual Apps and Desktops. Par ailleurs, vous devez modifier le port par défaut sur le serveur d'impression universelle.

Le numéro port est défini par défaut sur 8080.

Les numéros de port valides doivent se trouver dans une plage de 0 à 65535.

### Serveurs d'impression universelle d'équilibrage de la charge

Ce paramètre dresse la liste des serveurs d'impression universelle à utiliser pour répartir la charge des connexions aux imprimantes établies lors du lancement de la session, après l'évaluation d'autres paramètres de stratégie d'impression Citrix. Pour optimiser la durée de création des imprimantes, Citrix recommande que les mêmes imprimantes partagées soient installées sur tous les serveurs d'impression. Il n'existe aucune limite au nombre de serveurs d'impression qui peuvent être ajoutés pour l'équilibrage de charge.

Ce paramètre s'applique également à la détection de basculement de serveur d'impression et à la récupération de connexion d'imprimante. Les serveurs d'impression contrôlent la disponibilité périodiquement. Si une panne de serveur est détectée, ce serveur est supprimé du schéma d'équilibrage de charge. Les connexions d'imprimantes sur ce serveur sont également redistribuées entre les autres serveurs d'impression disponibles. Après reprise du serveur d'impression défaillant, il reprend sa place dans le schéma d'équilibrage de charge.

Cliquez sur **Valider les serveurs** pour vérifier que chaque serveur est un serveur d'impression, que la liste de serveurs ne contient pas de noms de serveur dupliqués et que tous les serveurs possèdent un ensemble identique d'imprimantes partagées. Cette opération peut prendre un certain temps.

### Seuil au-delà duquel les serveurs d'impression universelle sont hors service

Ce paramètre indique la durée pendant laquelle l'équilibrage de charge doit attendre le rétablissement de la connexion à un serveur d'impression universelle avant de considérer que le serveur est hors connexion et de répartir sa charge sur d'autres serveurs d'impression disponibles.

Par défaut, la valeur de seuil est de 180 (secondes).

### Délai d'expiration de connexion du service Web du serveur d'impression universelle (HTTP/SOAP)

Ce paramètre spécifie le nombre de secondes pendant lesquelles le client d'impression universelle attend l'expiration d'une opération connect() du service Web du serveur d'impression universelle. Ce paramètre a les valeurs suivantes. Toutes ces valeurs sont numériques et les unités (de temps) sont les secondes.

- La valeur minimale est 0
- La valeur maximale est 60.
- La valeur par défaut est 10.

Lorsque le délai d'expiration est compris entre 1 et 60 (inclus), le client d'impression universelle attend la fin de l'opération pendant la durée spécifiée. L'opération est une opération de connexion d'

un socket TCP. Les sockets sont une fonctionnalité du système d'exploitation Windows qui permet la communication entre processus sur les réseaux TCP/IP.

Lorsque le délai d'expiration est égal à 0, le client d'impression universelle utilise le délai d'expiration par défaut défini par le système d'exploitation. Cette configuration était la configuration disponible présente dans les versions précédentes du client d'impression universelle avant cette modification.

Le client d'impression universelle est le composant du Virtual Delivery Agent (VDA) qui communique avec le serveur d'impression universelle.

> **Remarque :**
>
> Ce paramètre de stratégie est applicable au VDA 7.35 et versions ultérieures.

### Délai de réception du service Web du serveur d'impression universelle (HTTP/SOAP)

Ce paramètre indique le nombre de secondes pendant lesquelles le client d'impression universelle doit attendre jusqu'à ce qu'une opération recv() du service Web du serveur d'impression universelle expire. Ce paramètre a les valeurs suivantes. Toutes ces valeurs sont numériques et les unités (de temps) sont des secondes.

- La valeur minimale est 0
- La valeur maximale est 60.
- La valeur par défaut est 10.

Lorsque le délai d'expiration est compris entre 1 et 60 (inclus), le client d'impression universelle attend la fin de l'opération pendant la durée spécifiée. L'opération est une opération de réception d'un socket TCP. Les sockets sont une fonctionnalité du système d'exploitation Windows qui permet la communication entre processus sur les réseaux TCP/IP.

Lorsque le délai d'expiration est égal à 0, le client d'impression universelle utilise le délai d'expiration par défaut défini par le système d'exploitation. Cette configuration était la configuration disponible présente dans les versions précédentes du client d'impression universelle avant cette modification.

Le client d'impression universelle est le composant du Virtual Delivery Agent (VDA) qui communique avec le serveur d'impression universelle.

> **Remarque :**
>
> Ce paramètre de stratégie est applicable au VDA 7.35 et versions ultérieures.

### Délai d'envoi du service Web du serveur d'impression universelle (HTTP/SOAP)

Ce paramètre indique le nombre de secondes pendant lesquelles le client d'impression universelle doit attendre jusqu'à ce qu'une opération send() du service Web du serveur d'impression universelle

expire. Ce paramètre a les valeurs suivantes. Toutes ces valeurs sont numériques et les unités (de temps) sont les secondes.

- La valeur minimale est 0
- La valeur maximale est 60.
- La valeur par défaut est 10.

Lorsque le délai d'expiration est compris entre 1 et 60 (inclus), le client d'impression universelle attend la fin de l'opération pendant la durée spécifiée. L'opération est une opération d'envoi d'un socket TCP. Les sockets sont une fonctionnalité du système d'exploitation Windows qui permet la communication entre processus sur les réseaux TCP/IP.

Lorsque le délai d'expiration est égal à 0, le client d'impression universelle utilise le délai d'expiration par défaut défini par le système d'exploitation. Cette configuration était la configuration disponible présente dans les versions précédentes du client d'impression universelle avant cette modification.

Le client d'impression universelle est le composant du Virtual Delivery Agent (VDA) qui communique avec le serveur d'impression universelle.

> **Remarque :**
>
> Ce paramètre de stratégie est applicable au VDA 7.35 et versions ultérieures.

## Paramètres de stratégie Impression universelle

June 27, 2024

La section **Impression universelle** contient des paramètres de stratégie permettant de gérer l'impression universelle.

### Mode de traitement de l'impression universelle EMF

Ce paramètre contrôle la méthode de traitement du fichier de spoule EMF sur la machine utilisateur Windows.

Par défaut, les enregistrements EMF sont spoulés directement sur l'imprimante.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Traiter à nouveau les EMF pour l'imprimante oblige le fichier de spoule EMF à être traité à nouveau et envoyé au travers du sous-système GDI sur la machine utilisateur. Vous pouvez utiliser ce paramètre pour les pilotes qui requièrent un nouveau traitement EMF mais qui peuvent ne pas être sélectionnés automatiquement dans une session.

- Spouler directement vers l'imprimante, lorsque utilisé avec le pilote d'impression universelle Citrix, assure que les données EMF sont spoulées et mises à disposition vers la machine utilisateur pour traitement. Généralement, ces fichiers de spoule EMF sont directement injectés dans la file d'attente du spoule du client. Pour les imprimantes et les pilotes qui sont compatibles avec le format EMF, ceci représente la méthode d'impression la plus rapide.

### Limite de compression d'image de l'impression universelle

Ce paramètre entraîne les effets suivants :

- Qualité maximale disponible pour les images imprimées avec le pilote d'impression universel Citrix
- Niveau de compression minimal disponible pour les images imprimées avec le pilote d'impression universel Citrix

Par défaut, la limite de compression d'image est définie sur Meilleure qualité (compression sans perte).

Si Aucune compression est sélectionnée, la compression est désactivée uniquement pour l'impression EMF.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Aucune compression
- Meilleure qualité (compression sans perte)
- Qualité élevée
- Qualité standard
- Qualité réduite (compression maximale)

Lorsque vous ajoutez ce paramètre à une stratégie qui comprend le paramètre **Valeurs par défaut de l'optimisation de l'impression universelle**, assurez-vous des éléments suivants :

- Vérifiez que le niveau de compression du paramètre **Limite de compression d'image de l'impression universelle** est inférieur au niveau défini dans le paramètre **Valeurs par défaut de l'optimisation de l'impression universelle**. Dans ce cas, les images sont compressées à l'aide du niveau défini dans le paramètre Limite de compression d'image de l'impression universelle.
- Si la compression est désactivée, les options Qualité d'image souhaitée et Activer la compression lourde du paramètre Valeurs par défaut de l'optimisation de l'impression universelle n'ont aucun effet sur la stratégie.

### Valeur par défaut d'optimisation de l'impression universelle

Ce paramètre spécifie les valeurs par défaut de l'optimisation de l'impression lorsque le pilote d'impression universelle est créé pour une session.

- Qualité d'image souhaitée spécifie la limite de compression d'image par défaut appliquée à l'impression universelle. Par défaut, Qualité standard est activée, signifiant que les utilisateurs peuvent uniquement imprimer des images à l'aide des compressions standard ou de qualité réduite.
- Activer la compression lourde active ou désactive la réduction de la bande passante au-delà du niveau de compression défini par l'option Qualité d'image souhaitée, sans perte de qualité d'image. Par défaut, la compression intensive est désactivée.
- Les paramètres Cache d'image et de police spécifient si vous pouvez mettre en cache ou non des images et des polices qui s'affichent plusieurs fois dans le flux d'impression. Ces paramètres garantissent que chaque image ou police est envoyée à l'imprimante une seule fois. Par défaut, les images incorporées et les polices sont mises en cache. Ces paramètres s'appliquent uniquement si la machine utilisateur prend ce comportement en charge.
- Autoriser les non-administrateurs à modifier ces paramètres spécifie si les utilisateurs peuvent ou non modifier les paramètres d'optimisation d'impression dans une session. Par défaut, les utilisateurs ne sont pas autorisés à modifier les paramètres par défaut d'optimisation de l'impression.

Remarque : toutes ces options sont prises en charge pour l'impression EMF. Pour l'impression XPS, seule l'option Qualité d'image souhaitée est prise en charge.

Lorsque vous ajoutez ce paramètre à une stratégie qui comprend le paramètre **Limite de compression d'image de l'impression universelle**, assurez-vous des éléments suivants :

- Vérifiez que le niveau de compression du paramètre **Limite de compression d'image de l'impression universelle** est inférieur au niveau défini dans le paramètre **Valeurs par défaut de l'optimisation de l'impression universelle**. Dans ce cas, les images sont compressées à l'aide du niveau défini dans le paramètre Limite de compression d'image de l'impression universelle.
- Si la compression est désactivée, les options Qualité d'image souhaitée et Activer la compression lourde du paramètre Valeurs par défaut de l'optimisation de l'impression universelle n'ont aucun effet sur la stratégie.

### Préférence d'aperçu d'impression universelle

Ce paramètre spécifie si la fonction d'aperçu d'impression doit être utilisée pour les imprimantes créées automatiquement ou les imprimantes universelles génériques.

Par défaut, l'aperçu d'impression n'est pas utilisé pour les imprimantes créées automatiquement ou les imprimantes universelles génériques.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Ne pas utiliser l'aperçu pour les imprimantes créées automatiquement ou universelles génériques
- Utiliser l'aperçu d'impression pour les imprimantes créées automatiquement uniquement
- Utiliser l'aperçu d'impression pour les imprimantes universelles génériques uniquement
- Utiliser l'aperçu pour les imprimantes créées automatiquement et universelles génériques

### Limite de qualité d'image de l'impression universelle

Ce paramètre spécifie le nombre maximal de points par pouce (ppp) disponible pour l'impression dans la session.

Par défaut, l'option Aucune limite est activée, signifiant que les utilisateurs peuvent sélectionner la qualité d'impression maximale autorisée par l'imprimante à laquelle ils se connectent.

Si ce paramètre est configuré, il limite la qualité d'impression maximale disponible auprès des utilisateurs en termes de résolution. À la fois la qualité d'impression elle-même et les capacités de qualité d'impression de l'imprimante à laquelle l'utilisateur se connecte sont restreintes au paramètre configuré.

Par exemple, si ce paramètre est configuré sur une résolution moyenne (600 ppp), les utilisateurs peuvent imprimer avec une qualité maximale de 600 ppp uniquement. En outre, le paramètre **Qualité d'impression** de l'onglet **Avancé** de la boîte de dialogue **Imprimante universelle** affiche les paramètres de résolution uniquement jusqu'à et y compris la qualité moyenne (600 ppp).

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- Brouillon (150 PPP)
- Basse résolution (300 PPP)
- Moyenne résolution (600 PPP)
- Haute résolution (1200 PPP)
- Sans limite

## Paramètres de stratégie Sécurité

June 27, 2024

La section **Sécurité** contient des paramètres de stratégie permettant de configurer le cryptage de session et des données d'ouverture de session.

### Niveau de cryptage minimum SecureICA

Ce paramètre spécifie le niveau minimal auquel crypter les données de session envoyées entre le serveur et une machine utilisateur.

**Important :** pour Virtual Delivery Agent 7.x, ce paramètre de stratégie peut être utilisé uniquement pour activer le cryptage des données d'ouverture de session à l'aide du cryptage RC5 128 bits. Cette option est fournie uniquement à des fins de compatibilité à effet rétroactif avec les versions d'ancienne génération de Citrix Virtual Apps and Desktops.

Pour VDA 7.x, le cryptage des données de session est défini à l'aide des paramètres de base du groupe de mise à disposition du VDA. Si l'option Activer Secure ICA est sélectionnée pour le groupe de mise à disposition, les données de session sont cryptées à l'aide du cryptage RC5 (128 bits). Si l'option Activer Secure ICA n'est pas sélectionnée pour le groupe de mise à disposition, les données de session sont cryptées à l'aide du cryptage de base.

Lors de l'ajout de ce paramètre à une stratégie, sélectionnez une option :

- De base crypte la connexion à l'aide d'un algorithme non RC5. Cet algorithme protège le flux de données d'une lecture directe, mais n'empêche pas le décryptage. Par défaut, le serveur utilise un cryptage de base pour le trafic client vers serveur.
- 128 bits - ouverture de session uniquement (RC5) crypte les données d'ouverture de session à l'aide du cryptage RC5 128 bits et la connexion cliente à l'aide du cryptage de base.
- 40 bits (RC5) crypte la connexion cliente à l'aide du cryptage RC5 40 bits.
- 56 bits (RC5) crypte la connexion cliente à l'aide du cryptage RC5 56 bits.
- 128 bits (RC5) crypte la connexion cliente à l'aide du cryptage RC5 128 bits.

Les paramètres que vous spécifiez pour le cryptage client-serveur peuvent interagir avec tout autre paramètre de cryptage de votre environnement et de votre système d'exploitation Windows. Vérifiez qu'un niveau de cryptage de priorité plus élevé est défini sur un serveur ou une machine utilisateur. Dans ce cas, les paramètres que vous spécifiez pour des ressources publiées peuvent être remplacés.

Vous pouvez augmenter les niveaux de cryptage afin de mieux sécuriser les communications et l'intégrité des messages pour certains utilisateurs. Si une stratégie requiert un niveau de cryptage plus élevé, les Citrix Receivers utilisant un niveau de cryptage inférieur se voient refuser la connexion.

SecureICA n'effectue pas d'authentification ni ne vérifie l'intégrité des données. Pour assurer un cryptage de bout en bout pour votre site, utilisez SecureICA avec le cryptage TLS.

SecureICA n'utilise pas d'algorithme conforme à la norme FIPS. Si ce paramètre pose un problème, configurez le serveur et Citrix Receiver pour éviter d'utiliser SecureICA.

SecureICA utilise le chiffrement par blocs RC5 décrit dans RFC 2040 pour assurer la confidentialité. La taille des blocs est 64 bits (un multiple d'unités de mots de 32 bits). La longueur de clé est 128 bits. Le nombre de boucles est 12.

Les clés du chiffrement par blocs RC5 sont négociées lors de la création d'une session. La négociation est effectuée à l'aide de l'algorithme Diffie-Hellman. Cette négociation utilise les paramètres publics Diffie-Hellman. Ces paramètres sont stockés dans le registre Windows lorsque Virtual Delivery Agent est installé. Les paramètres publics ne sont pas secrets. Le résultat de la négociation Diffie-Hellman est une clé secrète, à partir de laquelle sont dérivées les clés de session du chiffrement par blocs RC5. Des clés de session distinctes sont utilisées pour l'ouverture de session de l'utilisateur et pour le transfert de données. Des clés de session distinctes sont également utilisées pour le trafic à destination et en provenance de Virtual Delivery Agent. Il y a donc quatre clés de session pour chaque session. Les clés secrètes et les clés de session ne sont pas stockées. Les vecteurs d'initialisation du chiffrement par blocs RC5 sont également dérivés de la clé secrète.

## Paramètres de stratégie Limites de serveur

June 27, 2024

La section **Limites de serveur** contient le paramètre de stratégie permettant de contrôler les connexions inactives.

### Intervalle d'horloge inactive du serveur

Ce paramètre détermine la durée pendant laquelle une session utilisateur non interrompue pourra être maintenue si aucune entrée utilisateur n'est effectuée. Les données sont calculées en millisecondes.

Par défaut, les connexions inactives ne sont pas déconnectées (Intervalle d'horloge inactive du serveur = 0). Citrix vous recommande de définir cette valeur sur un minimum de 60 000 millisecondes (60 secondes).

Pour afficher la stratégie, sélectionnez **Versions multiples**, effacez les versions OS mono-session, puis sélectionnez **Limites de serveur**.

> **Remarque**
>
> Lorsque ce paramètre de stratégie est utilisé, une boîte de dialogue indiquant que le minuteur d'inactivité a expiré peut s'afficher lorsque la session a été inactive pendant la durée spécifiée. Les paramètres de stratégie Citrix ne contrôlent pas ce message de boîte de dialogue Microsoft.Pour plus d'informations, consultez http://support.citrix.com/article/CTX118618.

# Paramètres de stratégie des limites de session

June 27, 2024

La section **Limites de session** contient des paramètres de stratégie qui permettent de contrôler la durée pendant laquelle les sessions restent connectées avant que leur fermeture soit imposée.

## Horloge de session déconnectée

Ce paramètre active ou désactive une horloge permettant de déterminer la durée pendant laquelle un bureau déconnecté et verrouillé reste verrouillé avant fermeture de la session.

Si cette horloge est activée, la session déconnectée est fermée à l'expiration de l'horloge.

Par défaut, les sessions déconnectées ne sont pas fermées.

## Horloge de session déconnectée Remote PC Access

Ce paramètre active ou désactive une horloge qui met fin à une session utilisateur déconnectée après l'expiration de la minuterie de l'horloge. Si vous activez ce paramètre, utilisez le paramètre **Intervalle d'horloge de session déconnectée** pour spécifier combien de minutes un bureau déconnecté reste verrouillé avant que la session utilisateur ne soit terminée.

Par défaut, ce paramètre est désactivé.

## Intervalle d'horloge de session déconnectée

Ce paramètre détermine la durée, en minutes, pendant laquelle un bureau déconnecté et verrouillé reste verrouillé avant que la session ne se ferme.

Par défaut, ce délai est de 1440 minutes (24 heures).

## Horloge de session déconnectée : multi-session

Ce paramètre active ou désactive une horloge pour déterminer la durée pendant laquelle une session RDS déconnectée peut persister avant la fermeture de la session. Par défaut, cette horloge est désactivée et les sessions déconnectées ne sont pas fermées.

### Intervalle d'horloge de session déconnectée : multi-session

Ce paramètre détermine le nombre de minutes pendant lesquelles une session RDS déconnectée peut persister avant la fermeture de la session. Par défaut, ce délai est de 1440 minutes (24 heures).

### Horloge de connexion de session

Ce paramètre active ou désactive une horloge permettant de déterminer la durée maximale d'une connexion ininterrompue entre une machine utilisateur et un bureau. Si cette horloge est activée, la session est déconnectée ou fermée à l'expiration de l'horloge. Le paramètre Microsoft **Mettre fin à la session quand les délais d'expiration ont été atteints** détermine l'état suivant de la session.

Par défaut, cette horloge est désactivée.

### Intervalle d'horloge de connexion de session

Ce paramètre spécifie le nombre maximal de minutes d'une connexion ininterrompue entre une machine utilisateur et un bureau.

Par défaut, la durée maximale est de 1440 minutes (24 heures).

### Horloge de connexion de session : multi-session

Ce paramètre active ou désactive une horloge permettant de déterminer la durée maximale d'une connexion ininterrompue entre une machine utilisateur et un serveur terminal. Par défaut, cette horloge est désactivée.

### Intervalle d'horloge de connexion de session : multi-session

Ce paramètre spécifie le nombre maximal de minutes d'une connexion ininterrompue entre une machine utilisateur et une session RDS. Par défaut, la durée maximale est de 1440 minutes (24 heures).

### Horloge inactive de session

Si aucune valeur n'est entrée, ce paramètre est utilisé pour activer ou désactiver :

- Une horloge qui détermine la durée pendant laquelle une connexion ininterrompue entre une machine utilisateur et un bureau est maintenue.

Lorsque cette horloge expire, la session est placée dans l'état déconnecté et le paramètre **Horloge de session déconnectée** s'applique. Si le paramètre **Horloge de session déconnectée** est désactivé, la session n'est pas fermée.

Par défaut, cette horloge est activée.

### Intervalle d'horloge inactive de session

En l'absence de saisie de la part de l'utilisateur, ce paramètre est utilisé pour spécifier :

- Le nombre de minutes pendant lesquelles une connexion ininterrompue entre une machine utilisateur et un bureau est maintenue.

Par défaut, les connexions inactives sont maintenues pendant 1440 minutes (24 heures).

### Horloge d'inactivité de session : multi-session

Ce paramètre active ou désactive une horloge afin de déterminer la durée maximale d'une connexion inactive entre une machine utilisateur et un serveur Terminal Server. Par défaut, cette horloge est désactivée.

### Intervalle d'horloge d'inactivité de session : multi-session

Ce paramètre spécifie le nombre de minutes d'une connexion inactive entre une machine utilisateur et une session RDS. Par défaut, la durée maximale est de 1440 minutes (24 heures).

> **Remarque :**
>
> Les paramètres d'horloge pour les machines multisession configurées à l'aide des stratégies Citrix sont censés remplacer les paramètres d'horloge configurés via les stratégies de groupe. Pour éviter tout comportement inattendu, nous vous recommandons de configurer les paramètres d'horloge à l'aide de l'une des deux méthodes.

## Paramètres de stratégie Fiabilité de session

June 27, 2024

La section **Fiabilité de session** contient les paramètres de stratégie permettant de gérer les connexions de fiabilité de session.

### Connexions de fiabilité de session

Ce paramètre autorise ou empêche les sessions de rester ouvertes en cas de perte de connexion réseau. La fiabilité de session, associée à la reconnexion automatique des clients, permet aux utilisateurs de se reconnecter automatiquement à leurs sessions d'application Citrix Workspace suite au rétablissement de la connexion au réseau. Par défaut, la fiabilité de session est autorisée.

Les paramètres de Web Studio sont appliqués sur le client pour ce qui suit :

- Application Citrix Workspace 1808 et versions ultérieures.
- Citrix Receiver pour Windows 4.7 et versions ultérieures.

La stratégie Web Studio remplace l'objet de stratégie de groupe Citrix Receiver sur les clients. Les mises à jour vers ces stratégies dans Web Studio synchronisent la fiabilité de session du serveur et du client.

> **Remarque :**
>
> - Citrix Receiver pour Windows 4.7 et versions ultérieures, et applications Citrix Workspace pour Windows ; définissez la stratégie dans Web Studio.
> - Citrix Receiver pour Windows antérieurs à la version 4.7 : définissez des stratégies dans Web Studio. Définissez également le modèle d'objet de stratégie de groupe Citrix Receiver sur le client pour un comportement cohérent.

La fiabilité de session maintient les sessions actives sur l'écran de l'utilisateur lorsque la connectivité au réseau est interrompue. L'utilisateur peut donc visualiser l'application jusqu'à ce que la connexion réseau reprenne.

Utilisez la fiabilité de session pour maintenir la session active sur le serveur. Pour indiquer que la connectivité est interrompue, l'affichage de l'utilisateur devient opaque. L'utilisateur peut voir une session bloquée pendant l'interruption. L'utilisateur peut reprendre l'interaction avec l'application lorsque la connexion réseau est rétablie. La fonction de fiabilité de session permet aux utilisateurs de se reconnecter sans invite de s'authentifier à nouveau.

Si vous utilisez la fonction de fiabilité de session et la fonction de reconnexion automatique des clients, ces fonctions agissent l'une après l'autre. La fonction de fiabilité de session ferme (ou déconnecte) la session utilisateur après l'expiration de la durée spécifiée dans le paramètre Expiration de délai de la fiabilité de session. Ensuite, les paramètres de reconnexion automatique des clients s'appliquent et la fonction tente de reconnecter l'utilisateur à la session déconnectée.

Par défaut, la fiabilité de session est autorisée.

> **Remarque :**
>
> Lorsque Citrix ADC est en cours d'utilisation, vous devez sélectionner **Activer la fiabilité de session** dans Citrix StoreFront > **Gérer Citrix Gateways**/**Secure Ticket Authority** pour les connex-

> ions ICA proxy.

### Numéro de port de la fiabilité de session

Ce paramètre spécifie le numéro de port TCP pour les connexions de fiabilité de session entrantes.

Le numéro port est défini par défaut sur 2598.

### Expiration de délai de la fiabilité de session

Ce paramètre spécifie la durée, en secondes. Il s'agit de la durée pendant laquelle le proxy de fiabilité de session attend qu'un client se reconnecte avant d'autoriser la déconnexion de la session.

Bien que vous puissiez prolonger la durée pendant laquelle une session reste ouverte, mais le but de cette fonction consiste à éviter à l'utilisateur de devoir s'authentifier de nouveau. Plus une session reste ouverte longtemps, et plus les chances qu'un utilisateur laisse l'appareil sans surveillance et que ce dernier soit potentiellement accessible par des utilisateurs non autorisés augmentent.

Par défaut, le délai d'expiration est défini sur 180 secondes, ou trois minutes.

## Paramètres de stratégie Filigrane de session

June 27, 2024

La section **Filigrane de session** contient des paramètres de stratégie permettant de configurer cette fonctionnalité.
L'activation de cette fonctionnalité entraîne une augmentation significative de la bande passante réseau et de l'utilisation de l'UC par la machine VDA. Nous vous recommandons de configurer le filigrane de session pour les machines VDA sélectionnées en fonction de vos ressources matérielles disponibles.

> **Important**
>
> Activez le filigrane de session pour que les autres paramètres de stratégie de filigrane soient effectifs. Pour améliorer l'expérience utilisateur, n'activez pas plus de deux éléments de texte en filigrane.

### Activer filigrane de session

Lorsque vous activez ce paramètre, l'affichage de la session comporte un filigrane textuel opaque affichant des informations spécifiques à la session. Les autres paramètres de filigrane dépendent du

paramètre activé.

Par défaut, le filigrane de session est désactivé.

### Inclure adresse IP du client

Lorsque vous activez ce paramètre, la session affiche l'adresse IP du client actuel en tant que filigrane.

Par défaut, l'option Inclure adresse IP du client est désactivée.

### Inclure l'heure de connexion

Lorsque vous activez ce paramètre, le filigrane de session affiche une heure de connexion. Le format est aaaa/mm/jj hh:mm. L'heure affichée est basée sur l'horloge système et le fuseau horaire.

Par défaut, l'option Inclure l'heure de connexion est désactivée.

### Inclure nom d'utilisateur de connexion

Lorsque vous activez ce paramètre, la session affiche le nom d'utilisateur de connexion actuel en tant que filigrane. Le format d'affichage est NOMUTILISATEUR@NOMDOMAINE. Nous vous recommandons d'utiliser un nom d'utilisateur de 20 caractères maximum. Lorsqu'un nom d'utilisateur comporte plus de 20 caractères, des polices de caractère trop petites ou des troncations peuvent se produire et réduire l'efficacité du filigrane.

Par défaut, l'option Inclure nom d'utilisateur de connexion est activée.

### Inclure nom d'hôte du VDA

Lorsque vous activez ce paramètre, la session affiche le nom d'hôte du VDA de la session ICA en cours en tant que filigrane.

Par défaut, l'option Inclure nom d'hôte du VDA est activée.

### Inclure adresse IP du VDA

Lorsque vous activez ce paramètre, la session affiche l'adresse IP du VDA de la session ICA en cours en tant que filigrane.

Par défaut, l'option Inclure adresse IP du VDA est désactivée.

### Style de filigrane de session

Ce paramètre détermine si vous affichez un seul ou plusieurs filigranes. Choisissez **Multiple** ou **Simple** dans le menu déroulant **Valeur**.

L'option **Multiple** permet d'afficher cinq filigranes dans la session. un dans le centre et quatre dans les coins.

L'option **Simple** permet d'afficher un seul filigrane au centre de la session.

Par défaut, l'option Style de filigrane de session est définie sur Multiple.

### Texte personnalisé en filigrane

Ce paramètre vous permet d'afficher du texte personnalisé (par exemple, le nom de l'entreprise) dans le filigrane de la session. Lorsque vous configurez une chaîne non vide, elle affiche le texte dans une nouvelle ligne ajoutant d'autres informations activées dans le filigrane. Le texte personnalisé du filigrane est limité à 25 caractères Unicode. Si vous configurez une chaîne plus longue, elle est tronquée à 25 caractères.

Il n'y a pas de texte par défaut.

À partir de Citrix Virtual Apps and Desktops 7 2206, vous bénéficiez de plus d'options de personnalisation à l'aide de balises personnalisées dans le texte. Par conséquent, le nombre maximum de caractères dans le texte personnalisé est porté à 1024.

Les balises disponibles pour les paramètres de filigrane sont décrites dans le tableau suivant :

| Balise | Description | Exemple |
|---|---|---|
| `<font=value>` | Permet de modifier la police du texte du filigrane. La valeur est le nom d'une police disponible sur le VDA. | `<font=Courier New>` |
| `<fontzoom=value>` | Permet de définir le pourcentage du facteur de zoom de la police. La valeur est 200 pour un zoom de 200% sur le texte du filigrane. | `<fontzoom=200>` |

| Balise | Description | Exemple |
|---|---|---|
| <position=value> | Permet de modifier la position du texte du filigrane. Les valeurs sont center, topleft, topright, bottomleft et bottomright. Cette balise n'est applicable qu'avec un seul style. | <position=topright> |
| <rotation=value> | Permet de faire pivoter le texte du filigrane. La valeur est spécifiée en degrés et la plage est comprise entre -360 et 360. | <rotation=45> |
| <style=value> | Permet de modifier le style d'affichage. Cette balise remplace la stratégie Style de filigrane de session. | <style=single> |

Les styles de filigrane suivants sont disponibles :

- Style unique : un seul libellé de texte de filigrane apparaît au centre de la session. Vous pouvez utiliser la balise de position pour modifier l'emplacement.
- xstyle or multiple : cinq libellés de filigrane apparaissent dans la session, un au centre et un dans chaque coin.
- Mosaïque : plusieurs libellés apparaissent dans la session. Le texte du filigrane est placé uniformément sur tout l'écran.

Les balises disponibles pour modifier le texte du filigrane sont décrites dans le tableau suivant :

| Balise | Description |
|---|---|
| <clientip> | Adresse IP du point de terminaison. |
| <date> | Date à laquelle la session a été établie. |
| <domain> | Nom de domaine du compte d'utilisateur connecté. |
| <hostname> | Nom de la machine du VDA. |
| <newline> | Crée une ligne supplémentaire. |
| <serverip> | Adresse IP du VDA. |

| Balise | Description |
| --- | --- |
| <time> | Heure à laquelle la session a été établie. |
| <username> | Nom de l'utilisateur. |

> **Remarque :**
>
> - La stratégie **Texte personnalisé en filigrane** prend effet uniquement lorsque la stratégie **Activer filigrane de session** est activée. Sa valeur par défaut est *Désactivé*.
> - Si vous utilisez les balises pour modifier le texte du filigrane, toutes les autres stratégies de filigrane de session, à l'exception de **Activer filigrane de session**, sont ignorées. Si vous utilisez les balises pour les paramètres de texte du filigrane, vous pouvez utiliser toutes les autres stratégies de filigrane.

### Transparence du filigrane

Vous pouvez spécifier l'opacité du filigrane de 0 à 100. Plus la valeur spécifiée est grande, plus le filigrane est opaque.

Par défaut, la valeur est 17.

## Paramètres de stratégie Contrôle des fuseaux horaires

June 27, 2024

La section **Contrôle de fuseau horaire** contient des paramètres de stratégie liés à l'utilisation de l'heure locale dans les sessions.

### Estimation de l'heure locale des anciens clients

Ce paramètre permet d'activer ou de désactiver l'estimation de l'heure locale des machines des utilisateurs. Ces appareils incluent les machines utilisateur qui envoient des informations de fuseau horaire inexactes au serveur.

Par défaut, le serveur estime le fuseau horaire local, si nécessaire.

Ce paramètre est conçu pour être utilisé avec les versions antérieures de Citrix Receiver ou clients ICA qui n'envoient pas d'informations de fuseau horaire au serveur. Vérifiez si ce paramètre est utilisé avec les Citrix Receiver qui envoient des informations détaillées sur le fuseau horaire au serveur, par

exemple, les versions prises en charge de Citrix Receiver pour Windows. Dans ce cas, ce paramètre n'a aucun effet.

### Restaurer le fuseau horaire du système d'exploitation de bureau lors de la déconnexion ou de la fermeture de session

Vérifiez si l'utilisateur se déconnecte ou met fin à la session. Dans ce cas, ce paramètre détermine si le paramètre de fuseau horaire pour un VDA avec OS mono-session revient au fuseau horaire d'origine de la machine Si vous activez ce paramètre, le VDA rétablit le fuseau horaire de la machine sur son paramètre d'origine lorsque l'utilisateur se déconnecte ou met fin à la session. Pour que ce paramètre prenne effet, définissez **Utiliser l'heure locale du client** sur **Utiliser le fuseau horaire du client**.

Ce paramètre est activé par défaut.

### Utiliser l'heure locale du client

Ce paramètre permet de déterminer le fuseau horaire de la session utilisateur. Vous pouvez choisir entre le fuseau horaire de la session utilisateur (fuseau horaire du serveur) et le fuseau horaire de la machine utilisateur (fuseau horaire client).

Par défaut, le fuseau horaire de la session de l'utilisateur est utilisé.

Pour que ce paramètre prenne effet, activez le paramètre **Autoriser la redirection de fuseau horaire** dans l'Éditeur de stratégie de groupe. Ce paramètre se trouve dans **Stratégie Ordinateur local** > **Configuration ordinateur** > **Modèles d'administration** > **Composants Windows** > **Services Bureau à distance** > **Hôte de session Bureau à distance** > **Redirection de périphérique et de ressource**.

Si vous utilisez un VDA mono-session (anciennement VDA poste de travail) sur des machines exécutant un système d'exploitation de serveur, configurez le droit de l'utilisateur local **Modifier le fuseau horaire** sur **Tout le monde**. Ce droit d'utilisateur se trouve dans **Stratégie Ordinateur local** > **Configuration ordinateur** > **Paramètres Windows** > **Paramètres de sécurité** > **Stratégies locales** > **Attribution des droits utilisateur**.

> **Remarque :**
>
> Dans un système d'exploitation mono-session, les **utilisateurs** sont inclus dans l'attribution des droits utilisateur **Modifier le fuseau horaire**, mais pas dans un système d'exploitation multi-session. Dans un système d'exploitation multi-session, le fuseau horaire se synchronise à l'aide de la stratégie de groupe suivante : Configuration ordinateur\Modèles d'administration\Composants Windows\Services Bureau à distance\Hôte de session Bureau à distance\Redirection de périphérique et de ressource\Autoriser la redirection du fuseau horaire.

> Cette stratégie s'applique lorsque le serveur est un hôte de session Bureau à distance dans le VDA du système d'exploitation multi-session (installé avec la commande `/ServerVDI`). Dans un système d'exploitation multi-session, par défaut et par conception, les utilisateurs n'ont pas le droit local de modifier le fuseau horaire.

## Paramètres de stratégie Périphériques TWAIN

June 27, 2024

La section **Périphériques TWAIN** contient des paramètres de stratégie liés aux éléments suivants :

- Mappage des périphériques TWAIN clients, tels que des appareils photo numériques ou des scanneurs
- Optimisation des transferts d'images du serveur au client

> **Remarque :**
>
> TWAIN 2.0 est pris en charge par Citrix Receiver pour Windows version 4.5.

### Redirection de périphérique TWAIN client

Les périphériques TWAIN communiquent avec les applications de traitement d'images hébergées par le serveur à l'aide du protocole TWAIN.

Ce paramètre permet ou interdit aux utilisateurs d'accéder aux périphériques TWAIN sur la machine utilisateur. Par défaut, la redirection de périphérique TWAIN est autorisée.

Les paramètres de stratégie suivants sont associés :

- Niveau de compression TWAIN
- Limite de bande passante de redirection du périphérique TWAIN
- Pourcentage de limite de bande passante de redirection du périphérique TWAIN

### Niveau de compression TWAIN

Ce paramètre spécifie le niveau de compression des transferts d'images du client au serveur. Utilisez Basse pour une qualité d'image optimale, Moyenne pour une bonne qualité d'image ou Élevée pour une faible qualité d'image. Par défaut, la compression moyenne est appliquée.

# Paramètres de stratégie Périphériques USB

June 27, 2024

La section **Périphériques USB** contient des paramètres de stratégie permettant de gérer la redirection de fichiers pour les périphériques USB.

## Règles d'optimisation des périphériques USB clients

Les règles d'optimisation des périphériques USB clients peuvent être appliquées aux périphériques pour désactiver l'optimisation, ou pour modifier le mode d'optimisation.

Lorsqu'un utilisateur branche un périphérique USB, l'hôte vérifie si le périphérique est autorisé par les paramètres de **stratégie USB**. Si le périphérique est autorisé, l'hôte vérifie ensuite les **Règles d'optimisation de périphérique USB client** pour le périphérique. Si aucune règle n'est spécifiée, le périphérique n'est pas optimisé. Le mode capture (04) est la méthode recommandée pour les périphériques de signature. Pour les autres périphériques dont les performances se dégradent avec une latence élevée, les administrateurs peuvent activer le mode interactif (02). Voir les descriptions des modes disponibles dans le tableau de cet article.

## À savoir

- Pour l'utilisation de tablettes et de dispositifs de signature numérique Wacom, nous recommandons de désactiver l'écran de veille. Vous trouverez des procédures pour désactiver l'écran de veille à la fin de cette section.
- La prise en charge de l'optimisation des tablettes et des dispositifs de signature numérique Wacom STU a été préconfigurée dans l'installation de stratégies Citrix Virtual Apps and Desktops.
- Les périphériques de signature fonctionnent sur Citrix Virtual Apps and Desktops et ne requièrent pas de pilote pour être utilisés en tant que périphérique de signature. Wacom propose des logiciels supplémentaires qui peuvent être installés pour personnaliser le périphérique. Voir http://www.wacom.com/.
- Tablettes graphiques. Certains périphériques de dessin peuvent être considérés comme périphérique HID sur des bus PCI/ACPI et ne sont pas pris en charge. Connectez ces périphériques sur un contrôleur d'hôte USB sur le client pour être redirigés dans une session Citrix Virtual Desktops.

Les règles de stratégies sont au format tag=value (balise=valeur) séparées par des espaces. Les balises suivantes sont prises en charge :

| Nom de balise | Description |
| --- | --- |
| Mode | Le mode d'optimisation est pris en charge pour les périphériques d'entrée pour une classe=**03**. Les modes pris en charge sont : Aucune optimisation - valeur **01**. Mode interactif - valeur **02**. Recommandé pour les périphériques tels que des tablettes à stylet et des souris 3D Pro. Mode capture - valeur **04**. Mode préféré pour les périphériques tels que les dispositifs de signature numérique. |
| VID | ID fournisseur du descripteur de périphérique, sous forme de nombre hexadécimal à quatre chiffres. |
| PID | ID produit du descripteur de périphérique, sous forme de nombre hexadécimal à quatre chiffres. |
| REV | ID de révision du descripteur de périphérique, sous forme de nombre hexadécimal à quatre chiffres. |
| Classe | Classe du descripteur de périphérique ou d'un descripteur d'interface. |
| Sous-classe | Sous-classe du descripteur de périphérique ou d'un descripteur d'interface. |
| Prot | Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface. |

### Exemples

Mode=00000004 VID=067B PID=1230 class=03 #Périphérique fonctionnant en mode capture

Mode=00000002 VID=067B PID=1230 class=03 #Périphérique fonctionnant en mode interactif (valeur par défaut)

Mode=00000001 VID=067B PID=1230 class=03 #Périphérique fonctionnant sans optimisation

Mode=00000100 VID=067B PID=1230 #Optimisation de la configuration du périphérique désactivée (valeur par défaut)

Mode=00000200 VID=067B PID=1230 #Optimisation de la configuration du périphérique activée

### Désactivation de l'écran de veille des dispositifs de signature numérique Wacom

Pour l'utilisation de tablettes et de dispositifs de signature numérique Wacom, Citrix recommande de désactiver l'écran de veille comme suit :

1. Installez **Wacom-STU-Driver** après la redirection du périphérique.
2. Installez **Wacom-STU-Display MSI** pour pouvoir accéder au panneau de configuration du dispositif de signature.
3. Accédez à **Control Panel > Wacom STU Display > STU430** ou **STU530** et sélectionnez l'onglet de votre modèle.
4. Choisissez sur **Change**, puis sélectionnez **Yes** lorsque la fenêtre de sécurité de compte utilisateur (UAC) s'affiche.
5. Sélectionnez **Disable slideshow**, puis **Apply**.

Une fois que le paramètre est défini pour un modèle de dispositif de signature numérique, il est appliqué à tous les modèles.

### Redirection de périphérique USB client

Ce paramètre permet d'autoriser ou d'empêcher la redirection de périphériques USB vers et depuis la machine utilisateur.

Par défaut, les périphériques USB ne sont pas redirigés.

### Règles de redirection de périphérique USB client

Ce paramètre spécifie les règles de redirection des périphériques USB.

Par défaut, aucune règle n'est spécifiée.

Lorsqu'un utilisateur connecte un périphérique USB, la machine hôte vérifie celui-ci par rapport à chacune des règles de stratégie jusqu'à ce qu'une correspondance soit trouvée. La première correspondance trouvée pour un périphérique est considérée comme définitive. Si la première correspondance est une règle Autoriser, le périphérique est envoyé vers le bureau virtuel. Si la première correspondance est une règle Refuser, le périphérique n'est disponible que pour le bureau local. Si aucune correspondance n'est trouvée, les règles par défaut sont utilisées.

Les règles de stratégies sont au format {Allow:|Deny:} et sont suivies d'un ensemble d'expressions tag=value (balise=valeur) séparées par des espaces. Les balises suivantes sont prises en charge :

| Nom de balise | Description |
|---|---|
| VID | ID fournisseur du descripteur de périphérique |
| PID | ID de produit du descripteur de périphérique |
| REL | ID de version du descripteur de périphérique |
| Classe | Classe du descripteur de périphérique ou d'un descripteur d'interface |
| Sous-classe | Sous-classe du descripteur de périphérique ou d'un descripteur d'interface |
| Prot | Protocole à partir du descripteur de périphérique ou d'un descripteur d'interface |

Lors de la création de règles de stratégie, rappelez-vous ce qui suit :

- Les règles ne sont pas sensibles à la casse.
- Les règles peuvent éventuellement comporter un commentaire, introduit par #, à la fin.
- Les espaces vides et les lignes de commentaires pures sont ignorés.
- Les balises doivent utiliser l'opérateur de correspondance = (par exemple, VID=067B_).
- Chaque règle doit commencer sur une nouvelle ligne ou faire partie d'une liste séparée par des points-virgules.
- Reportez-vous aux codes de classe USB disponibles sur le site Web USB Implementers Forum, Inc.

Exemples de règles de stratégie USB définies par l'administrateur :

- Allow: VID=067B PID=0007 # Another Industries, Another Flash Drive
- Deny: Class=08 subclass=05 # Mass Storage
- Pour créer une règle qui refuse tous les périphériques USB, utilisez « DENY: » sans aucune autre balise.

### Redirection de périphérique Plug and Play USB client

Ce paramètre permet d'autoriser ou d'empêcher l'utilisation de périphériques Plug and Play comme les appareils photo ou les périphériques de point de vente dans une session cliente.

Par défaut, la redirection de périphériques Plug and Play est autorisée. Lorsque l'option est définie sur Autorisé, tous les périphériques Plug and Play d'un utilisateur ou d'un groupe spécifique sont redirigés. Lorsque l'option est définie sur Interdit, aucun périphérique n'est redirigé.

## Configurer la redirection automatique des périphériques USB

Les périphériques USB sont automatiquement redirigés lorsque la prise en charge USB est activée. Les paramètres de préférences de l'utilisateur USB sont également définis pour la connexion automatique aux périphériques USB.

> **Remarque :**
>
> Dans Receiver pour Windows 4.2, les périphériques USB sont également automatiquement redirigés lorsqu'ils se trouvent en mode Desktop Appliance. De plus, la barre de connexion est absente. Dans les versions précédentes de Citrix Receiver pour Windows, les périphériques USB sont également redirigés automatiquement lorsqu'ils sont utilisés dans les cas suivants :
>
> - Mode ordinateur de bureau
> - Applications hébergées sur des machines virtuelles (VM)

Il n'est pas toujours recommandé de rediriger tous les périphériques USB. Les utilisateurs peuvent rediriger explicitement les périphériques de la liste de périphériques USB qui n'est pas automatiquement redirigée. Pour empêcher l'ajout à la liste ou la redirection des périphériques USB, utilisez DeviceRules sur le point de terminaison du client ou sur la stratégie DDC. Voir les guides d'administration pour plus de détails.

> **Attention :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

### Paramètres de préférences utilisateur pour la redirection automatique des périphériques USB

Stratégie :

1. Ouvrez **Éditeur de stratégie de groupe local** et accédez à **Modèles d'administration > Composants Citrix > Citrix Receiver > Accès à distance des périphériques clients > Utilisation à distance de dispositifs USB génériques**.
2. Ouvrez **Nouveaux périphériques USB**, sélectionnez **Activé** et cliquez sur **OK**.
3. Ouvrez **Périphériques USB existants**, sélectionnez **Activé** et cliquez sur **OK**.

Citrix Receiver :

1. Accédez à **Préférences Citrix Receiver > Connexions**.
2. Assurez-vous que les options suivantes sont sélectionnées :

- Au démarrage d'une session, connecter les périphériques automatiquement
- Lorsqu'un nouveau périphérique est connecté alors qu'une session est en cours, connecter le périphérique automatiquement

3. Cliquez sur **OK**.

Toutes les clés de registre et les modifications de stratégie sont appliquées au périphérique client Windows.

#### Redirection des imprimantes USB standard

La meilleure solution pour les imprimantes USB standard consiste à utiliser le pilote d'imprimante universel dédié et le canal virtuel pour effectuer une impression. Par défaut, les imprimantes USB standard ne sont pas automatiquement redirigées.

Les imprimantes standard sont détectées à l'aide de méthodes heuristiques. En outre, il est probable que les imprimantes avancées, dotées de fonctions de numérisation par exemple, doivent être redirigées à l'aide du support USB pour fonctionner complètement.

Utilisez ce registre pour configurer si les imprimantes standard sont automatiquement redirigées :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nom : AutoRedirectPrinters

Type : DWORD

Données : 00000000

La valeur par défaut est 0 (ne redirige pas automatiquement). La modification de la valeur sur une valeur supérieure à zéro permet au support USB de rediriger les imprimantes USB standard.

Vous pouvez également déployer des stratégies Active Directory sur cette clé de registre et remplacer la valeur différente de la stratégie si les deux sont présentes :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nom : AutoRedirectAudio

Type : DWORD

Données : 00000000

#### Redirection de périphériques audio standard

Comme pour les imprimantes standard, la meilleure expérience utilisateur est obtenue en utilisant le canal virtuel audio dédié d'ICA pour envoyer des données audio à partir de périphériques audio standard. Cependant, vous devrez peut-être rediriger certains périphériques spécialisés à l'aide du

support USB. Les méthodes heuristiques permettent de déterminer quels périphériques sont des périphériques audio standard.

Utilisez ce registre sur le point de terminaison client pour configurer si les périphériques audio standard sont automatiquement redirigés :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nom : AutoRedirectAudio

Type : DWORD

Données : 00000000

La valeur par défaut est 0 (ne redirige pas automatiquement). En modifiant la valeur sur une valeur autre que zéro, les périphériques audio USB standard sont redirigés vers un support USB.

Vous pouvez utiliser des stratégies Active Directory pour déployer cette valeur sur la clé de registre et remplacer la valeur différente de la stratégie si les deux sont présentes :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nom : AutoRedirectVideo

Type : DWORD

Données : 00000000

**Redirection des périphériques de stockage standard (périphérique de stockage de masse)**

Pour les périphériques de stockage standard, vous obtenez la meilleure expérience utilisateur possible en utilisant le canal virtuel dédié, tel que le mappage de lecteur client qui effectue également une optimisation. Outre la simple lecture ou écriture de fichiers, pour effectuer certaines tâches spéciales telles que la gravure d'un CD / DVD ou l'accès à des périphériques de systèmes de fichiers chiffrés, il peut être nécessaire de rediriger le périphérique à l'aide du support USB générique.

Les méthodes heuristiques permettent de déterminer quels périphériques sont des périphériques de stockage standard. Utilisez cette clé de registre pour configurer si les périphériques de stockage standard sont automatiquement redirigés :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nom : AutoRedirectStorage

Type : DWORD

Données : 00000000

La valeur par défaut est 0 (ne redirige pas automatiquement). En modifiant la valeur sur une valeur autre que zéro, les périphériques de stockage USB standard sont redirigés à l'aide d'un support USB générique.

Vous pouvez aussi utiliser des stratégies Active Directory pour déployer cette valeur sur la clé de registre suivante et remplacer la valeur différente de la stratégie si les deux sont présentes :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nom : AutoRedirectStorage

Type : DWORD

Données : 00000000

> **Remarque :**
>
> L'accès en lecture seule au périphérique de stockage standard n'est pas configurable si vous utilisez le support USB générique, alors qu'il est configurable si vous utilisez CDM.

#### Clés USB avec redirection de cryptage matériel

Les clés USB avec cryptage matériel sont généralement composées d'une partition de stockage cryptée et d'une seconde partition *utilitaire* contenant un utilitaire permettant de déverrouiller la partition cryptée. Pour les périphériques Lecteur Flash USB, vous obtenez la meilleure expérience utilisateur possible en utilisant le canal virtuel HDX de mappage de lecteur client/mappage de clé USB dynamique dédié qui effectue également une optimisation.

La redirection USB générique est nécessaire pour les opérations suivantes :

- Clients non Windows (par exemple, clients Linux)
- Clients pour lesquels le client dispose d'un accès utilisateur restreint (verrouillé) aux fonctions locales du client

La redirection USB générique peut rediriger n'importe quel périphérique de stockage USB sans cryptage matériel vers les sessions VDA avec OS mono-session et OS multi-session.

Avant Citrix Virtual Apps and Desktops 7 1808, les clés USB avec cryptage matériel ne pouvaient être redirigées de manière utile vers des sessions VDA avec OS mono-session et OS multi-session. Une nouvelle amélioration de la fonctionnalité introduite dans Citrix Virtual Apps and Desktops 7 1808 prend en charge la redirection USB générique des clés USB avec cryptage matériel dans les sessions VDA avec OS mono-session et OS multi-session.
Une fois le périphérique redirigé, aucun de ses lecteurs n'apparaît sur le client local. Si le déverrouillage du lecteur est requis, effectuez-le dans la session. Cette fonctionnalité nécessite la mise à jour Windows KB4074590.

#### Périphériques à images fixes standard (scanners et appareils photo numériques)

Pour les périphériques à images fixes standard, vous obtenez la meilleure expérience utilisateur possible en utilisant le canal virtuel dédié (tel que le canal virtuel TWAIN) qui effectue également une opti-

misation. Ces périphériques doivent être conformes aux normes de l'industrie. Vérifiez si un appareil n'est pas conforme ou s'il n'est pas utilisé conformément aux intentions initiales. Dans ce cas, la redirection USB générique peut être le seul moyen d'utiliser le périphérique. Les méthodes heuristiques permettent de déterminer quels périphériques sont des périphériques à images fixes standard.

Utilisez cette clé de registre pour configurer si les périphériques à images fixes standard sont automatiquement redirigés :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nom : AutoRedirectImage

Type : DWORD

Données : 00000000

La valeur par défaut est 0 (ne redirige pas automatiquement). En modifiant la valeur sur une valeur autre que zéro, les périphériques à images fixes USB standard sont redirigés à l'aide d'USB générique.

Vous pouvez aussi utiliser des stratégies Active Directory pour déployer cette valeur sur la clé de registre suivante et remplacer la valeur différente de la stratégie si les deux sont présentes :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nom : AutoRedirectImage

Type : DWORD

Données : 00000000

**Paramètres spécifiques au périphérique**

Les méthodes heuristiques utilisées pour sélectionner les périphériques optimisables Citrix ne correspondent pas toujours à ce que vous souhaitez. Les exemples de périphériques optimisables Citrix incluent les imprimantes, les périphériques audio, vidéo, de stockage et à images fixes. Il peut être utile de contrôler la redirection automatique des périphériques non répertoriés ci-dessus. Vous pouvez contrôler la redirection automatique en fonction du périphérique.

Par exemple, le lecteur de code à barres DemoTech 2 000 n'a pas besoin d'être redirigé via le support USB. Il a l'identifiant de fournisseur 12AB et l'identifiant de produit 5678. Ces nombres hexadécimaux se trouvent dans le Gestionnaire de périphériques.

Pour éviter la redirection automatique dans ce cas, créez cette clé de registre spécifique au périphérique :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Nom : AutoRedirect

Type : DWORD

Données : 00000000

Une valeur de 0 empêche le périphérique d'être automatiquement redirigé. Une valeur différente de zéro indique que le périphérique doit être pris en compte pour la redirection automatique (en fonction des préférences de l'utilisateur). Il y a un seul espace entre les identificateurs de fournisseur et de produit.

Vous pouvez également déployer cette valeur à l'aide de stratégies Active Directory sur cette clé de registre. Elle remplace la valeur différente de la stratégie si les deux sont présentes :

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Nom : AutoRedirect

Type : DWORD

Données : 00000000

Les paramètres AutoRedirect spécifiques à un périphérique ont priorité sur les valeurs plus générales AutoRedirectXXX expliquées ci-dessus. Les méthodes heuristiques par défaut pour les périphériques optimisés Citrix peuvent interpréter un périphérique comme générique par erreur. Par conséquent, définissez la valeur AutoRedirect spécifique à l'appareil sur 1 pour le rediriger automatiquement.

### Autoriser la connexion automatique des périphériques USB existants

Ce paramètre autorise ou empêche la connexion automatique des périphériques USB existants connectés au point de terminaison au début d'une session à la session distante.

Lorsque vous ajoutez ce paramètre à une stratégie, sélectionnez l'une des options suivantes :

- Demander avant de rediriger les périphériques USB disponibles.
- Ne pas rediriger automatiquement les périphériques USB disponibles.
- Rediriger automatiquement les périphériques USB disponibles.

Par défaut, l'option **Demander avant de rediriger les périphériques USB disponibles** est sélectionnée. En fonction de la stratégie sélectionnée, l'option sélectionnée dans la section **Préférences** > **Appareils** du client peut être remplacée.

> **Remarque :**
>
> Actuellement, la stratégie **Autoriser la connexion automatique des périphériques USB existants** s'applique uniquement à l'application Citrix Workspace pour Windows.

### Autoriser la connexion automatique des nouveaux périphériques USB

Ce paramètre autorise ou empêche la connexion automatique des périphériques USB insérés sur le point de terminaison pendant une session à la session distante.

Lorsque vous ajoutez ce paramètre à une stratégie, sélectionnez l'une des options suivantes :

- Demander avant de rediriger les périphériques USB disponibles.
- Ne pas rediriger automatiquement les périphériques USB disponibles.
- Rediriger automatiquement les périphériques USB disponibles.

Par défaut, l'option **Demander avant de rediriger les périphériques USB disponibles** est sélectionnée. En fonction de la stratégie sélectionnée, l'option sélectionnée dans la section **Préférences** > **Appareils** du client peut être remplacée.

> **Remarque :**
>
> Actuellement, la stratégie **Autoriser la connexion automatique des nouveaux périphériques USB** s'applique uniquement à l'application Citrix Workspace pour Windows.

### Règles de redirection de périphérique USB client (version 2)

Ce paramètre définit les règles de filtrage, de division et de connexion automatique des périphériques USB à une session distante.

Lorsque ce paramètre est sélectionné, l'hôte remplace le paramètre *Règles de redirection de périphérique USB client* par les règles du périphérique configurées dans ce paramètre.

Pour plus d'informations, consultez la section Configuration de la redirection de périphérique USB composite.

## Paramètres de stratégie de liste d'autorisation des canaux virtuels

June 28, 2024

Le paramètre de stratégie **Liste verte des canaux virtuels** permet l'utilisation d'une liste d'autorisation qui spécifie les canaux virtuels autorisés à être ouverts dans une session ICA.

Lorsque cette option est désactivée, tous les canaux virtuels sont autorisés.

Lorsque cette option est activée, seuls les canaux virtuels Citrix sont autorisés.

Pour utiliser des canaux virtuels personnalisés ou tiers, ajoutez les canaux virtuels à la liste. Pour ajouter un canal virtuel à la liste :

1. Entrez le nom du canal virtuel suivi d'une virgule.
2. Entrez le chemin d'accès au processus qui accède au canal virtuel.

D'autres chemins exécutables peuvent être répertoriés, et les chemins sont séparés par des virgules.

Par exemple,

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

À compter de Citrix Virtual Apps and Desktops 7 2109, les listes vertes des canaux virtuels sont activées par défaut. Pour plus d'informations sur l'ajout de canaux virtuels à la liste des canaux autorisés, voir Ajouter des canaux virtuels à la liste des canaux autorisés

Si vous utilisez HDX RealTime Optimization Pack pour Skype Entreprise, ajoutez le canal virtuel à la liste d'autorisation. Pour en savoir plus, consultez la documentation HDX RealTime Optimization Pack.

> **Important :**
>
> Les machines VDA doivent être redémarrées pour que le paramètre prenne effet.

Pour plus d'informations sur les canaux virtuels, consultez la section Canaux virtuels ICA.

### Journalisation de la liste d'autorisation des canaux virtuels

Vous pouvez utiliser ce paramètre de stratégie pour configurer le niveau de journalisation de la liste verte des canaux virtuels.

Les options suivantes sont disponibles :

| Options | Description |
| --- | --- |
| Désactivé | Désactive tous les événements du journal. |
| Avertissements de journal uniquement | Les événements sont enregistrés uniquement pour les canaux virtuels personnalisés qui tentent de s'ouvrir et ne figurent pas dans la liste verte. |
| Enregistrer tous les événements | Tous les événements sont enregistrés |

### Limitation des événements de la liste verte des canaux virtuels consignés dans le journal

Vous pouvez utiliser ce paramètre de stratégie pour configurer la fréquence de journalisation des événements d'une session active.

Tous les événements de chaque canal virtuel seront enregistrés lors de leur première occurrence. Les événements répétés seront supprimés pendant la durée de la période de limitation lorsque la session est active. Si une session est déconnectée, la période de limitation est réinitialisée.

## Paramètres de stratégie Affichage visuel

June 27, 2024

La section **Affichage visuel** contient des paramètres de stratégie permettant de contrôler la qualité des images envoyées depuis des bureaux virtuels vers la machine utilisateur.

### Nombre de couleurs préféré pour les graphiques simples

Ce paramètre de stratégie est disponible dans les versions VDA 7.6 FP3 et ultérieures. L'option 8 bits est disponible dans les versions VDA 7.12 et ultérieures.

Ce paramètre permet de réduire le nombre de couleurs à partir duquel les graphiques simples sont envoyés via le réseau. La réduction à 8 bits ou 16 bits par pixel améliore potentiellement le temps de réponse sur les connexions à faible bande passante. Cependant, cette action peut entraîner une légère dégradation de la qualité de l'image. Le nombre de couleurs 8 bits n'est pas pris en charge lorsque le paramètre de stratégie Utiliser codec vidéo pour la compression est réglé sur **Pour l'écran entier**.

Par défaut, le nombre de couleurs est de 24 bits par pixel.

Les VDA retournent au nombre de couleurs 24 bits (valeur par défaut) si le paramètre 8 bits est appliqué sur le VDA 7.11 et versions antérieures.

### Taux de trames cible

Ce paramètre spécifie le nombre maximal de trames par seconde envoyées depuis le bureau virtuel vers la machine utilisateur.

La valeur maximale par défaut est de 30 trames par seconde.

La définition d'un nombre élevé de trames par seconde (par exemple 30) améliore l'expérience utilisateur mais exige plus de bande passante. La réduction du nombre de trames par seconde (par exemple 10) augmente la capacité du serveur à monter en charge au détriment de l'expérience utilisateur. Pour les machines utilisateur possédant des UC plus lents, spécifiez une valeur inférieure pour améliorer l'expérience de l'utilisateur.

Le taux maximal pris en charge est 60 trames par seconde.

### Qualité visuelle

Ce paramètre spécifie la qualité visuelle désirée pour les images affichées sur la machine utilisateur.

Par défaut, cette option est définie sur Moyenne.

Pour spécifier la qualité des images, choisissez l'une des options suivantes :

- **Faible :** recommandé pour les réseaux à bande passante limitée où la qualité visuelle peut être sacrifiée pour une meilleure interactivité
- **Moyen :** offre les meilleures performances et une bande passante optimale dans la plupart des cas d'utilisation
- **Élevée :** recommandé si vous avez besoin de qualité d'image visuelle sans perte
- **Sans perte si possible :** envoie des images avec perte à la machine utilisateur durant les périodes de forte activité réseau et des images sans perte après réduction de l'activité réseau. Ce paramètre améliore les performances des connexions réseau avec une bande passante réduite.
- **Toujours sans perte :** lorsque la préservation des données d'images est vitale, sélectionnez **Toujours sans perte** pour vous assurer que les données avec perte ne sont jamais envoyées à la machine utilisateur. Par exemple, lors de l'affichage d'images radiographiques où aucune perte de qualité n'est acceptable.

## Paramètres de stratégie des images en mouvement

June 27, 2024

La section **Images en mouvement** contient des paramètres qui vous permettent de supprimer ou de modifier la compression des images dynamiques.

### Qualité d'image minimale

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre spécifie la qualité d'image minimale acceptable pour l'affichage adaptatif. La qualité des images est d'autant plus élevée que la compression est faible. Choisissez entre les valeurs de compression Ultra élevée, Très élevée, Élevée, Normale et Basse.

Par défaut, cette option est définie sur Normale.

### Compression d'images en mouvement

Ce paramètre spécifie si l'affichage adaptatif est activé ou non. L'affichage adaptatif ajuste automatiquement la qualité d'image des vidéos et des diapositives de transition des diaporamas en fonction de la bande passante disponible. Lorsque l'affichage adaptatif est activé, les utilisateurs doivent voir des présentations fluides sans réduction de qualité.

Par défaut, l'affichage adaptatif est activé.

Pour les versions VDA 7.0 à 7.6, ce paramètre s'applique uniquement lorsque le mode graphique d'ancienne génération est activé. Pour les versions VDA 7.6 FP1 et versions ultérieures, ce paramètre s'applique lorsque le mode graphique d'ancienne génération est activé, ou lorsque le mode graphique d'ancienne génération est désactivé et qu'aucun codec vidéo n'est utilisé pour compresser les graphiques.

Lorsque le mode graphique d'ancienne génération est activé, la session doit être redémarrée pour que les modifications prennent effet. L'affichage adaptatif et l'affichage progressif sont mutuellement exclusifs ; l'activation de l'affichage adaptatif désactive l'affichage progressif et vice versa. Il est cependant possible de désactiver l'affichage progressif et l'affichage adaptatif en même temps. L'utilisation de l'affichage progressif en tant que fonctionnalité d'ancienne génération n'est pas recommandée avec XenApp ou XenDesktop. La définition du niveau de seuil de l'affichage progressif désactive l'affichage adaptatif.

### Niveau de compression progressif

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre permet un affichage initial d'images moins détaillé, mais plus rapide.

Par défaut, la compression progressive n'est pas appliquée.

L'image plus détaillée définie par le paramètre de compression avec perte normale, s'affiche lorsqu'elle devient disponible. Utilisez une compression très élevée ou extrêmement élevée pour un affichage optimal des images à utilisation intensive de la bande passante, telles que des photographies.

Pour que la compression progressive soit efficace, son niveau de compression doit être supérieur à celui du paramètre Niveau de compression avec perte.

Remarque : le niveau amélioré de compression associé à la compression progressive optimise également l'interactivité des images dynamiques via les connexions clientes. La qualité d'une image dynamique, telle qu'un modèle pivotant à trois dimensions, est temporairement réduite jusqu'à ce que l'image devienne fixe, moment auquel le paramètre de compression avec perte normale est appliqué.

Les paramètres de stratégie suivants sont associés :

- Valeur de seuil de compression progressif
- Compression lourde progressive

### Valeur de seuil de compression progressif

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre représente la bande passante maximale, en kilobits par seconde, pour une connexion à laquelle la compression progressive est appliquée. Cela ne concerne que les connexions clientes liées à cette bande passante.

Par défaut, la valeur de seuil est de 2 147 483 647 kilobits par seconde.

Les paramètres de stratégie suivants sont associés :

- Valeur de seuil de compression progressif
- Compression lourde progressive

### Taux de trame minimum cible

Ce paramètre spécifie le taux de trame minimum par seconde que le système tente de conserver, des images dynamiques, dans des conditions de bande passante faible.

Par défaut, cette option est définie sur 10fps.

Pour les versions VDA 7.0 à 7.6, ce paramètre s'applique uniquement lorsque le mode graphique d'ancienne génération est activé. Pour les versions VDA 7.6 FP1 et versions ultérieures, ce paramètre s'applique lorsque le mode graphique d'ancienne génération est activé ou désactivé.

> **Remarque :**
>
> La stratégie Taux de trame minimum cible n'est plus prise en charge et est définie sur 10 images par seconde. Ce paramètre peut être modifié par les utilisateurs à l'aide du curseur Qualité de l'indicateur d'état des graphiques.

## Paramètres de stratégie Images immobiles

June 27, 2024

La section **Images immobiles** contient des paramètres qui vous permettent de supprimer ou de modifier la compression des images statiques.

### Compression de couleur supplémentaire

Ce paramètre active ou désactive l'utilisation d'une compression de couleur supplémentaire sur les images mises à disposition sur les connexions côté client qui sont limitées en bande passante, améliorant les temps de réponse en réduisant la qualité des images affichées.

Par défaut, la compression de couleur supplémentaire est désactivée.

Lorsqu'elle est activée, la compression de couleur supplémentaire est appliquée uniquement lorsque la bande passante de connexion cliente se trouve en dessous de la valeur du Seuil de compression de couleur supplémentaire. Lorsque la bande passante de connexion cliente se trouve en dessus de la valeur de seuil ou que Désactivé est sélectionné, la compression de couleur supplémentaire n'est pas appliquée.

### Seuil de compression de couleur supplémentaire

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre représente la bande passante maximale, en kilobits par seconde, pour une connexion en dessous de laquelle la compression de couleur supplémentaire est appliquée. Si la bande passante de connexion cliente tombe en dessous de la valeur définie, la compression de couleur supplémentaire, si activée, est appliquée.

Par défaut, la valeur de seuil est de 8 192 kilobits par seconde.

### Compression lourde

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre vous permet d'activer ou de désactiver la réduction de bande passante au-delà de la compression progressive sans perte de qualité d'image, en utilisant un algorithme graphique plus évolué, mais qui nécessite des ressources processeur importantes.

Par défaut, la compression intensive est désactivée.

Lorsqu'elle est activée, la compression intensive s'applique à tous les paramètres de compression avec perte. Elle est prise en charge sur application Citrix Workspace, mais n'a aucun effet sur les autres plug-ins.

Les paramètres de stratégie suivants sont associés :

- Niveau de compression progressif
- Valeur de seuil de compression progressif

### Niveau de compression avec perte

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre permet de contrôler le niveau de compression avec perte utilisé sur des images fournies sur des connexions clientes à bande passante limitée. Le cas échéant, l'affichage des images sans compression risque d'être ralenti.

Par défaut, la compression moyenne est sélectionnée.

Pour améliorer la réactivité avec des images à utilisation intensive de la bande passante, utilisez une compression élevée. Si la conservation des données d'images est un élément essentiel, par exemple lors de l'affichage de radiographies où la perte de qualité ne peut pas être tolérée, il est préférable de ne pas utiliser une compression avec perte.

Paramètre de stratégie connexe : valeur de seuil de compression avec perte

### Valeur de seuil de compression avec perte

Remarque : pour Virtual Delivery Agent 7.x, ce paramètre de stratégie s'applique uniquement lorsque le paramètre de stratégie du Mode graphique d'ancienne génération est activé.

Ce paramètre représente la bande passante maximale, en kilobits par seconde, pour une connexion à laquelle la compression avec perte est appliquée.

Par défaut, la valeur de seuil est de 2 147 483 647 kilobits par seconde.

L'ajout du paramètre Niveau de compression avec perte à une stratégie et l'inclusion d'un seuil non spécifié peut améliorer la vitesse d'affichage des bitmaps comprenant un nombre de détails élevés, tels que les photographies, dans un réseau local.

Paramètre de stratégie connexe : niveau de compression avec perte

## Paramètres de stratégie WebSockets

June 27, 2024

La section **WebSockets** contient des paramètres de stratégie pour accéder aux bureaux virtuels et aux applications hébergées avec l'application Citrix Workspace pour HTML5. La fonctionnalité WebSockets renforce la sécurité et réduit la charge en réalisant une communication bidirectionnelle entre les applications et les serveurs de navigateur. Elle n'ouvre pas plusieurs connexions HTTP.

### Connexions WebSockets

Ce paramètre autorise ou interdit les connexions WebSockets.

Par défaut, les connexions WebSockets sont interdites.

### Numéro de port WebSockets

Ce paramètre identifie le port pour les connexions WebSockets entrantes.

Par défaut, la valeur est 8008.

### Liste des serveurs d'origine approuvés WebSockets

Ce paramètre fournit une liste séparée par des virgules des serveurs d'origine de confiance, habituellement l'application Citrix Workspace pour Web, exprimée sous la forme d'adresses URL. Le serveur accepte uniquement les connexions WebSockets provenant de l'une de ces adresses.

Par défaut, des caractères génériques sont utilisés pour faire confiance à toutes les adresses URL de l'application Citrix Workspace pour Web.

Si vous choisissez d'entrer une adresse dans la liste, utilisez la syntaxe suivante :

<protocole>://<Nom de domaine complet de l'ordinateur hôte>:[port]

Le protocole doit être HTTP ou HTTPS. Si le port n'est pas spécifié, le port 80 pour HTTP et le port 443 est utilisé pour HTTPS.

Le caractère générique `*` peut être utilisé dans l'adresse URL, sauf dans le cadre d'une adresse IP (`10.105.*.*`).

## Paramètres de stratégie des périphériques WIA

June 27, 2024

La section **Périphériques WIA** contient des paramètres de stratégie pour gérer la redirection de scanner à l'aide de l'acquisition d'images Windows (WIA).

### Redirection WIA

Les périphériques WIA, tels que les appareils photo numériques et les scanners, communiquent avec les applications de traitement d'images hébergées sur le serveur à l'aide de la structure WIA.

Ce paramètre permet ou interdit aux utilisateurs d'accéder aux périphériques WIA sur la machine utilisateur. Par défaut, la redirection WIA est interdite.

Pour plus d'informations sur les périphériques compatibles WIA, reportez-vous à Périphériques WIA.

## Fonctions HDX gérées via le registre

June 27, 2024

> **Remarque :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Pour ouvrir l'Éditeur du Registre, exécutez `regedit.exe` sur le serveur. Accédez ensuite à la clé de Registre pour ajouter ou modifier les paramètres.

### Appareils

#### Claviers Bloomberg

Citrix Virtual Apps and Desktops prend en charge les modèles de clavier Starboard 3 et 4 de Bloomberg. Par défaut, la prise en charge du clavier Bloomberg amélioré est désactivée.

Pour activer la prise en charge du clavier Bloomberg, définissez la valeur de Registre suivante sur l'ordinateur client avant de démarrer une connexion :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **Nom de la valeur** : `EnableBloombergHID`
- **Type de valeur** : `DWORD`
- **Données de valeur** :
  - `0` - Désactiver
  - `1` - Activer

Pour plus d'informations, consultez la section Clavier Bloomberg.

#### Lecteurs clients mappés

Par mesure de sécurité, lorsqu'un utilisateur ouvre une session sur Citrix Virtual Apps and Desktops, par défaut, le serveur mappe les lecteurs clients sans autorisation d'exécution de l'utilisateur. Pour permettre aux utilisateurs d'exécuter des fichiers exécutables résidant sur des lecteurs clients mappés, remplacez cette valeur par défaut en modifiant le registre sur le serveur.

Pour autoriser l'accès, modifiez la valeur de registre suivante (créez **CDMSettings** si elle n'existe pas) :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- **Nom de la valeur** : `ExecuteFromMappedDrive`
- **Type de valeur** : `DWORD`
- **Données de valeur** :
  - `1` - Autoriser l'autorisation
  - `0` - Refuser l'autorisation sur les lecteurs mappés

La modification prend effet avec les sessions connectées après la modification du registre.

Citrix Virtual Apps and Desktops 7 2006 est la première version à contenir cet emplacement de registre. Les versions antérieures de Citrix Virtual Apps and Desktops utilisaient un emplacement de registre différent.

Pour plus d'informations, consultez la section Mappage des lecteurs clients.

#### Stylets Microsoft Surface Pro et Surface Book

Citrix Virtual Apps and Desktops prend en charge la fonctionnalité de stylet standard avec les applications Windows Ink. Cette fonctionnalité est activée par défaut.

Pour désactiver ou activer cette fonctionnalité, définissez la valeur de registre suivant :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **Nom de la valeur** : `DisablePen`
- **Type de valeur** : `DWORD`
- **Données de valeur** :
  - `1` - Désactiver
  - `0` - Activer

Pour plus d'informations, consultez Stylets Microsoft Surface Pro et Surface Book.

#### Liste d'autorisation d'applications Acquisition d'image Windows

Ce paramètre vous permet de contrôler quelles applications du VDA peuvent accéder à la redirection du scanner d'acquisition d'images Windows.

Par défaut, aucune application n'a accès à l'acquisition d'image Windows.

Pour ajuster l'acquisition d'image Windows pour les applications du VDA, créez le paramètre de Registre suivant :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- **Nom de la valeur** : `WIAAllowedProcesses`

  Sélectionnez et cliquez avec le bouton droit sur **WIAAllowedProcesses**. Choisissez **Nouveau > Valeur de chaînes multiples** et renommez la nouvelle valeur en **AllowProcesses**.
- Données de valeur : entrez le chemin complet et le nom du processus pour chaque application pouvant accéder à l'acquisition d'image Windows. Indiquez chaque application sur une nouvelle ligne.

Toutes les modifications apportées à ce paramètre prennent effet lors du prochain lancement d'une session sur le VDA.

### General

#### Réducteur HDX

Vous pouvez configurer la version de l'algorithme de compression HDX (Reducer) que vous souhaitez utiliser dans l'hôte de session.

Pour activer Reducer V4 dans un VDA mono-session, définissez la valeur de registre suivante :

**Clé :** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings`

**Nom de la valeur :** `ReducerOverrideMask`
**Type de valeur :** `DWORD`
**Données de valeur :** 23 (Décimal)

Pour activer Reducer V4 dans un VDA multi-session, définissez la valeur de registre suivante :

- **Clé** : `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **Nom de la valeur** : `ReducerOverrideMask`
- **Type de valeur** : `DWORD`
- **Données de valeur** : 23 (décimal)

#### Configurer le délai d'expiration EDT

Vous pouvez configurer le délai d'expiration EDT sur n'importe quelle valeur comprise entre 5 et 25 secondes sur le VDA. La valeur du délai EDT par défaut est de 25 secondes.

- **Clé** : `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters`
- **Type de valeur** : `DWORD`
- **Nom de la valeur** : `edtConnectionTimeout`
- **Données de valeur** : durée en secondes comprise entre 5 et 25 (décimal)

Vous pouvez également configurer le délai d'expiration de l'application Citrix Workspace pour Windows :

- **Clé** : `HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT`
- **Type de valeur** : `String / REG_SZ`
- **Nom de la valeur** : `edtConnectionTimeout`
- **Données de valeur** : durée en secondes comprise entre 5 et 25 (décimal)

#### Configurer la version de Rendezvous

Pour configurer la version de Rendezvous à utiliser, définissez la valeur de registre suivante :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- **Type de valeur** : `DWORD`
- **Nom de la valeur** : `GctRegistration`
- **Données de valeur** :
  - `1` - Pour activer la V2
  - `0` - Pour activer la V1

#### Configurer l'ouverture de session automatique sur le VDA

Ce paramètre vous permet d'activer ou de désactiver le paramètre de stratégie Microsoft **Toujours demander un mot de passe** sur les VDA avec OS mono-session et multisession Windows 10.

Si **Toujours demander un mot de passe** est activé, les utilisateurs doivent entrer des informations d'identification sur le VDA lorsqu'ils démarrent une session distante. Si ce paramètre est désactivé, les utilisateurs se connectent automatiquement à la session distante sans fournir d'informations d'identification sur le VDA.

Par défaut, le paramètre de stratégie Microsoft est désactivé. Pour activer ou désactiver le paramètre **Toujours demander un mot de passe**, définissez la valeur de Registre suivante sur le VDA :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica`
- **Nom de la valeur** : `AutoLogon`
- **Type de valeur** : `DWORD`
- **Données de valeur** :
  - `1` - Désactive le paramètre de stratégie Microsoft et permet aux utilisateurs de se connecter automatiquement à une session à distance.
  - `0` - Active le paramètre de stratégie Microsoft et invite les utilisateurs à fournir des informations d'identification lorsqu'ils lancent une session à distance.

#### Désactiver l'avertissement d'expiration

Par défaut, les utilisateurs avec des sessions inactives reçoivent un message d'avertissement deux minutes avant que leur session se déconnecte automatiquement.

Ce paramètre désactive et supprime le message d'avertissement pour les utilisateurs atteignant la limite du délai d'expiration de session inactive sur les systèmes suivants :

- Windows Server 2004
- OS multi-session Windows 10 2004 ou version ultérieure

Pour supprimer l'avertissement, définissez la valeur de Registre suivante sur le VDA :

- **Clé** : `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP`
- **Nom de la valeur** : `fEnableTimeoutWarning`
- **Type de valeur** : `DWORD`
- **Données de valeur** :
  - `1` - Désactiver le message d'avertissement
  - `0` - Activer le message d'avertissement

Pour afficher le message d'avertissement, supprimez la valeur du Registre ou définissez la valeur sur `0`.

#### Découverte MTU EDT

La découverte MTU permet à EDT de déterminer automatiquement l'unité de transmission maximale (MTU) lors de l'établissement d'une session. Cela empêche la fragmentation des paquets EDT, qui pourrait entraîner une dégradation des performances ou l'échec de l'établissement d'une session.

Ce paramètre est activé par défaut. Pour désactiver la découverte MTU EDT, configurez la valeur de registre suivante et redémarrez le VDA.

- **Clé** : `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **Nom de la valeur** : `MtuDiscovery`
- **Type de valeur** : `DWORD`
- **Données de valeur** : `0`

Ce paramètre s'applique à l'échelle de la machine et affecte toutes les sessions se connectant à partir d'un client pris en charge.

#### Activer le mode de tolérance aux pertes

Vous pouvez accéder à l'audio adaptatif à l'aide du mode de tolérance aux pertes pour le service audio bidirectionnel pour l'application Citrix Workspace pour Windows, VDA multi-utilisateur et VDA de bureau. Cette option est désactivée par défaut. Pour activer le mode de tolérance aux pertes, configurez la valeur de registre suivante en fonction de la machine que vous utilisez et redémarrez la machine correspondante.

Pour le client de l'application Citrix Workspace pour Windows,

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **Nom de la valeur** : `EdtUnreliableAllowed`
- **Type de valeur** : `REG_SZ`
- **Données de valeur** : `1`

Pour VDA TS,

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio`
- **Nom de la valeur** : `EdtUnreliableAllowed`
- **Type de valeur** : `DWORD`
- **Données de valeur** : `1`

Pour VDA WS,

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio`
- **Nom de la valeur** : `EdtUnreliableAllowed`
- **Type de valeur** : `DWORD`
- **Données de valeur** : `1`

## Redirection de contenu générale

### Ajout de types d'URL pour la redirection hôte vers client

Par défaut, nous prenons en charge la redirection des types d'URL suivants : HTTP, HTTPS, RTSP, RTSPU, PNM et MMS. Vous pouvez ajouter des types d'URL à la liste en créant les clés de registre et les valeurs suivantes sur le client Windows.

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA`
- **Nom de la valeur** : `ExtraURLProtocols`
- **Type de valeur** : `REG_SZ`
- **Données de valeur** : spécifiez les types d'URL requis séparés par un point-virgule. Incluez tout ce qui se trouve avant la partie autorité de l'URL. Par exemple : `ftp://;mailto:;customtype1://;custometype2://`

Vous pouvez ajouter des types d'URL uniquement pour les clients Windows. Les clients ne disposant pas de ce paramètre de registre rejettent la redirection vers la session Citrix. Une application doit être installée et configurée chez le client pour gérer les types d'URL spécifiés.

Pour plus d'informations, voir Redirection hôte vers client.

### Redirection de dossiers clients

La redirection de dossiers clients modifie la manière dont les fichiers côté client sont accessibles sur la session côté hôte. Supposons que vous activez la redirection de dossiers clients sur le serveur et que l'utilisateur la configure sur la machine utilisateur. Dans ce cas, la partie du volume local spécifiée par l'utilisateur est redirigée.

Pour activer la redirection de dossiers clients sur le serveur, définissez la valeur de Registre suivante :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`
- **Nom de la valeur** : `CFROnlyModeAvailable`
- **Type de valeur** : `DWORD`
- **Données de valeur** : `1`

Pour plus d'informations, consultez la section Redirection des dossiers clients.

#### Redirection hôte vers client pour un ensemble spécifique de sites Web

Pour activer la redirection hôte vers client pour un ensemble spécifique de sites Web, définissez la valeur de registre suivante sur le VDA de serveur.

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **Nom de la valeur** : `ValidSites`
- **Type de valeur** : `REG_MULTI_SZ`
- **Données de valeur** : spécifiez toute combinaison de noms de domaine complet (FQDN). Tapez les noms de domaine complet sur des lignes distinctes. N'incluez que le nom de domaine complet, sans protocoles (`http://` ou `https://`). Un nom de domaine complet peut inclure un astérisque (`*`) en tant que caractère générique dans la position la plus à gauche uniquement. Ce caractère générique correspond à un seul niveau de domaine, ce qui est compatible avec les règles définies dans RFC 6125. Par exemple :

```
www.example.com
```

```
*.example.com
```

Pour plus d'informations, voir Redirection hôte vers client.

#### Comportement de l'application locale lors de la fermeture de session et de la déconnexion

Par défaut, les applications locales continuent de s'exécuter lorsqu'un utilisateur ferme sa session ou se déconnecte de l'ordinateur virtuel. Après la reconnexion, les applications locales sont réintégrées si elles sont disponibles dans le bureau virtuel. Pour configurer le comportement des applications locales lors de la fermeture de session et de la déconnexion, définissez la valeur de Registre suivante dans le bureau hébergé :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **Nom de la valeur** : `Session State`
- **Type de valeur** : `DWORD`
- **Données de valeur** :
  - `1` : les applications locales continuent de s'exécuter lorsqu'un utilisateur ferme sa session ou se déconnecte du bureau virtuel. Lors de la reconnexion, les applications locales sont réintégrées si elles sont disponibles dans le bureau virtuel.
  - `3` : les applications locales se ferment lorsqu'un utilisateur ferme sa session ou se déconnecte du bureau virtuel.

Pour plus d'informations, voir Local App Access et redirection d'adresse URL.

#### Supprimer les types d'URL de la liste par défaut pour la redirection hôte vers client

Pour supprimer des types d'URL de la liste de redirection par défaut, créez les clés de registre et les valeurs suivantes sur le VDA du serveur.

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA`
- **Nom de la valeur** : `DisableServerFTA`
- **Type de valeur** : `DWORD`
- **Données de valeur** : `1`
- **Nom de la valeur** : `NoRedirectClasses`
- **Type de valeur** : `REG_MULTI_SZ`
- **Données de valeur** : spécifiez n'importe quelle combinaison de valeurs : `http`, `https`, `rtsp`, `rtspu`, `pnm` ou `mms`. Tapez les valeurs multiples sur des lignes distinctes. Par exemple :

```
http
https
rtsp
```

Pour plus d'informations, voir Redirection hôte vers client.

#### Configuration du navigateur par défaut du VDA serveur

Vous pouvez activer la redirection hôte vers client pour remplacer n'importe quelle configuration de navigateur par défaut sur le VDA serveur. Si une URL Web n'est pas redirigée, Citrix Launcher transmet l'URL au navigateur configuré dans la clé de registre `command_backup`. La clé pointe vers Internet Explorer par défaut, mais vous pouvez la modifier pour inclure le chemin d'accès à un autre navigateur.

- Internet Explorer (par défaut)
  - **Clé** : `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Nom de la valeur** : `Default`
  - **Type de valeur** : `REG_SZ`
  - **Données de valeur** : `"c:\program files\internet explorer\iexplore.exe""%1"`
  - **Clé** : `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Nom de la valeur** : `Default`

  - **Type de valeur** : `REG_SZ`
  - **Données de valeur** : `"c:\program files\internet explorer\iexplore.exe""%1"`

- Google Chrome
  - **Clé** : `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Nom de la valeur** : `Default`
  - **Type de valeur** : `REG_SZ`
  - **Données de valeur** : `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"`
  - **Clé** : `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Nom de la valeur** : `Default`
  - **Type de valeur** : `REG_SZ`
  - **Données de valeur** : `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"`

- Microsoft Edge
  - **Clé** : `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Nom de la valeur** : `Default`
  - **Type de valeur** : `REG_SZ`
  - **Données de valeur** : `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"`
  - **Clé** : `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Nom de la valeur** : `Default`
  - **Type de valeur** : `REG_SZ`
  - **Données de valeur** : `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"`

#### Local App Access pour les applications publiées

Local App Access s'intègre en toute transparence aux applications Windows installées localement dans un environnement de bureau hébergé sans passer d'un bureau à l'autre. Pour fournir un accès aux applications publiées, définissez la valeur de Registre suivante sur le serveur :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`
- **Nom de la valeur** : `ClientHostedAppsEnabled`
- **Type de valeur** : `DWORD`
- **Données de valeur** :
  - `1` - Activer
  - `0` - Désactiver

Pour plus d'informations, voir Local App Access et redirection d'adresse URL.

### Graphiques

#### Accélération de processeur graphique pour les applications CUDA ou OpenCL

L'accélération GPU d'applications CUDA et OpenCL exécutées dans une session utilisateur est désactivée par défaut.

Pour utiliser les fonctionnalités d'évaluation d'accélération CUDA, activez le paramètre de Registre suivant :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **Nom de la valeur** : `CUDA`
- **Type de valeur** : `DWORD`
- **Données de valeur** : `00000001`

Pour utiliser les fonctionnalités d'évaluation d'accélération OpenCL, activez le paramètre de Registre suivant :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper`
- **Nom de la valeur** : `OpenCL`
- **Type de valeur** : `DWORD`
- **Données de valeur** : `00000001`

Pour de plus amples informations, consultez la section Accélération GPU pour OS multi-session Windows.

#### Mode progressif

Le mode progressif est désactivé par défaut. Vous pouvez changer l'état du mode progressif avec la valeur de registre suivante :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics`
- **Type de valeur** : `REG_DWORD`
- **Nom de la valeur** : `ProgressiveDisplay`
- **Données de valeur** :
  - `0` = Toujours désactivé (Désactive le mode progressif. Cette valeur est la valeur par défaut.)
  - `1` = Automatique (Bascule en fonction des conditions du réseau).
  - `2` = Toujours activé

Pour plus d'informations, consultez la section Mode progressif.

> **Remarque :**
>
> Le mode progressif est obsolète. Thinwire est une alternative qui optimise la diffusion des images et maintient l'efficacité du cache tout en offrant presque tous les avantages du mode progressif.

#### Rendu Windows Presentation Foundation (WPF)

HDX 3D Pro permet aux applications exigeantes en ressources graphiques exécutées dans de sessions d'OS multi-session Windows d'être restituées sur le processeur graphique du serveur (GPU). En déplaçant la restitution Windows Presentation Foundation (WPF) sur le processeur graphique du serveur, l'unité centrale du serveur n'est pas ralentie par la restitution des graphiques.

Pour activer la restitution des applications WPF à l'aide du GPU du serveur, créez les paramètres suivants dans le registre du serveur exécutant un OS multi-session Windows :

1. Ouvrez l'Éditeur du Registre sur le VDA et accédez à la clé suivante :

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. Créez ou modifiez les valeurs de registre suivantes :

   - [REG_DWORD] AdapterHandle = 0x00000001
   - [REG_DWORD] DevicePath = 0x00000001
   - [REG_DWORD] Flag = 0x00000412
   - [REG_DWORD] WPF = 0x00000001

3. Créez une sous-clé avec le nom exécutable de votre application WPF. Par exemple, si votre application s'appelle « mywpfapp.exe », créez la clé suivante :

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe`

4. Redémarrez le serveur pour que le paramètre soit pris en compte.

Pour plus d'informations, consultez Accélération GPU pour OS multi-session Windows et le blog sur Tirer le meilleur parti des applications WPF sur OS multisession Windows.

## Multimédia

### Éviter l'écho pendant les conférences multimédia

Citrix Virtual Apps and Desktops fournit une option d'annulation d'écho qui minimise tout écho. Cette fonctionnalité est activée par défaut. Pour désactiver l'annulation d'écho, vous pouvez modifier l'un des paramètres de Registre suivants :

- **Clé** :
  - 32 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
  - 64 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **Nom de la valeur** : `EchoCancellation`
- **Type de valeur** : `String`/`REG_SZ`
- **Données de valeur** : `False`

Pour plus d'informations, consultez la section Fonctionnalités audio.

### Limitation audio

Après avoir installé un périphérique audio sur votre client, activé la redirection audio et démarré une session RDS, les fichiers audio peuvent ne pas lire l'audio. Pour résoudre ce problème, ajoutez la clé de Registre suivante sur la machine RDS, puis redémarrez la machine :

- **Clé** : `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig`
- **Nom de la valeur** : `EnableSvchostMitigationPolicy`
- **Type de valeur** : `DWORD`
- **Données de valeur** : `0`

Pour plus d'informations, consultez la section Fonctionnalités audio.

### Redirection du contenu du navigateur et DPI

Lorsque vous utilisez la redirection de contenu du navigateur avec la mise à l'échelle DPI définie sur une valeur supérieure à 100 % sur la machine de l'utilisateur, l'écran de contenu du navigateur redirigé s'affiche de manière incorrecte. Pour éviter ce problème, désactivez l'accélération GPU de redirection de contenu du navigateur pour Chrome en créant la valeur de Registre suivante sur l'ordinateur de l'utilisateur :

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream`

- **Nom de la valeur** : `GPU`
- **Type de valeur** : `DWORD`
- **Données de valeur** : `0`

Pour plus d'informations, consultez la section Redirection du contenu du navigateur et DPI.

#### Résolution de webcam haute définition

Si la négociation du type de média échoue, HDX revient à la résolution VGA par défaut (640 x 480 pixels). Vous pouvez utiliser des clés de Registre sur le client pour configurer la résolution par défaut. Avant de définir les clés de Registre suivantes, assurez-vous que la caméra prend en charge la résolution spécifiée.

- **Clé** : `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- Largeur
  - **Nom de la valeur** : `DefaultWidth`
  - **Type de valeur** : `DWORD`
  - **Données de valeur** : largeur désirée en décimal (par exemple 1280)
- Hauteur
  - **Nom de la valeur** : `DefaultHeight`
  - **Type de valeur** : `DWORD`
  - **Données de valeur** : hauteur désirée en décimal (par exemple 720)

#### Mode de secours Microsoft Teams

Si Microsoft Teams ne parvient pas à se charger en mode VDI optimisé ("Citrix HDX non connecté" dans Teams/À propos de/Version), le VDA revient aux technologies HDX héritées comme la redirection de Webcam et la redirection de l'audio et du microphone client. Si vous utilisez un système d'exploitation ou une version d'application Workspace qui ne prend pas en charge l'optimisation Microsoft Teams, les clés de Registre de secours ne s'appliquent pas.

Pour contrôler le mécanisme de secours, définissez l'une des valeurs de Registre suivantes sur le VDA :

- **Clé** (une seule clé est nécessaire) :
  - **Paramètre ordinateur** `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams` :
  - **Paramètre utilisateur** `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams` :
- **Nom de la valeur** : `DisableFallback`

- **Type de valeur** : DWORD
- Données de valeur :
  - 1 - Désactiver le mode de secours
  - 2 - Activer uniquement le son

Si la valeur n'est pas présente ou est définie sur 0, le mode de secours est activé. Cette fonctionnalité requiert l'utilisation de Microsoft Teams version 1.3.0.13565 ou ultérieure. Pour plus d'informations, consultez Optimisation pour Microsoft Teams.

#### Optimisation pour Microsoft Teams avec Citrix App Layering

Si vous utilisez Citrix App Layering pour gérer les installations de VDA et de Microsoft Teams dans différentes couches, créez une clé de registre vide nommée **PortICA** sous Windows avant d'installer Microsoft Teams avec l'indicateur ALLUSER=1 de la ligne de commande. Conservez le type, les données et le nom de la valeur par défaut.

- Clé pour la version 32 bits de l'Éditeur du Registre : HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA
- Clé pour la version 64 bits de l'Éditeur du Registre : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

Pour plus d'informations, consultez Optimisation pour Microsoft Teams.

#### Authentification unique avec authentification Windows intégrée pour la redirection de contenu du navigateur

Ce paramètre fournit une authentification unique à un serveur Web configuré avec l'authentification Windows intégrée (IWA) dans le même domaine que le VDA. Pour activer l'authentification unique, définissez la valeur de Registre suivante sur 1 :

- **Clé** :
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

  ou
  - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream
- **Nom de la valeur** : WebBrowserRedirectionIwaSupport
- **Type de valeur** : DWORD
- **Données de valeur** : 1

Pour plus d'informations, consultez la section Authentification unique avec authentification Windows intégrée.

#### En-tête de requête agent-utilisateur

L'en-tête agent-utilisateur permet d'identifier les requêtes HTTP envoyées à partir de la redirection du contenu du navigateur. Ce paramètre peut être utile lorsque vous configurez des règles de proxy et de pare-feu. Par exemple, si le serveur bloque les requêtes envoyées à partir de la redirection du contenu du navigateur, vous pouvez créer une règle contenant l'en-tête agent-utilisateur pour contourner certaines exigences. Seuls les périphériques Windows prennent en charge l'en-tête de requête agent-utilisateur.

Par défaut, la chaîne d'en-tête de requête agent-utilisateur est désactivée. Pour activer l'en-tête agent-utilisateur pour le contenu rendu par le client, utilisez l'éditeur du Registre.

Sur chaque application Citrix Workspace pour clients Windows, définissez un des paramètres de registre suivants :

- **Clé** :
  - 32 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream`
  - 64 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream`

- **Nom de la valeur** : `EnableCefUserAgentString`
- **Type de valeur** : `DWORD`
- **Données de valeur** : 1

Après avoir ajouté la valeur de Registre, l'en-tête agent-utilisateur contient le texte CitrixBCR/2102.1, où 2102.1 est la version de l'application Citrix Workspace pour Windows.

#### Compression logicielle webcam

Si une webcam prend en charge le codage matériel, la compression vidéo HDX utilise le codage matériel par défaut. Le codage matériel peut consommer plus de bande passante que le logiciel de codage. Pour forcer la compression logicielle, ajoutez les valeurs suivantes sur le client :

- **Clé** : `HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime`
- **Nom de la valeur** : `DeepCompress_ForceSWEncode`
- **Type de valeur** : `DWORD`
- **Données de valeur** : 1

Pour plus d'informations, consultez la section Compression vidéo de webcam HDX.

#### Compression vidéo de webcam

La compression vidéo de webcam HDX envoie la vidéo H.264 directement à l'application de visioconférence exécutée dans la session virtuelle. Pour optimiser les ressources VDA, la compression de webcam HDX n'effectue pas de codage, de transcodage ni de décodage de la vidéo webcam. Cette fonctionnalité est activée par défaut.

Pour désactiver la diffusion vidéo directe du serveur vers l'application de visioconférence, définissez la valeur de Registre suivante sur le VDA.

- **Clé** : `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime`
- **Nom de la valeur** : `OfferH264ToApp`
- **Type de valeur** : `DWORD`
- **Données de valeur** : `0`

Pour plus d'informations, consultez la section Compression vidéo de webcam HDX.

#### Fréquence d'images de compression vidéo webcam

Pour ajuster la fréquence d'images vidéo préférée, modifiez la valeur de Registre suivante sur le client :

- **Clé** : `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime`
- **Nom de la valeur** : `FramesPerSecond`
- **Type de valeur** : `DWORD`
- **Données de valeur** : `15`

Si la webcam ne prend pas en charge la fréquence d'images spécifiée, l'application utilise 15 IPS par défaut.

Pour plus d'informations, consultez la section Compression vidéo de webcam HDX.

## Paramètres de stratégie Gestion de la charge

June 27, 2024

La section **Gestion de la charge** contient des paramètres de stratégie pour l'activation et la configuration de la gestion de la charge entre les serveurs mettant à disposition des machines avec OS multi-session Windows.

Pour de plus amples informations sur le calcul de l'index de calculateur de charge, consultez l'article CTX202150.

### Tolérance d'ouvertures de session simultanée

Ce paramètre spécifie le nombre maximal d'ouvertures de session simultanées qu'un serveur peut accepter.

Par défaut, cette option est définie sur 2.

Lorsque ce paramètre est activé, l'équilibrage de charge fait en sorte de ne pas dépasser le nombre spécifié d'ouvertures de session actives en même temps sur un VDA serveur. Toutefois, la limite n'est pas strictement appliquée. Pour appliquer la limite (et entraîner l'échec des ouvertures de session simultanées qui dépassent le nombre spécifié), créez la clé de registre suivante :

> HKLM\Software\Citrix\DesktopServer\LogonToleranceIsHardLimit
> Type : DWORD
> Valeur : 1

### Utilisation du processeur

Ce paramètre spécifie le niveau d'utilisation de l'UC, sous la forme d'un pourcentage, à laquelle le serveur signale une pleine charge. Lorsque cette option est activée, la valeur par défaut à laquelle le serveur signale une pleine charge est 90%.

Par défaut, ce paramètre est désactivé et l'utilisation de l'UC est exclue du calcul de la charge.

### Priorité de processus exclue de l'utilisation UC

> **Remarque :**
>
> Dans les scénarios où les machines sont gérées par Workspace Environment Management, l'utilisation de ce paramètre ainsi que les paramètres Priorité UC peut avoir des résultats inattendus. Nous vous recommandons de désactiver ce paramètre si vous choisissez d'utiliser les paramètres de priorité de l'UC.

Ce paramètre spécifie le niveau de priorité auquel l'utilisation de l'UC est exclue de l'index de charge de l'utilisation de l'UC.

Par défaut, cette option est définie sur **Inférieure à la normale** ou **Basse**.

### Utilisation du disque

Ce paramètre spécifie la longueur de la file d'attente à laquelle le serveur signale une pleine charge 75%. Lorsque cette option est activée, la valeur par défaut de file d'attente du disque est de 8.

Par défaut, ce paramètre est désactivé et l'utilisation du disque est exclue du calcul des charges.

### Nombre maximum de sessions

Ce paramètre spécifie le nombre maximal de sessions qu'un serveur peut héberger. Lorsqu'il est activé, le paramètre par défaut pour le nombre maximal de sessions qu'un serveur peut héberger est 250.

Ce paramètre est activé par défaut.

### Utilisation de la mémoire

Ce paramètre spécifie le niveau d'utilisation de la mémoire, sous la forme d'un pourcentage, à laquelle le serveur signale une pleine charge. Lorsque cette option est activée, la valeur par défaut à laquelle le serveur signale une pleine charge est 90%.

Par défaut, ce paramètre est désactivé et l'utilisation de mémoire est exclue du calcul de la charge.

### Charge de base d'utilisation mémoire

Ce paramètre spécifie une approximation de l'utilisation de la mémoire du système d'exploitation de base. Définit également, en Mo, l'utilisation de la mémoire en dessous de laquelle un serveur est considéré comme ayant une charge nulle.

Par défaut, cette option est définie sur 768 Mo.

## Paramètres de stratégie Profile Management

June 27, 2024

Cette section contient les paramètres de stratégie permettant d'activer et de configurer Profile Management.

Pour d'autres informations, telles que les suivantes, consultez la section Stratégies Profile Management :

- Noms du paramètre de fichier .ini équivalent
- Quelle version de Profile Management est requise pour un paramètre de stratégie

## Paramètres de stratégie Avancés

June 27, 2024

### Nombre de tentatives d'accès à des fichiers verrouillés

Définit le nombre de tentatives d'accès à des fichiers verrouillés.

Si cette stratégie est désactivée, la valeur par défaut (5 tentatives) est utilisée. Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, la valeur par défaut est utilisée.

### Traiter les cookies Internet à la fermeture de session

Certains déploiements engendrent des cookies Internet supplémentaires qui ne sont pas référencés par le fichier `Index.dat`. Ces cookies laissés sur le système de fichiers après une navigation intensive peuvent entraîner la saturation du profil. Cette stratégie vous permet d'activer Profile Management pour forcer le traitement du fichier Index.dat et supprimer les cookies supplémentaires. Étant donné que cette stratégie augmente la durée de la fermeture de session, ne l'activez que si vous rencontrez ce problème.

Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, Index.dat n'est pas traité.

### Désactiver la configuration automatique

Profile Management examine maintenant tout environnement Citrix Virtual Desktops, pour détecter par exemple la présence de Personal vDisks, et configure la stratégie de groupe en conséquence. Seules les stratégies Profile Management dont l'état est Non configuré sont modifiées, de sorte que toutes les personnalisations que vous avez effectuées sont conservées.

Cette stratégie vous permet d'accélérer le déploiement et de simplifier l'optimisation. Il n'est pas nécessaire de configurer cette stratégie. Toutefois, vous pouvez désactiver la configuration automatique lorsque vous effectuez l'une des opérations suivantes :

- Mise à niveau pour conserver les paramètres des versions antérieures
- Dépannage

Vous pouvez considérer la configuration automatique en tant qu'outil d'analyse de la configuration dynamique qui configure automatiquement les paramètres de stratégie par défaut en fonction des environnements lors de l'exécution. Cela élimine le besoin de configurer les paramètres manuellement. Les environnements d'exécution comprennent :

- Système d'exploitation Windows
- Versions du système d'exploitation Windows
- Présence de Citrix Virtual Desktops

- Présence de Personal vDisks

La configuration automatique peut modifier les stratégies suivantes si l'environnement change :

- Réécriture active
- Toujours mettre en cache
- Supprimer les profils mis en cache localement à la fermeture de session
- Délai avant la suppression des profils mis en cache
- Streaming des profils

Consultez le tableau suivant pour connaître le statut par défaut des stratégies sur différents systèmes d'exploitation :

| | OS multi-session | OS mono-session |
|---|---|---|
| Réécriture active | Activé | *Désactivé* si Personal vDisk est utilisé ; sinon, Activé. |
| Toujours mettre en cache | Désactivé | *Désactivé* si Personal vDisk est utilisé ; sinon, Activé. |
| Supprimer les profils mis en cache localement à la fermeture de session | Activé | *Désactivé* si l'une des situations suivantes se produit : si Personal vDisk est utilisé ou si Citrix Virtual Desktops est attribué ou si Citrix Virtual Desktops n'est pas installé ; sinon, activé. |
| Délai avant la suppression des profils mis en cache | 0 seconde | 60 secondes si les modifications de l'utilisateur ne sont pas persistantes ; sinon, 0 seconde. |
| Streaming des profils | Activé | *Désactivé* si Personal vDisk est utilisé ; sinon, Activé. |

Toutefois, si la configuration automatique est désactivée, toutes les stratégies ci-dessus sont **désactivées** par défaut.

> **Important :**
>
> Personal vDisk est obsolète. Pour de plus amples informations, consultez la section Suppression de PvD, AppDisks et d'hôtes non pris en charge.

À partir de Profile Management 1909, vous pouvez bénéficier d'une expérience améliorée avec le menu Démarrer sous Windows 10 (version 1607 et ultérieure) et Windows Server 2016 et versions ultérieures. Cette amélioration est réalisée grâce à la configuration automatique des stratégies suivantes :

- Ajout de `Appdata\Local\Microsoft\Windows\Caches` et `Appdata\Local\Packages` à **Dossiers en miroir**
- Ajout de `Appdata\Local\Microsoft\Windows\UsrClass.Dat*` aux **Fichiers à synchroniser**

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, la configuration automatique est activée. Dans ce cas, les paramètres de Profile Management peuvent changer si l'environnement change.

### Fermer la session de l'utilisateur si un problème se produit

Permet de spécifier si Profile Management ferme la session des utilisateurs en cas de problème.

Si cette stratégie est désactivée ou n'est pas configurée, Profile Management attribue un profil temporaire aux utilisateurs en cas de problème. Par exemple, le magasin de l'utilisateur n'est pas disponible.

Si elle est activée, un message d'erreur s'affiche et la session des utilisateurs est fermée. Cela peut simplifier la résolution du problème.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, un profil temporaire est fourni.

### Programme d'amélioration de l'expérience utilisateur

Par défaut, le programme d'amélioration de l'expérience utilisateur est activé pour améliorer la qualité et les performances des produits Citrix en collectant des statistiques anonymes et des données d'utilisation.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

### Autoriser roaming de l'index de recherche pour Outlook

Autorisez l'expérience de recherche dans Outlook basée sur l'utilisateur en itinérant automatiquement les données de recherche Outlook avec le profil utilisateur. Cette fonctionnalité nécessite un espace supplémentaire dans le magasin de l'utilisateur pour stocker les index de recherche pour Outlook.

Déconnectez-vous, puis reconnectez-vous pour que cette stratégie prenne effet.

### Base de données d'index de recherche Outlook : sauvegarde et restauration

Permet de spécifier les actions que Profile Management exécute lors de l'ouverture de session lorsque la stratégie Autoriser roaming de l'index de recherche pour Outlook est activée.

Si cette fonctionnalité est activée, Profile Management enregistre une sauvegarde de la base de données d'index de recherche chaque fois que la base de données est montée correctement lors de l'ouverture de session. Profile Management traite la sauvegarde comme la copie correcte de la base de données d'index de recherche. Lorsqu'une tentative de montage de la base de données d'index de recherche échoue en raison d'une corruption de la base de données, Profile Management revient automatiquement à la dernière copie correcte connue de la base de données d'index de recherche.

> Remarque :
>
> Profile Management supprime la sauvegarde précédemment enregistrée après l'enregistrement d'une nouvelle sauvegarde. La sauvegarde consomme l'espace de stockage disponible des fichiers VHDX.

#### Activer la prise en charge des sessions simultanées pour le roaming des données de recherche de Outlook

Permet à Profile Management de fournir une expérience de recherche Outlook native lors de sessions simultanées d'un même utilisateur. Utilisez cette stratégie avec la stratégie Roaming de l'index de recherche pour Outlook.

Lorsque cette stratégie est activée, chaque session simultanée utilise un fichier OST Outlook distinct.

Par défaut, seuls deux disques VHDX peuvent être utilisés pour stocker les fichiers OST Outlook (un fichier par disque). Si l'utilisateur démarre d'autres sessions, ses fichiers OST Outlook sont stockés dans le profil utilisateur local. Vous pouvez spécifier le nombre maximal de disques VHDX pour le stockage des fichiers OST Outlook.

#### Activer le conteneur OneDrive

Permet aux dossiers OneDrive de se déplacer avec les utilisateurs.

Le conteneur OneDrive est une solution d'itinérance de dossiers basée sur VHDX. Profile Management crée un fichier VHDX par utilisateur sur un partage de fichiers et stocke les dossiers OneDrive des utilisateurs dans les fichiers VHDX. Les fichiers VHDX sont attachés lorsque les utilisateurs ouvrent une session et sont détachés lorsque les utilisateurs se déconnectent.

### Itinérance des applications UWP

Permet aux applications UWP (Universal Windows Platform) de se déplacer avec les utilisateurs. Par conséquent, les utilisateurs peuvent accéder aux mêmes applications UWP à partir de différents appareils.

Lorsque cette stratégie est activée, Profile Management permet aux applications de se déplacer avec les utilisateurs en les stockant sur des disques VHDX distincts. Ces disques sont attachés lors de la connexion des utilisateurs et détachés lors des déconnexions des utilisateurs.

Priorité de la configuration :

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.
Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, cette fonctionnalité est désactivée.

#### Activer le traitement asynchrone pour la stratégie de groupe utilisateur à la connexion

Windows fournit deux modes de traitement pour la stratégie de groupe utilisateur : synchrone et asynchrone. Windows utilise une valeur de registre pour déterminer le mode de traitement pour la prochaine ouverture de session utilisateur. Si la valeur de registre n'existe pas, le mode synchrone est appliqué. La valeur de registre est un paramètre au niveau de la machine et ne se déplace pas avec les utilisateurs. Ainsi, le mode asynchrone ne sera pas appliqué comme prévu si les utilisateurs :

- Ouvrent une session sur différentes machines.
- Ouvrent une session sur la même machine que celle sur laquelle la stratégie Supprimer les profils mis en cache localement à la fermeture de session est activée.

Lorsque cette stratégie est activée, la valeur de registre se déplace avec les utilisateurs. Par conséquent, le mode de traitement est appliqué chaque fois que les utilisateurs ouvrent une session.

#### Taux d'espace libre pour déclencher le compactage des disques VHD

Applicable lorsque l'option Activer le compactage des disques VHD est activée. Permet de spécifier le taux d'espace libre pour déclencher le compactage des disques VHD. Lorsque le taux d'espace libre dépasse la valeur spécifiée à la fermeture de session de l'utilisateur, le compactage des disques est déclenché.

Taux d'espace libre = (taille actuelle du fichier VHD —taille de fichier VHD minimale requise*) ÷ taille actuelle du fichier VHD

* Obtenue à l'aide de la méthode GetSupportedSize de la classe `MSFT_Partition` à partir du système d'exploitation Microsoft Windows.

#### Nombre de fermetures de session pour déclencher le compactage des disques VHD

Applicable lorsque l'option Activer le compactage des disques VHD est activée. Permet de spécifier le nombre de fermetures de session pour déclencher le compactage des disques VHD.

Lorsque le nombre de fermetures de session depuis le dernier compactage atteint la valeur spécifiée, le compactage des disques est à nouveau déclenché.

#### Désactiver la défragmentation pour le compactage des disques VHD

Applicable lorsque l'option Activer le compactage des disques VHD est activée. Permet de spécifier si la défragmentation des fichiers doit être désactivée pour le compactage des disques VHD.

Lorsque le compactage des disques VHD est activé, le fichier du disque VHD est d'abord automatiquement défragmenté à l'aide de l'outil `defrag` intégré à Windows, puis compacté. La défragmentation des disques VHD produit de meilleurs résultats de compactage, tandis que sa désactivation permet d'économiser des ressources système.

### Activer la réécriture multisession pour les conteneurs de profils

Active la réécriture pour les conteneurs de profil dans des scénarios multi-sessions. Si cette option est activée, les modifications apportées à toutes les sessions sont écrites dans les conteneurs de profil. Sinon, seules les modifications apportées à la première session sont enregistrées car seule la première session est en mode lecture/écriture dans les conteneurs de profils. Les conteneurs de profils Citrix Profile Management sont pris en charge à partir de Citrix Profile Management 2103. FSLogix Profile Container est pris en charge à partir de Citrix Profile Management 2003.

Pour utiliser cette stratégie avec FSLogix Profile Container, assurez-vous que les conditions préalables suivantes sont remplies :

- La fonctionnalité FSLogix Profile Container est installée et activée.
- Le type de profil est défini sur **Try for read-write profile and fallback to read-only** dans FSLogix.

### Répliquer magasins d'utilisateurs

Permet de répliquer le magasin de profils utilisateur distant vers plusieurs chemins à chaque ouverture et fermeture de session. Cela permet à Profile Management de fournir une redondance des profils pour les connexions des utilisateurs.

L'activation de la stratégie augmente les E/S système et peut prolonger les déconnexions.

> **Remarque :**
>
> - Cette fonctionnalité est disponible à la fois pour le magasin d'utilisateurs et pour le conteneur de profils complet.
> - Les conteneurs de profils répliqués fournissent une redondance des profils pour les connexions des utilisateurs, mais pas pour le basculement en cours de session.

### Activer l'accès basé sur les informations d'identification aux magasins d'utilisateurs

Par défaut, Citrix Profile Management utilise l'identité de l'utilisateur actuel pour accéder au magasin de l'utilisateur. Activez cette fonctionnalité si vous ne souhaitez pas que Profile Management emprunte l'identité de l'utilisateur actuel lors de l'accès au magasin de l'utilisateur. Vous pouvez placer des magasins d'utilisateurs dans des référentiels de stockage (par exemple, Fichiers Azure) auxquels l'utilisateur actuel n'a aucune autorisation d'accès.

Pour vous assurer que Profile Management peut accéder aux magasins d'utilisateurs, enregistrez les informations d'identification du serveur de stockage de profils dans Workspace Environment Management (WEM) ou dans le Gestionnaire d'informations d'identification Windows. Nous vous recommandons d'utiliser Workspace Environment Management pour éliminer la nécessité de configurer les mêmes informations d'identification pour chaque machine sur laquelle Profile Management s'exécute. Si vous utilisez le Gestionnaire d'informations d'identification Windows, utilisez le compte Système local pour enregistrer les informations d'identification en toute sécurité.

> **Remarque :**
>
> Cette stratégie est disponible à la fois pour les magasins utilisateur basés sur des fichiers et basés sur VHDX. Pour les versions de Profile Management antérieures à 2212, cette stratégie n'est disponible que pour les magasins utilisateur basés sur VHDX.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée. Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, il est désactivé par défaut.

### Personnaliser le chemin de stockage des fichiers VHDX

Profile Management offre les stratégies VHDX suivantes : Conteneur de profils, Roaming de l'index de recherche pour Outlook et Accélérer la mise en miroir des dossiers. Par défaut, les fichiers VHDX sont stockés dans le magasin de l'utilisateur. Cette stratégie vous permet de spécifier un chemin d'accès distinct pour les stocker.

### Capacité par défaut des conteneurs VHD

Permet de définir la capacité de stockage par défaut (en Go) des conteneurs VHD.

Priorité de la configuration :

1. Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée.
2. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, la valeur par défaut est 50 (Go).

### Rattacher automatiquement les disques VHDX dans les sessions

Lorsque cette stratégie est activée, Profile Management garantit un haut niveau de stabilité des stratégies basées sur VHDX. Cette stratégie est activée par défaut.

Lorsque cette stratégie est activée, Profile Management surveille les disques VHDX qui sont utilisés par les stratégies basées sur VHDX. Si l'un des disques est détaché, Profile Management le réattache automatiquement.

### Seuil d'expansion automatique des conteneurs de profils

Permet de spécifier le pourcentage d'utilisation de la capacité de stockage à laquelle les conteneurs de profils déclenchent l'expansion automatique.

Priorité de la configuration :

- Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée.
- Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, la valeur par défaut est 90 (%) de capacité de stockage.

### Incrément d'expansion automatique des conteneurs de profils

Permet de spécifier la capacité de stockage (en Go) par laquelle les conteneurs de profils s'étendent automatiquement lorsque l'expansion automatique est déclenchée.

Priorité de la configuration :

- Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée.
- Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, la valeur par défaut est 10 (Go).

### Limite d'expansion automatique des conteneurs de profils

Permet de spécifier la capacité de stockage maximale (en Go) à laquelle les conteneurs de profils peuvent s'étendre automatiquement lorsque l'expansion automatique est déclenchée.

Priorité de la configuration :

- Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée.
- Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, la valeur par défaut est 80 (Go).

### Activer les paramètres de stratégie au niveau de l'utilisateur

Lorsque cette stratégie est activée, les paramètres de stratégie au niveau de la machine peuvent fonctionner au niveau de l'utilisateur, et les paramètres au niveau de l'utilisateur remplacent les paramètres au niveau de la machine.

Priorité de la configuration :

1. Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée.
2. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, elle est désactivée.

### Définir l'ordre de priorité pour les groupes d'utilisateurs

Spécifiez l'ordre de priorité pour les groupes d'utilisateurs. L'ordre détermine quel groupe est prioritaire lorsqu'un utilisateur appartient à plusieurs groupes avec des paramètres de stratégie différents.

Lorsqu'un utilisateur appartient à plusieurs groupes dont les paramètres de stratégie sont en conflit, tenez compte des points suivants :

- Si l'utilisateur appartient à un ou plusieurs groupes définis dans cette stratégie, le groupe ayant la priorité la plus élevée est prioritaire.
- Si l'utilisateur n'appartient à aucun des groupes définis dans cette stratégie, le groupe dont le SID est répertorié en premier dans l'ordre alphabétique est prioritaire.

### Méthode de sélection du magasin utilisateur

Vous permet de préciser la méthode de sélection du magasin utilisateur lorsque plusieurs options sont disponibles. Les options sont les suivantes :

- **Ordre de configuration.** Profile Management sélectionne le premier magasin configuré.
- **Performances d'accès.** Profile Management sélectionne le magasin offrant les meilleures performances d'accès.

Priorité de la configuration :

1. Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est prise en compte.
2. Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, l'**Ordre de configuration** est utilisé.

# Paramètres de stratégie De base

June 27, 2024

Cette section contient des paramètres de stratégie liés à la configuration de base de Profile Management.

## Activer Profile Management

Par défaut, Profile Management ne traite pas les ouvertures/fermetures de session pour faciliter le déploiement. N'activez Profile Management qu'après avoir terminé toutes les autres tâches de configuration et testé le comportement des profils utilisateur Citrix dans votre environnement.

Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, Profile Management ne traite pas les profils utilisateur Windows.

## Groupes traités

Les groupes d'ordinateurs locaux et les groupes de domaines (locaux, globaux et universels) peuvent être utilisés. Les groupes de domaines doivent être spécifiés au format : NOM DE DOMAINE\NOM DE GROUPE.

Si cette stratégie est configurée ici, Profile Management traite uniquement les membres appartenant à ces groupes d'utilisateurs. Si cette stratégie est désactivée, Profile Management traite tous les utilisateurs. Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, les membres de tous les groupes d'utilisateurs sont traités.

## Groupes exclus

Vous pouvez utiliser des groupes d'ordinateurs locaux et des groupes de domaines (locaux, globaux et universels) pour empêcher le traitement de certains profils utilisateur spécifiques. Spécifiez les groupes de domaines au format : NOM DE DOMAINE\NOM DE GROUPE

Si ce paramètre est configuré ici, Profile Management exclut les membres appartenant à ces groupes d'utilisateurs. Si ce paramètre est désactivé, Profile Management n'exclut aucun utilisateur. Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée. Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, aucun membre des groupes n'est exclu.

### Traiter les connexions des administrateurs locaux

Spécifie si les ouvertures de session des membres du groupe BUILTIN\Administrateurs sont traitées. Supposons que cette stratégie est désactivée ou qu'elle n'est pas configurée sur les systèmes d'exploitation multi-sessions, tels que les environnements Citrix Virtual Apps. Dans ce cas, Profile Management suppose que les ouvertures de session des utilisateurs du domaine, mais pas des administrateurs locaux, doivent être traitées. Sur les systèmes d'exploitation mono-session (tel que les environnements Citrix Virtual Desktops), les ouvertures de session des administrateurs locaux sont traitées. Cette stratégie permet aux utilisateurs du domaine disposant de droits d'administrateur local, généralement les utilisateurs de Citrix Virtual Desktops avec des bureaux virtuels attribués, de :

- Ignorer tout traitement
- Ouvrir une session
- Résoudre les problèmes rencontrés sur le bureau avec Profile Management

Remarque : les ouvertures de session des utilisateurs du domaine peuvent être soumises à des restrictions imposées par l'appartenance à un groupe. Ces dernières sont généralement mises en place pour garantir le respect des exigences relatives à l'attribution de licences pour les produits.
Si cette stratégie est désactivée, les ouvertures de session des administrateurs locaux ne sont pas traitées par Profile Management. Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, les administrateurs ne sont pas traités.

### Chemin d'accès au magasin de l'utilisateur

Définit le chemin d'accès au répertoire (le magasin de l'utilisateur) dans lequel les paramètres utilisateur (modifications apportées au registre et fichiers synchronisés) sont enregistrés.

Le chemin d'accès peut être :

- Un chemin d'accès relatif. Il doit être relatif au répertoire de base (qui est généralement configuré en tant qu'attribut #homeDirectory# pour un utilisateur dans Active Directory).
- Un chemin UNC. Il spécifie généralement un partage de serveurs ou un espace de noms DFS.
- Désactivé ou non configuré. Dans ce cas, la valeur #homeDirectory#\Windows est utilisée.

Les types de variables suivants peuvent être utilisés pour cette stratégie :

- Variables d'environnement système entourées de symboles pourcentage (par exemple, %ProfVer%). Les variables d'environnement système requièrent généralement une configuration supplémentaire.
- Attributs de l'objet utilisateur Active Directory entourés de hachages (par exemple, #sAMAccountName#).

- Variables Profile Management. Pour de plus amples informations, consultez la documentation de Variables Profile Management.

Les variables d'environnement système ne peuvent pas être utilisées, à l'exception de %username% et %userdomain%. Vous pouvez également créer des attributs personnalisés pour définir des variables d'organisation telles que l'emplacement ou les utilisateurs. Les attributs sont sensibles à la casse.

Exemples :

- \server\share#sAMAccountName# stocke les paramètres utilisateur dans le chemin UNC \\server\share\JohnSmith (si #sAMAccountName# correspond à JohnSmith pour l'utilisateur actuel)
- \server\profiles$%USERNAME%.%USERDOMAIN%!CTX_OSNAME!!CTX_OSBITNESS! peut donc correspondre à \server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64

Important : quels que soient les attributs ou variables que vous utilisez, vérifiez que cette stratégie est appliquée au dossier de niveau supérieur du dossier contenant NTUSER.DAT. Par exemple, si le fichier figure dans \server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile, définissez le chemin d'accès au magasin de l'utilisateur comme tel : \server\profiles$\JohnSmith.Finance\Win8x64 (en n'incluant pas le sous-dossier \UPM_Profile).

Pour de plus amples informations sur l'utilisation de variables lors de la spécification du chemin d'accès au magasin de l'utilisateur, consultez les rubriques suivantes :

- Partager les profils utilisateur Citrix sur des serveurs de fichiers multiples
- Gérer des profils au sein d'unités d'organisation et entre ces dernières
- Haute disponibilité et récupération d'urgence avec Profile Management

Si Chemin d'accès au magasin de l'utilisateur est désactivé, les paramètres utilisateur sont enregistrés dans le sous-répertoire Windows du répertoire de base.

Si cette stratégie est désactivée, les paramètres utilisateur sont enregistrés dans le sous-répertoire Windows du répertoire de base. Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, le répertoire Windows du lecteur de base est utilisé.

### Migrer le magasin utilisateur

Spécifie le chemin d'accès au dossier dans lequel les paramètres utilisateur (modifications du registre et fichiers synchronisés) ont été précédemment enregistrés (chemin d'accès au magasin utilisateur précédemment utilisé).

Si ce paramètre est configuré, les paramètres utilisateur stockés dans le magasin utilisateur précédent sont migrés vers le magasin utilisateur actuel spécifié dans la stratégie Chemin d'accès au magasin de l'utilisateur.

Le chemin peut être un chemin UNC absolu ou relatif au répertoire de base.

Dans les deux cas, vous pouvez utiliser les types de variables suivants :

- Variables d'environnement système entourées de symboles de pourcentage
- Attributs de l'objet utilisateur Active Directory entourés de symboles de hachage

Exemples :

- Le dossier `Windows\\%ProfileVer%` stocke les paramètres utilisateur dans un sous-dossier appelé `Windows\W2K3` du magasin utilisateur (si %ProfileVer% est une variable d'environnement système qui correspond à W2K3).
- `\\server\share\\#SAMAccountName#` stocke les paramètres utilisateur sur le chemin UNC `\\server\share\<JohnSmith>` (si `#SAMAccountName#` correspond à JohnSmith pour l'utilisateur actuel).

Dans le chemin d'accès, vous pouvez utiliser des variables d'environnement utilisateur, à l'exception de `%username%` et `%userdomain%`.

Si ce paramètre est désactivé, les paramètres utilisateur sont enregistrés dans le magasin utilisateur actuel.

Si ce paramètre n'est pas configuré ici, le paramètre correspondant du fichier .ini est utilisé.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, les paramètres utilisateur sont enregistrés dans le magasin utilisateur actuel.

### Réécriture active

Les fichiers et dossiers (mais pas les entrées de registre) qui sont modifiés peuvent être synchronisés avec le magasin d'utilisateur durant une session, avant la fermeture de session.

Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, elle est activée.

Prise en charge des profils déconnectés

Cette stratégie permet la synchronisation des profils avec le magasin de l'utilisateur dans les plus brefs délais. Il vise plus particulièrement les utilisateurs d'ordinateurs portables ou de périphériques mobiles itinérants. Lorsque la connexion au réseau est interrompue, les profils restent inchangés sur l'ordinateur portable ou le périphérique même après redémarrage ou mise en veille prolongée. Lorsque les utilisateurs mobiles travaillent, leurs profils sont mis à jour localement. Ils sont également synchronisés avec le magasin de l'utilisateur lorsque la connexion réseau est rétablie.

Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, les profils déconnectés sont désactivés.

### Registre en réécriture active

Utilisez cette stratégie avec la « Réécriture active ». Les entrées de Registre modifiées peuvent être synchronisées avec le magasin de l'utilisateur au milieu d'une session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si vous ne configurez pas ce paramètre ici ou dans le fichier .ini, le registre en réécriture active est désactivé.

#### Réécriture active sur verrouillage et déconnexion de session

Si cette stratégie et la stratégie **Réécriture active** sont activées, les fichiers et les dossiers de profil ne sont réécrits que lorsqu'une session est verrouillée ou déconnectée.

Si cette stratégie et les stratégies **Réécriture active** et **Registre en réécriture active** sont activées, les entrées de registre ne sont réécrites que lorsqu'une session est verrouillée ou déconnectée.

### Prise en charge des profils déconnectés

Active la fonctionnalité de profils déconnectés. Cette fonctionnalité est destinée aux ordinateurs qui sont généralement supprimés des réseaux. Par exemple, les ordinateurs portables ou les appareils mobiles et non les serveurs ou les ordinateurs de bureau.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, la prise en charge des profils déconnectés est désactivée.

## Paramètres de stratégie Multi-plateformes

June 27, 2024

Cette section contient des paramètres de stratégie liés à la configuration de la fonctionnalité de paramètres **multi-plateformes de Profile Management**.

### Activer les paramètres multi-plateformes

Pour faciliter le déploiement, les paramètres multi-plateformes sont désactivés par défaut. L'activation de cette stratégie permet d'activer le traitement, mais elle doit se faire après une planification détaillée et des tests approfondis de cette fonctionnalité.

Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, aucun paramètre multi-plateforme n'est appliqué.

### Paramètres multi-plateformes des groupes d'utilisateurs

Entrez un ou plusieurs groupes d'utilisateurs Windows. Par exemple, vous pouvez utiliser cette stratégie pour traiter uniquement les profils d'un groupe d'utilisateurs test. Si cette stratégie est configurée, la fonctionnalité Paramètres multi-plateformes de Profile Management traite uniquement les membres appartenant à ces groupes d'utilisateurs. Si cette stratégie est désactivée, les processus de la fonctionnalité traitent tous les utilisateurs spécifiés par la stratégie Groupes traités.

Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, tous les groupes d'utilisateurs sont traités.

### Chemin d'accès aux définitions multi-plateformes

Identifie l'emplacement réseau des fichiers de définition que vous avez copiés depuis le pack de téléchargement. Ce chemin doit être un chemin UNC. Les utilisateurs doivent avoir accès à cet emplacement, et les administrateurs doivent y posséder un accès en écriture. L'emplacement doit être un partage de fichiers SMB (Server Message Block) ou CIFS (Common Internet File System).

Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, aucun paramètre multi-plateforme n'est appliqué.

### Chemin d'accès au magasin des paramètres multi-plateformes

Définit le chemin d'accès au magasin des paramètres multi-plateformes, le dossier dans lequel les paramètres multi-plateformes des utilisateurs sont enregistrés. Les utilisateurs doivent posséder des droits en écriture sur cette zone. Le chemin peut être un chemin UNC absolu ou relatif au répertoire de base.

Cette zone est une zone commune du magasin de l'utilisateur dans laquelle les données de profil partagées par de multiples plates-formes sont stockées. Les utilisateurs doivent posséder des droits en écriture sur cette zone. Le chemin peut être un chemin UNC absolu ou relatif au répertoire de base. Vous pouvez utiliser les mêmes variables que pour le **Chemin d'accès au magasin de l'utilisateur**.

Si cette stratégie est désactivée, le chemin d'accès Windows\PM_CP est utilisé. Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, la valeur par défaut est utilisée.

### Source utilisée pour créer les paramètres multi-plateformes

Spécifie une plate-forme en tant que plateforme de base si cette stratégie est activée dans l'unité d'organisation de cette plate-forme. Cette stratégie effectue la migration des données depuis les profils de la plate-forme de base vers le magasin de paramètres multi-plateformes.

Le jeu de profils de chaque plate-forme est stocké dans une unité d'organisation distincte. Vous devez décider quelles données de profil de la plate-forme utiliser pour amorcer le magasin de paramètres multi-plateformes. On parle de plate-forme de base. Supposons que le magasin des paramètres multi-plateformes contient un fichier de définition sans aucune donnée, ou que les données mises en cache dans un profil mono-plateforme sont plus récentes que les données de définition du magasin. Dans ce cas, Profile Management migre les données du profil mono-plateforme vers le magasin sauf si vous désactivez ce paramètre.

> **Important :**
>
> Si cette stratégie est activée dans plusieurs unités d'organisation, ou plusieurs objets d'utilisateur ou de machine, la plate-forme sur laquelle le premier utilisateur ouvre une session devient le profil de base.
> Cette stratégie est activée par défaut.

## Paramètres de stratégie Système de fichiers

June 27, 2024

Cette section contient des stratégies qui définissent les éléments suivants :

- Quels fichiers d'un profil utilisateur sont synchronisés entre le système sur lequel le profil est installé et le magasin utilisateur
- Quels répertoires d'un profil utilisateur sont synchronisés entre le système sur lequel le profil est installé et le magasin utilisateur

## Paramètres de stratégie Exclusions

June 27, 2024

Cette section décrit les paramètres de stratégie permettant de configurer les fichiers et les répertoires dans un profil utilisateur qui sont exclus du processus de synchronisation.

### Liste d'exclusion - fichiers

Liste des fichiers ignorés durant la synchronisation. Les noms de fichier doivent être des chemins d'accès relatifs au profil utilisateur (%USERPROFILE%). Les caractères génériques sont pris en charge dans les noms de fichiers et les noms de dossiers, mais seuls les caractères génériques dans les noms de fichiers sont appliqués de manière récursive.

Exemples :

- `Desktop\Desktop.ini` ignore le fichier `Desktop.ini` du dossier `Desktop`
- `%USERPROFILE%\*.tmp` ignore tous les fichiers ayant l'extension `.tmp` dans l'ensemble du profil
- `AppData\Roaming\MyApp\*.tmp` ignore tous les fichiers ayant l'extension `.tmp` dans une partie du profil
- `Downloads\*\a.txt` ignore `a.txt` dans n'importe quel sous-dossier immédiat du dossier `Downloads`.

Si cette stratégie est désactivée, aucun fichier n'est exclu. Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, aucun fichier n'est exclu.

### Activer liste d'exclusion par défaut - répertoires

Liste par défaut des répertoires ignorés durant la synchronisation. Utilisez cette stratégie pour spécifier des répertoires d'exclusion de GPO sans avoir à les remplir manuellement.

Si vous désactivez cette stratégie, Profile Management n'exclut aucun répertoire par défaut.

Si vous ne configurez pas cette stratégie ici, Profile Management utilise la valeur du fichier .ini. Si vous ne configurez pas cette stratégie ici ou dans le fichier .ini, Profile Management n'exclut aucun répertoire par défaut.

### Liste d'exclusion - répertoires

Liste des dossiers ignorés durant la synchronisation. Les noms de dossier doivent être spécifiés en tant que chemins d'accès relatifs au profil utilisateur (%USERPROFILE%). Les caractères génériques dans les noms de dossiers sont pris en charge, mais ne sont pas appliqués de manière récursive.

Exemple :

- `Desktop` ignore le dossier `Desktop` du profil utilisateur

Si cette stratégie est désactivée, aucun dossier n'est exclu. Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, aucun dossier n'est exclu.

### Vérification des éléments exclus à l'ouverture de session

Ce paramètre configure ce que Profile Management fait si un profil dans le magasin d'utilisateurs contient des fichiers ou des dossiers exclus. Les paramètres de stratégie possibles et les actions correspondantes sont répertoriés dans le tableau suivant :

| Paramètre de stratégie | Action |
|---|---|
| Le paramètre est désactivé ou « Synchroniser les fichiers ou dossiers à l'ouverture de session » est défini sur la valeur par défaut | Profile Management synchronise les fichiers ou dossiers exclus du magasin de l'utilisateur vers le profil local lorsqu'un utilisateur ouvre une session. |
| Le paramètre est défini sur « Ignorer les fichiers ou dossiers exclus à l'ouverture de session » | Profile Management ignore les fichiers ou dossiers exclus du magasin de l'utilisateur lorsqu'un utilisateur ouvre une session. |
| Le paramètre est défini sur « Supprimer les fichiers ou dossiers exclus lors de l'ouverture de session » | Profile Management supprime les fichiers ou dossiers exclus du magasin de l'utilisateur lorsqu'un utilisateur ouvre une session. |
| Le paramètre n'est pas configuré dans Web Studio | La valeur du fichier .ini est utilisée |
| Le paramètre n'est pas configuré dans Web Studio ni dans le fichier .ini | Les fichiers ou dossiers exclus sont synchronisés à partir du magasin utilisateur vers un profil local lorsqu'un utilisateur ouvre une session. |

### Traitement de fichiers de grande taille : fichiers à créer en tant que liens symboliques

Pour améliorer les performances d'ouverture de session et traiter les fichiers volumineux, Profile Management crée un lien symbolique au lieu de copier les fichiers dans cette liste.

Vous pouvez utiliser des caractères génériques dans les stratégies qui font référence aux fichiers, par exemple `!ctx_localappdata!\Microsoft\Outlook\*.OST`.

Pour traiter le fichier de dossiers en mode hors connexion (`*.ost`) de Microsoft Outlook, assurez-vous que le dossier **Outlook** n'est pas exclu pour Profile Management.

Ces fichiers ne peuvent pas être accessibles simultanément dans plusieurs sessions.

# Paramètres de stratégie Synchronisation

June 27, 2024

La section **Synchronisation** contient des paramètres de stratégie pour spécifier les fichiers et les dossiers dans un profil utilisateur qui sont synchronisés entre le système sur lequel le profil est installé et le magasin de l'utilisateur.

## Répertoires à synchroniser

Par défaut, Profile Management synchronise le profil utilisateur entre le système sur lequel il est installé et le magasin d'utilisateur. Si vous excluez un dossier de la synchronisation, cette stratégie vous permet d'inclure les sous-dossiers contenus dans le dossier exclu lors de la synchronisation.

Les chemins d'accès de cette liste doivent être relatifs au profil utilisateur. Les caractères génériques dans les noms de dossiers sont pris en charge, mais ne sont pas appliqués de manière récursive.

Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, seuls les dossiers non exclus dans le profil utilisateur sont synchronisés.

## Fichiers à synchroniser

Par défaut, Profile Management synchronise le profil utilisateur entre le système sur lequel il est installé et le magasin d'utilisateur. Si vous excluez un dossier de la synchronisation, cette stratégie vous permet d'inclure les fichiers contenus dans le dossier exclu lors de la synchronisation.

Les chemins d'accès de cette liste doivent être relatifs au profil utilisateur. Les caractères génériques sont pris en charge dans les noms de fichiers et les noms de dossiers, mais seuls les caractères génériques dans les noms de fichiers sont appliqués de manière récursive. Les caractères génériques ne peuvent pas être imbriqués.

Exemples :

- `AppData\Local\Microsoft\Office\Access.qat` spécifie un fichier sous un dossier exclus dans la configuration par défaut.
- `AppData\Local\MyApp\*.cfg` spécifie tous les fichiers avec l'extension `.cfg` dans le dossier de profil `AppData\Local\MyApp` et ses sous-dossiers.

Si vous désactivez cette stratégie, cela revient à l'activer et à configurer une liste vide.

Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, seuls les fichiers non exclus dans le profil utilisateur sont synchronisés.

### Dossiers en miroir

Cette stratégie permet de faciliter la résolution des problèmes similaires rencontrés avec tout dossier transactionnel (également appelé dossier référentiel). Ce dossier contient des fichiers interdépendants, dans lequel un fichier fait référence à l'autre.

La mise en miroir de dossiers permet à Profile Management de traiter un dossier transactionnel et son contenu en tant qu'entité unique, ce qui évite l'engorgement du profil. Vous pouvez par exemple mettre en miroir le dossier **Cookies d'Internet Explorer** de façon à synchroniser le fichier Index.dat avec les cookies qu'il indexe. Dans ces situations, le modèle « Last Write Wins » s'applique. Cela veut dire que les fichiers présents dans les dossiers mis en miroir qui ont été modifiés dans plus d'une session sont écrasés par la dernière mise à jour, ce qui se traduit par la perte des modifications apportées au profil.

Par exemple, le tableau suivant décrit comment Index.dat fait référence aux cookies lorsqu'un utilisateur navigue sur Internet :

| Scénario | Comment Index.dat fait référence aux cookies |
|---|---|
| Un utilisateur dispose de deux sessions Internet Explorer, chacune sur un serveur différent, et visite des sites différents au cours de chaque session.|Les cookies de chaque site sont ajoutés au serveur approprié.| Les cookies de chaque site sont ajoutés au serveur approprié. |
|L'utilisateur se déconnecte de la première session ou au milieu d'une session (si la fonction de réécriture active est configurée)| Les cookies de la deuxième session doivent remplacer ceux de la première session.|
|Les première et deuxième sessions sont fusionnées et les références aux cookies dans Index.dat deviennent périmées| Lorsque l'utilisateur accède de nouveau à des sites dans les nouvelles sessions, cela entraîne davantage de fusions et la saturation du dossier de cookies.|

La mise en miroir du dossier de cookies résout le problème. Dans ce cas, les cookies sont remplacés par ceux de la dernière session chaque fois que l'utilisateur se déconnecte. Index.dat reste donc constamment à jour.

Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, aucun dossier n'est mis en miroir.

### Accélérer la mise en miroir des dossiers

Lorsque cette stratégie et la stratégie **Dossiers en miroir** sont activées, **Profile Management stocke les dossiers mis en miroir** sur un disque virtuel VHDX. Il attache le disque virtuel lors de l'ouverture de session et le détache à la fin de la session. L'activation de cette stratégie élimine la nécessité de copier les dossiers entre le magasin de l'utilisateur et les profils locaux et accélère la mise en miroir des dossiers.

## Paramètres de stratégie Redirection de dossiers

June 27, 2024

Cette section contient des paramètres de stratégie permettant de spécifier si vous souhaitez rediriger les dossiers qui apparaissent communément dans des profils vers un emplacement réseau partagé.

### Accorder l'accès administrateur

Ce paramètre permet à un administrateur d'accéder au contenu des dossiers redirigés des utilisateurs.

> **Remarque :**
>
> Ce paramètre accorde des autorisations aux administrateurs disposant d'un accès complet et sans restriction au domaine.

Par défaut, ce paramètre est désactivé et les utilisateurs disposent d'un accès exclusif au contenu de leurs dossiers redirigés.

### Inclure le nom de domaine

Ce paramètre permet d'activer l'inclusion de la variable d'environnement `%userdomain%` dans le chemin d'accès UNC. Ce chemin UNC est spécifié pour les dossiers redirigés.

Par défaut, ce paramètre est désactivé. La variable d'environnement `%userdomain%` n'est pas incluse dans le chemin UNC spécifié pour les dossiers redirigés.

## Paramètres de stratégie AppData (Roaming)

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **AppData (Roaming)** vers un emplacement réseau partagé.

### Chemin AppData (Roaming)

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier **AppData(Roaming)** est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Paramètres de redirection du dossier AppData(Roaming)

Ce paramètre spécifie comment rediriger le contenu du dossier **AppData(Roaming)**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC. Pour plus d'informations, consultez la section Chemin d'accès au magasin de l'utilisateur.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

## Paramètres de stratégie Contacts

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **Contacts** vers un emplacement réseau partagé.

### Chemin d'accès au dossier Contacts

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier **Contacts** est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Paramètres de redirection du dossier Contacts

Ce paramètre spécifie comment rediriger le contenu du dossier **Contacts**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

## Paramètres de stratégie Bureau

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier `Desktop` vers un emplacement réseau partagé.

### Chemin d'accès au dossier Bureau

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier **Desktop** est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Paramètres de redirection du dossier Bureau

Ce paramètre spécifie comment rediriger le contenu du dossier **Bureau**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

## Paramètres de stratégie Documents

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **Documents** vers un emplacement réseau partagé.

### Chemin d'accès au dossier Mes documents

Ce paramètre spécifie l'emplacement réseau vers lequel les fichiers du dossier **Documents** sont redirigés.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

Le paramètre **Chemin d'accès** au dossier Documents doit être activé non seulement pour rediriger les fichiers vers le dossier **Documents**, mais aussi pour rediriger les fichiers vers les dossiers **Musique**, **Images** et **Vidéos**.

### Paramètres de redirection du dossier Mes documents

Ce paramètre spécifie la manière de rediriger le contenu du dossier **Documents**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler la manière de rediriger le contenu du dossier **Documents**, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Redirections de contenu pour le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Documents.
- Rediriger vers le répertoire de base de l'utilisateur. Redirections de contenu pour le répertoire de base utilisateur, généralement configuré en tant qu'attribut #homeDirectory# pour un utilisateur dans Active Directory.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

## Télécharge les stratégies de groupe

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **Téléchargements** vers un emplacement réseau partagé.

### Chemin d'accès au dossier Téléchargements

Ce paramètre spécifie l'emplacement réseau vers lequel les fichiers du dossier **Téléchargements** sont redirigés.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Paramètres de redirection du dossier Téléchargements

Ce paramètre spécifie la redirection du contenu du dossier **Téléchargements**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

## Paramètres de stratégie Favoris

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **Favoris** vers un emplacement réseau partagé.

### Chemin d'accès au dossier Favoris

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier **Favoris** est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Paramètres de redirection du dossier Favoris

Ce paramètre spécifie la façon de rediriger le contenu du dossier **Favoris**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

## Paramètres de stratégie Liens

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **Liens** vers un emplacement réseau partagé.

### Chemin d'accès au dossier Liens

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier **Liens** est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Paramètres de redirection du dossier Liens

Ce paramètre spécifie comment rediriger le contenu du dossier **Liens**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

## Paramètres de stratégie Musique

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **Musique** vers un emplacement réseau partagé.

### Chemin d'accès au dossier Ma musique

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier **Musique** est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Paramètres de redirection du dossier Ma musique

Ce paramètre spécifie comment rediriger le contenu du dossier **Musique**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler comment rediriger le contenu du dossier **Musique**, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Permet de rediriger du contenu vers le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Musique.
- Rediriger en fonction du dossier Documents. Permet de rediriger du contenu vers un dossier relatif au dossier Documents.

Pour rediriger du contenu vers un dossier relatif au dossier **Documents**, le paramètre **Chemin d'accès au dossier Documents** doit être activé.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

# Paramètres de stratégie Images

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **Images** vers un emplacement réseau partagé.

### Chemin d'accès au dossier Mes images

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier **Images** est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Paramètres de redirection du dossier Mes images

Ce paramètre spécifie la façon de rediriger le contenu du dossier **Images**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler la manière dont le contenu du dossier **Images** est redirigé, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Permet de rediriger du contenu vers le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Images.
- Rediriger en fonction du dossier Documents. Permet de rediriger du contenu vers un dossier relatif au dossier Documents.

Pour rediriger du contenu vers un dossier relatif au dossier **Documents**, le paramètre **Chemin d'accès au dossier Documents** doit être activé.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

# Paramètres de stratégie Parties enregistrées

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **Parties enregistrées** vers un emplacement réseau partagé.

### Paramètres de redirection du dossier Parties enregistrées

Ce paramètre spécifie comment rediriger le contenu du dossier **Parties enregistrées**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Chemin d'accès au dossier Parties enregistrées

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier **Parties enregistrées** est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

## Paramètres de stratégie Menu Démarrer

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **Menu Démarrer** vers un emplacement réseau partagé.

### Paramètres de redirection du menu Démarrer

Ce paramètre spécifie comment rediriger le contenu du dossier **Menu Démarrer**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Chemin d'accès au menu Démarrer

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier **Menu Démarrer** est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

# Paramètres de stratégie Recherches

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **Recherches** vers un emplacement réseau partagé.

### Paramètres de redirection du dossier Recherches

Ce paramètre spécifie comment rediriger le contenu du dossier **Recherches**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Chemin d'accès au dossier Recherches

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier **Recherches** est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

# Paramètres de stratégie Vidéo

June 27, 2024

Cette section contient les paramètres de stratégie permettant de rediriger le contenu du dossier **Vidéo** vers un emplacement réseau partagé.

### Paramètres de redirection pour la vidéo

Ce paramètre spécifie comment rediriger le contenu du dossier **Vidéo**.

Par défaut, le contenu est redirigé vers un chemin d'accès UNC.

Pour contrôler comment rediriger le contenu du dossier **Vidéo**, choisissez l'une des options suivantes :

- Rediriger vers le chemin UNC suivant. Permet de rediriger du contenu vers le chemin d'accès UNC spécifié dans le paramètre de stratégie Chemin d'accès au dossier Vidéo.

- Rediriger en fonction du dossier Documents. Permet de rediriger du contenu vers un dossier relatif au dossier Documents.

Pour rediriger du contenu vers un dossier relatif au dossier **Documents**, le paramètre **Chemin d'accès au dossier Documents** doit être activé.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

### Chemin d'accès au dossier Vidéo

Ce paramètre spécifie l'emplacement réseau vers lequel le contenu du dossier **Vidéo** est redirigé.

Par défaut, ce paramètre est désactivé et aucun emplacement n'est spécifié.

Si ce paramètre n'est pas configuré ici, Profile Management ne redirige pas le dossier spécifié.

## Paramètres de stratégie Journal

June 27, 2024

Cette section contient des paramètres de stratégie permettant de configurer la journalisation Profile Management.

### Actions Active Directory

Ce paramètre active ou désactive la journalisation détaillée des actions effectuées dans Active Directory.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre **Activer la journalisation** est également activé.

Si ce paramètre n'est pas configuré dans Web Studio, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré dans Web Studio ou dans le fichier .ini, les informations suivantes sont consignées :

- Errors
- Informations générales

### Informations courantes

Ce paramètre active ou désactive la journalisation détaillée des informations courantes.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre **Activer la journalisation** est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré dans Web Studio ou dans le fichier .ini, les informations suivantes sont consignées :

- Errors
- Informations générales

### Avertissements courants

Ce paramètre active ou désactive la journalisation détaillée des avertissements courants.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre **Activer la journalisation** est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré dans Web Studio ou dans le fichier .ini, les informations suivantes sont consignées :

- Errors
- Informations générales

### Activer la journalisation

Ce paramètre active ou désactive la journalisation de Profile Management en mode (journalisation détaillée) de débogage. En mode de débogage, les informations d'état complètes sont journalisées dans les fichiers journaux situées dans "%SystemRoot%\System32\Logfiles\UserProfileManager".

Par défaut, ce paramètre est désactivé et seules les erreurs sont journalisées.

Citrix vous recommande d'activer ce paramètre uniquement si vous effectuez la résolution des problèmes de Profile Management.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, seules les erreurs sont consignées.

### Actions du système de fichiers

Ce paramètre active ou désactive la journalisation détaillée des actions effectuées dans le système de fichiers.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre **Activer la journalisation** est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré dans Web Studio ou dans le fichier .ini, les informations suivantes sont consignées :

- Errors
- Informations générales

### Notifications du système de fichiers

Ce paramètre active ou désactive la journalisation détaillée des notifications des systèmes de fichiers.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre **Activer la journalisation** est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré dans Web Studio ou dans le fichier .ini, les informations suivantes sont consignées :

- Errors
- Informations générales

### Fermeture de session

Ce paramètre active ou désactive la journalisation détaillée des fermetures de session de l'utilisateur.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre **Activer la journalisation** est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré dans Web Studio ou dans le fichier .ini, les informations suivantes sont consignées :

- Errors
- Informations générales

### Ouverture de session

Ce paramètre active ou désactive la journalisation détaillée des ouvertures de session d'utilisateur.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre **Activer la journalisation** est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré dans Web Studio ou dans le fichier .ini, les informations suivantes sont consignées :

- Errors
- Informations générales

### Taille maximale du fichier journal

Ce paramètre spécifie la taille maximale autorisée pour le fichier journal de Profile Management, en octets.

Par défaut, ce paramètre est défini sur 1048576 octets (1 Mo).

Citrix recommande d'augmenter la taille de ce fichier à 5 Mo ou plus, si vous disposez de suffisamment d'espace disque. Si la taille du fichier journal dépasse la taille maximale :

- Une sauvegarde existante du fichier (.bak) est supprimée.
- Le fichier journal est renommé .bak.
- Un fichier journal est créé.

Le fichier journal est créé dans %SystemRoot%\System32\Logfiles\UserProfileManager.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, la valeur par défaut est utilisée.

### Chemin vers le fichier journal

Ce paramètre spécifie un chemin alternatif sur lequel enregistrer le fichier journal de Profile Management.

Par défaut, ce paramètre est désactivé et les fichiers journaux sont enregistrés à l'emplacement par défaut : %SystemRoot%\System32\Logfiles\UserProfileManager.

Le chemin peut pointer vers un lecteur local ou un lecteur réseau distant (chemin d'accès UNC). Les chemins d'accès distants peuvent s'avérer utiles dans les environnements de grande taille distribués, mais ils peuvent engendrer un volume important de trafic réseau, ce qui ne convient pas aux fichiers journaux. Pour les machines virtuelles pré-configurées dotées d'un disque dur persistant, définissez un chemin d'accès local à ce lecteur. Ce paramètre garantit la préservation des fichiers journaux lorsque la machine redémarre. Pour les machines virtuelles qui ne sont pas équipées d'un disque dur persistant, la définition d'un chemin d'accès UNC vous permet de conserver les fichiers journaux. Mais le compte système des machines doit disposer d'un accès en écriture au partage UNC. Utilisez un chemin d'accès local pour les ordinateurs portables gérés par la fonctionnalité de profils déconnectés.

Si un chemin d'accès UNC est utilisé pour les fichiers journaux, Citrix recommande d'appliquer une liste de contrôle d'accès appropriée au dossier du fichier journal. Il s'agit de s'assurer que seuls les comptes d'ordinateur ou d'utilisateur autorisés puissent accéder aux fichiers stockés.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, l'emplacement par défaut %SystemRoot%\System32\Logfiles\UserProfileManager est utilisé.

### Informations utilisateur personnalisées

Ce paramètre active ou désactive la journalisation détaillée des informations utilisateur personnalisées.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre **Activer la journalisation** est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré dans Web Studio ou dans le fichier .ini, les informations suivantes sont consignées :

- Errors
- Informations générales

### Valeurs de stratégie à l'ouverture et fermeture de session

Ce paramètre active ou désactive la journalisation détaillée des valeurs de stratégie lorsqu'un utilisateur ouvre ou ferme une session.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre **Activer la journalisation** est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré dans Web Studio ou dans le fichier .ini, les informations suivantes sont consignées :

- Errors
- Informations générales

### Actions du registre

Ce paramètre active ou désactive la journalisation détaillée des actions effectuées dans le Registre.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre **Activer la journalisation** est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré dans Web Studio ou dans le fichier .ini, les informations suivantes sont consignées :

- Errors
- Informations générales

### Différences de registre à la fermeture de session

Ce paramètre active ou désactive la journalisation détaillée des différences dans le registre lorsqu'un utilisateur ferme sa session.

Par défaut, ce paramètre est désactivé.

Lorsque vous activez ce paramètre, assurez-vous que le paramètre **Activer la journalisation** est également activé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré dans Web Studio ou dans le fichier .ini, les informations suivantes sont consignées :

- Errors
- Informations générales

## Paramètres de stratégie Gestion des profils

June 27, 2024

Cette section contient des paramètres de stratégie qui spécifient la manière dont Profile Management gère les profils utilisateur.

### Délai avant la suppression des profils mis en cache

Ce paramètre spécifie une extension facultative pour le délai, en minutes, avant que Profile Management supprime les profils mis en cache localement à la fermeture de session.

Une valeur de 0 supprime les profils immédiatement, à la fin du processus de fermeture de session. Profile Management vérifie les fermetures de session toutes les minutes. Par conséquent, une valeur de 60 garantit que les profils sont supprimés entre une et deux minutes après que les utilisateurs aient fermé leur session. Cette action dépend de la date de la dernière vérification. L'extension du délai est utile si vous savez qu'un processus conserve les fichiers ou que la ruche du Registre de l'utilisateur est ouverte durant la fermeture de session. Avec des profils importants, cela peut également accélérer la fermeture de session.

Par défaut, cette option est définie sur 0 et Profile Management supprime les profils mis en cache localement immédiatement.

Lorsque vous activez ce paramètre, assurez-vous que l'option Supprimer les profils mis en cache localement à la fermeture de session est également activée.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les profils sont immédiatement supprimés.

### Supprimer les profils mis en cache localement à la fermeture de session

Ce paramètre spécifie si les profils mis en cache localement sont supprimés après qu'un utilisateur ferme sa session.

Si ce paramètre est activé, le cache de profil local d'un utilisateur est supprimé après fermeture de leur session. Citrix vous recommande d'activer ce paramètre pour les serveurs Terminal Server.

Par défaut, ce paramètre est désactivé, le cache de profil local d'un utilisateur est conservé après la fermeture de session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, les profils mis en cache ne sont pas supprimés.

### Gestion des conflits de profils locaux

Ce paramètre configure le comportement de Profile Management si un profil utilisateur existe dans les deux cas suivants :

- Magasin de l'utilisateur
- Profil utilisateur Windows local (pas un profil utilisateur Citrix)

Par défaut, Profile Management utilise le profil Windows local mais n'y apporte aucune modification.

Pour contrôler le comportement de Profile Management, choisissez l'une des options suivantes :

- Utiliser profil local. Profile Management utilise le profil local, mais n'y apporte aucune modification.
- Supprimer profil local. Profile Management supprime le profil utilisateur Windows local, puis importe le profil utilisateur Citrix à partir du magasin de l'utilisateur.
- Renommer profil local. Profile Management renomme le profil utilisateur Windows local (à des fins de sauvegarde) et importe le profil utilisateur Citrix à partir du magasin de l'utilisateur.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, les profils locaux existants sont utilisés.

### Migration des profils existants

Ce paramètre spécifie les types de profil migrés vers le magasin de l'utilisateur lors de l'ouverture de session si un utilisateur ne dispose d'aucun profil courant dans le magasin de l'utilisateur.

Profile Management peut effectuer la migration des profils existants « à la volée » durant l'ouverture de session si l'utilisateur ne dispose d'aucun profil dans le magasin de l'utilisateur. Ensuite, le profil du magasin utilisateur est utilisé par Profile Management dans les deux cas suivants :

- Session en cours
- Toute autre session configurée avec le chemin d'accès au même magasin utilisateur

Par défaut, les profils locaux et itinérants sont migrés vers le magasin de l'utilisateur lors de l'ouverture de session.

Pour spécifier les types de profil migrés vers le magasin de l'utilisateur lors de l'ouverture de session, choisissez l'une des options suivantes :

- Profils locaux et itinérants
- Local
- Itinérance
- Aucun (désactivé)

Si vous sélectionnez **Aucun**, le système utilise le mécanisme Windows existant de création de profils, comme dans un environnement dans lequel Profile Management n'est pas installé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, les profils locaux et itinérants existants sont migrés.

### Migration automatique des profils d'application existants

Ce paramètre active ou désactive la migration automatique des profils d'application existants sur différents systèmes d'exploitation. Les profils d'application incluent à la fois les données d'application dans le dossier `AppData` et les entrées de registre sous `HKEY_CURRENT_USER\SOFTWARE`. Ce paramètre peut être utile dans les cas où vous souhaitez migrer vos profils d'application sur différents systèmes d'exploitation.

Par exemple, supposons que vous mettez à niveau votre système d'exploitation (OS) de Windows 10 version 1803 vers Windows 10 version 1809. Si ce paramètre est activé, Profile Management migre automatiquement les paramètres d'application existants vers Windows 10 version 1809 la première fois que chaque utilisateur ouvre une session. Par conséquent, les données d'application dans le dossier `AppData` et les entrées de registre sous HKEY_CURRENT_USER\SOFTWARE sont migrées.

Si plusieurs profils d'application sont présents, Profile Management effectue la migration dans l'ordre de priorité suivant :

1. Profils du même type d'OS (OS mono-session vers OS mono-session et OS multi-session vers OS multi-session).
2. Profils de la même famille de systèmes d'exploitation Windows (par exemple, Windows 10 à Windows 10 ou Windows Server 2016 à Windows Server 2016)
3. Profils d'une version antérieure du système d'exploitation (par exemple, Windows 7 vers Windows 10 ou Windows Server 2012 vers Windows Server 2016)
4. Profils du système d'exploitation le plus proche

**Remarque :** Vous devez spécifier le nom court du système d'exploitation en incluant la variable « !CTX_OSNAME! » dans le chemin du magasin utilisateur. Cela permet à Profile Management de localiser les profils d'application existants.

Si ce paramètre n'est pas configuré ici, les paramètres du fichier .ini sont utilisés.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, il est désactivé par défaut.

### Chemin d'accès au profil modèle

Ce paramètre spécifie le chemin d'accès au profil que vous souhaitez que Profile Management utilise comme modèle pour la création de profils utilisateur.

Le chemin d'accès spécifié doit être le chemin d'accès complet au dossier contenant le fichier de registre NTUSER.DAT ainsi que tout autre dossier et fichier requis pour le profil modèle.

Remarque : n'incluez pas NTUSER.DAT dans le chemin d'accès. Par exemple, avec le fichier \\nomserveur\mesprofils\modèle\ntuser.dat, définissez l'emplacement en tant que \\nomserveur\mesprofils\modèle.

Utilisez des chemins d'accès absolus. Il peut s'agir de chemins UNC où de chemins sur la machine locale. Vous pouvez utiliser ces derniers pour spécifier, par exemple, un profil modèle de manière permanente sur une image Citrix Provisioning Services. les chemins d'accès relatifs ne sont pas pris en charge.

Remarque : ce paramètre ne prend pas en charge l'expansion d'attributs Active Directory, de variables d'environnement système ou des variables %USERNAME% et %USERDOMAIN%.

Par défaut, ce paramètre est désactivé et les nouveaux profils utilisateur sont créés à partir du profil utilisateur par défaut sur la machine sur laquelle un utilisateur ouvre une session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

### Le profil modèle remplace le profil local

Ce paramètre active le profil modèle pour remplacer le profil local lors de la création de profils utilisateur.

Supposons qu'un utilisateur n'a pas de profil utilisateur Citrix, mais qu'il a un profil utilisateur Windows local. Dans ce cas, par défaut, le profil local est utilisé et migré vers le magasin utilisateur, si cette valeur est activée. L'activation de cette stratégie permet au profil modèle de remplacer le profil local utilisé lors de la création de profils utilisateur.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

### Le profil modèle remplace le profil itinérant

Ce paramètre active le profil modèle pour remplacer un profil itinérant lors de la création de profils utilisateur.

Supposons qu'un utilisateur n'a pas de profil utilisateur Citrix, mais qu'il a un profil utilisateur Windows itinérant. Dans ce cas, par défaut, le profil itinérant est utilisé et migré vers le magasin utilisateur, si cette valeur est activée. L'activation de ce paramètre de stratégie permet au profil modèle de remplacer le profil itinérant utilisé lors de la création de profils utilisateur.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

### Profil modèle utilisé en tant que profil Citrix obligatoire pour toutes les ouvertures de session

Ce paramètre permet d'activer Profile Management de manière à utiliser le profil modèle comme profil par défaut pour la création de tous les profils utilisateur.

Par défaut, ce paramètre est désactivé et les nouveaux profils utilisateur sont créés à partir du profil utilisateur par défaut sur la machine sur laquelle un utilisateur ouvre une session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici où dans le fichier .ini, aucun modèle n'est utilisé.

## Paramètres de stratégie Registre

June 27, 2024

Cette section contient des paramètres de stratégie permettant de spécifier les clés de Registre qui sont inclues et exclues du traitement Profile Management.

### Liste d'exclusion

Liste des clés de registre de la ruche HKCU qui sont ignorées durant la fermeture de session.

Exemple : Software\Policies

Si cette stratégie est désactivée, aucune clé de registre n'est exclue. Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, aucune clé de registre n'est exclue.

### Liste d'inclusion

Liste des clés de registre de la ruche HKCU qui sont traitées durant la fermeture de session.

Exemple : Software\Adobe.

Si cette stratégie est activée, seules les clés figurant dans cette liste sont traitées. Si cette stratégie est désactivée, la ruche HKCU entière est traitée. Si cette stratégie n'est pas configurée ici, la valeur du fichier .ini est utilisée. Si cette stratégie n'est pas configurée ici ou dans le fichier .ini, toutes les entrées de HKCU sont traitées.

### Activer liste d'exclusion par défaut - Profile Management 5.5

Liste par défaut des clés de registre de la ruche HKCU qui ne sont pas synchronisées avec le profil de l'utilisateur. Utilisez cette stratégie pour spécifier des fichiers d'exclusion de GPO sans avoir à les remplir manuellement.

Si vous désactivez cette stratégie, Profile Management n'exclut aucune clé de registre par défaut. Si vous ne configurez pas cette stratégie ici, Profile Management utilise la valeur du fichier .ini. Si vous ne configurez pas cette stratégie ici ou dans le fichier .ini, Profile Management n'exclut aucune clé de registre par défaut.

### Copie de sauvegarde de NTUSER.DAT

Permet d'effectuer une sauvegarde de la dernière copie correcte du fichier NTUSER.DAT et de le restaurer s'il venait à être endommagé.

Si vous ne configurez pas cette stratégie ici, Profile Management utilise la valeur du fichier .ini. Si vous ne configurez pas cette stratégie ici ou dans le fichier .ini, Profile Management n'effectue pas de sauvegarde du fichier NTUSER.DAT.

## Paramètres de stratégie Profils utilisateur streamés

June 27, 2024

Cette section contient des paramètres de stratégie spécifiant la manière dont Profile Management traite les profils utilisateur livrés en streaming.

### Toujours mettre en cache

Ce paramètre spécifie si Profile Management met en cache les fichiers streamés dès que possible après qu'un utilisateur ouvre une session. La mise en cache de fichiers après qu'un utilisateur ouvre une session économise de la bande passante réseau, améliorant ainsi l'expérience utilisateur.

Utilisez ce paramètre avec le paramètre **Streaming des profils**.

Par défaut, ce paramètre est désactivé et les fichiers streamés ne sont pas mis en cache dès que possible après qu'un utilisateur ouvre une session.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, il est désactivé.

### Taille au-delà de laquelle toujours mettre en cache

Ce paramètre spécifie une limite inférieure, en Mo, à la taille des fichiers streamés. Profile Management met en cache les fichiers de taille égale ou supérieure dès que possible après qu'un utilisateur ouvre une session.

Par défaut, la valeur est définie sur 0 (zéro) et la fonctionnalité de mise en cache du profil entier est utilisée. Lorsque la fonctionnalité de mise en cache du profil entier est activée, Profile Management récupère le contenu des profils dans le magasin de l'utilisateur, lorsqu'un utilisateur ouvre une session, en arrière-plan.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, il est désactivé.

### Streaming des profils

Ce paramètre active ou désactive la fonctionnalité de profils utilisateur streamés Citrix. Lorsque cette option est activée, les fichiers et les dossiers de profil sont récupérés du magasin de l'utilisateur vers l'ordinateur local uniquement lorsque les utilisateurs y accèdent après l'ouverture de session. Les entrées de registre et les fichiers dans la zone d'attente sont récupérés immédiatement.

Par défaut, le streaming des profils est désactivé.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ou dans le fichier .ini, il est désactivé.

### Groupes des profils utilisateurs streamés

Ce paramètre spécifie les profils utilisateur qui sont livrés en streaming au sein d'une unité d'organisation, en fonction des groupes d'utilisateurs Windows.

Lorsque ce paramètre est activé, seuls les profils utilisateur dans les groupes d'utilisateurs spécifiés sont livrés en streaming. Tous les autres profils utilisateur sont traités normalement.

Par défaut, ce paramètre est désactivé et tous les profils utilisateur au sein d'une unité d'organisation sont traités normalement.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ni dans le fichier .ini, tous les profils utilisateur sont traités.

### Activer l'exclusion du streaming des profils

Lorsque l'exclusion du streaming des profils est activée :

- Profile Management ne livre pas en streaming les dossiers spécifiés dans la liste d'exclusion.
- Tous les dossiers sont récupérés immédiatement du magasin utilisateur vers l'ordinateur local lorsqu'un utilisateur ouvre une session

Pour de plus amples informations, consultez la section Streamer des profils utilisateur.

### Délai d'expiration des fichiers de verrous de la zone d'attente

Ce paramètre spécifie la période (en jours) après laquelle les fichiers des utilisateurs sont écrits dans le magasin de l'utilisateur à partir de la zone d'attente si le magasin de l'utilisateur reste verrouillé lorsque son serveur de stockage ne répond plus. Ce comportement évite l'engorgement dans la zone d'attente et garantit que le magasin de l'utilisateur contient toujours la dernière version des fichiers.

Par défaut, ce paramètre est défini sur 1 (un) jour.

Si ce paramètre n'est pas configuré ici, la valeur du fichier .ini est utilisée.

Si ce paramètre n'est pas configuré ici ni dans le fichier .ini, la valeur par défaut est utilisée.

#### Activer le streaming de profils pour la zone d'attente

Permet d'activer la fonctionnalité de streaming de profils pour les fichiers et les dossiers dans la zone d'attente.

La zone d'attente est utilisée pour garantir la cohérence du profil lorsque le streaming de profils est activé. Elle stocke temporairement les fichiers et les dossiers de profil modifiés au cours de sessions simultanées.

Par défaut, cette stratégie est désactivée et tous les fichiers et dossiers de la zone d'attente sont récupérés dans le profil local lors de l'ouverture de session. Lorsque cette stratégie est activée, les fichiers de la zone d'attente sont récupérés dans le profil local uniquement lorsqu'ils sont demandés. Utilisez la stratégie avec la stratégie Streaming des profils pour garantir une expérience d'ouverture de session optimale dans les scénarios de sessions simultanées.

La stratégie s'applique aux dossiers de la zone d'attente lorsque la stratégie Activer le streaming de profils pour les dossiers est activée.

## Paramètres de stratégie de couche de personnalisation de l'utilisateur

June 27, 2024

Pour activer le montage des couches utilisateur dans les VDA, utilisez les paramètres de configuration pour spécifier :

- Où accéder aux couches utilisateur sur le réseau.
- À quelle taille les nouveaux disques de couche utilisateur peuvent augmenter.

Ces deux stratégies apparaissent dans la liste des stratégies disponibles :

- Chemin du référentiel de couche utilisateur : entrez un chemin au format « \nom du serveur ou nom du dossier d'adresse » dans le champ Valeur.
- Taille de la couche utilisateur en Go - La taille de couche utilisateur par défaut est de 10 Go, le minimum recommandé par Citrix. Une couche utilisateur est un disque à allocation dynamique qui s'étend à la taille définie au fur et à mesure que l'espace est utilisé. Les couches utilisateur ne diminuent jamais en taille.

> **Remarque :**
>
> L'augmentation de la taille de la couche utilisateur affecte les nouvelles couches utilisateur et étend les couches existantes. La diminution de la taille de la couche n'affecte que les nouvelles couches utilisateur. Les couches utilisateur existantes ne diminuent jamais en taille.

Pour plus d'informations, voir Couche de personnalisation de l'utilisateur.

# Paramètres de stratégie Virtual Delivery Agent

June 27, 2024

La section Virtual Delivery Agent (VDA) contient des paramètres de stratégie qui contrôlent les communications entre le VDA et les contrôleurs d'un site.

Important : le VDA requiert des informations fournies par ces paramètres pour s'enregistrer auprès d'un Delivery Controller, si vous n'utilisez pas la fonctionnalité de mise à jour automatique. Comme ces informations sont requises pour l'enregistrement, vous devez configurer les paramètres suivants avec l'éditeur de stratégie de groupe, à moins que vous ne fournissiez ces informations pendant l'installation du VDA :

- Masque réseau IPv6 d'enregistrement du contrôleur
- Port d'enregistrement du contrôleur
- SID de Contrôleur
- Controller
- Uniquement utiliser l'enregistrement du contrôleur IPv6
- GUID de site

## Masque réseau IPv6 d'enregistrement du contrôleur

Ce paramètre de stratégie permet aux administrateurs de restreindre le VDA uniquement à un sous-réseau favori (plutôt qu'une adresse IP globale, si elle est enregistrée). Ce paramètre spécifie l'adresse IPv6 et le réseau où le VDA s'enregistre. Le VDA s'enregistre uniquement sur la première adresse qui correspond au masque de sous-réseau spécifié. Ce paramètre est uniquement valide si le paramètre de stratégie Uniquement utiliser l'enregistrement du contrôleur IPv6 est activé.

Par défaut, ce paramètre est vide.

## Port d'enregistrement du contrôleur

Utilisez ce paramètre uniquement si le paramètre de stratégie **Activer la mise à jour automatique des contrôleurs** est désactivé.

Ce paramètre spécifie le numéro de port TCP/IP que le VDA utilise pour s'enregistrer auprès d'un Controller, en cas d'utilisation de l'enregistrement basé sur le registre.

Le numéro port est défini par défaut sur 80.

### SID de Contrôleur

Utilisez ce paramètre uniquement si le paramètre de stratégie **Activer la mise à jour automatique des contrôleurs** est désactivé.

Ce paramètre spécifie une liste d'identificateurs de sécurité (SID) de Controller séparés par des espaces que le VDA utilise pour s'enregistrer auprès d'un Controller, en cas d'utilisation de l'enregistrement basé sur le registre. Il s'agit d'un paramètre facultatif, qui peut être utilisé avec le paramètre **Contrôleurs** pour limiter la liste des contrôleurs utilisés pour l'enregistrement.

Par défaut, ce paramètre est vide.

### Controller

Utilisez ce paramètre uniquement si le paramètre de stratégie **Activer la mise à jour automatique des contrôleurs** est désactivé.

Ce paramètre spécifie une liste de noms de domaines complets (FQDN) de contrôleurs séparés par des espaces que le VDA utilise pour s'enregistrer auprès d'un Controller, en cas d'utilisation de l'enregistrement basé sur le registre. Il s'agit d'un paramètre facultatif, qui peut être utilisé avec le paramètre **SID de Controller**.

Par défaut, ce paramètre est vide.

### Activer la mise à jour automatique des contrôleurs

Ce paramètre permet d'activer le VDA pour s'enregistrer auprès d'un Controller automatiquement après l'installation.

Après l'enregistrement du VDA, le Controller auquel il s'enregistre envoie une liste des domaines complets (FQDN) et le SID de ce contrôleur au VDA Le VDA inscrit cette liste dans le stockage permanent. Chaque Controller vérifie également la base de données du site toutes les 90 minutes pour obtenir des informations de Controller. Le Controller envoie des listes mises à jour à ses VDA enregistrés si l'une des situations suivantes se produit :

- Un Controller a été ajouté ou retiré depuis la dernière vérification
- Un changement de stratégie s'est produit

Le VDA accepte les connexions provenant de tous les Controller figurant dans la dernière liste reçue.

Ce paramètre est activé par défaut.

### Uniquement utiliser l'enregistrement du contrôleur IPv6

Ce paramètre détermine le format d'adresse utilisé par le VDA pour s'enregistrer avec le Controller :

- lorsque cette option est activée, le VDA s'enregistre auprès du Controller à l'aide de l'adresse IPv6 de la machine. Lorsque le VDA communique avec le Controller, il utilise l'ordre d'adresse suivant : adresse IP globale, adresse locale unique (ULA), adresse locale au lien (si aucune autre adresse IPv6 n'est disponible).
- Lorsque cette stratégie est désactivée, le VDA s'enregistre et communique avec le Controller à l'aide de l'adresse IPv4 de la machine.

Par défaut, ce paramètre est désactivé.

### GUID de site

Utilisez ce paramètre uniquement si le paramètre de stratégie **Activer la mise à jour automatique des contrôleurs** est désactivé.

Ce paramètre spécifie le GUID (Globally Unique Identifier) du site que le VDA utilise pour s'enregistrer auprès d'un Controller en cas d'utilisation de l'enregistrement à partir d'Active Directory.

Par défaut, ce paramètre est vide.

## Paramètres de stratégie HDX 3D Pro

June 27, 2024

La section HDX 3D Pro contient des paramètres de stratégie permettant d'activer et de configurer l'outil de configuration de la qualité d'image pour vos utilisateurs. Cet outil permet aux utilisateurs d'optimiser l'utilisation de la bande passante disponible. Pour cette optimisation, l'équilibre entre qualité d'image et réactivité est ajusté en temps réel.

### Activer sans perte

Ce paramètre détermine si les utilisateurs peuvent ou non activer ou désactiver la compression sans perte à l'aide de l'outil de configuration de la qualité d'image. Par défaut, les utilisateurs n'ont pas la possibilité d'activer la compression sans perte.

Supposons qu'un utilisateur active la compression sans perte. Dans ce cas, la qualité d'image est automatiquement définie sur la valeur maximale disponible dans l'outil de configuration de la qualité

d'image. Par défaut, il est possible d'utiliser la compression basée sur le processeur graphique ou sur l'UC, en fonction des possibilités de la machine utilisateur et de l'ordinateur hôte.

### Paramètres de qualité HDX 3D Pro

Ce paramètre spécifie les valeurs minimale et maximale disponibles pour les utilisateurs dans l'outil de configuration de la qualité d'image. En utilisant ces valeurs, les utilisateurs peuvent définir la plage de réglage de la qualité d'image dans l'outil de configuration de la qualité d'image.

Indiquez des valeurs de qualité entre 0 et 100 (inclus). La valeur maximale doit être supérieure ou égale à la valeur minimale.

## Paramètres de stratégie Surveillance

June 27, 2024

La section **Surveillance** contient des paramètres de stratégie pour la surveillance des processus, des ressources et des échecs d'application.

La portée de ces stratégies peut être définie sur la base des éléments suivants :

- Site
- Le groupe de mise à disposition
- Type de groupe de mise à disposition
- Unité d'organisation
- Balises

### Stratégies pour la surveillance des processus et des ressources

Chaque point de données pour l'UC, la mémoire et les processus est collecté depuis le VDA et stocké dans la base de données de surveillance. L'envoi de points de données depuis le VDA consomme de la bande passante réseau et leur stockage occupe énormément d'espace dans la base de données de surveillance. Supposons que vous ne souhaitez pas surveiller les données de ressources ou les données de processus ou les deux pour une portée spécifique. Par exemple, un groupe de mise à disposition ou une unité organisationnelle spécifique. Dans ce cas, il est recommandé de désactiver la stratégie.

#### Activer le suivi des processus

Activez ce paramètre pour autoriser le suivi des processus en cours d'exécution sur des machines avec VDA. Les statistiques telles que l'utilisation d'UC et de mémoire sont envoyées au service de surveillance. Les statistiques sont utilisées à des fins de notification en temps réel et pour générer des rapports historiques dans Director.

Par défaut, ce paramètre est désactivé.

#### Activer le suivi des ressources

Activez ce paramètre pour permettre le suivi des compteurs de performance critiques sur les machines équipées de VDA. Les statistiques (telles que l'utilisation d'UC et de mémoire, les données de nombre d'E/S par seconde et de latence de disque) sont envoyées au service de surveillance. Les statistiques sont utilisées à des fins de notification en temps réel et pour générer des rapports historiques dans Director.

Par défaut, ce paramètre est activé.

#### Scalabilité

Les données du processeur et de la mémoire sont transmises à la base de données à partir de chaque VDA à des intervalles de 5 minutes. Les données de processus (si cette option est activée) sont transmises à la base de données à des intervalles de 10 minutes. Les données d'E/S par seconde et de latence de disque sont transmises à la base de données à intervalles réguliers d'1 heure.

#### Données d'UC et de mémoire

Les données d'UC et de mémoire sont **activées** par défaut. Les valeurs de rétention des données sont les suivantes (licence Platinum) :

| Granularité des données | Nombre de jours |
|---|---|
| 5 minutes | 1 jour |
| 10 minutes | 7 jours |
| 1 heure | 30 jours |
| 1 jour | 90 jours |

**Données E/S par seconde et latence de disque**

Les données E/S par seconde et latence de disque sont **activées** par défaut. Les valeurs de rétention des données sont les suivantes (licence Platinum) :

| Granularité des données | Nombre de jours |
|---|---|
| 1 heure | 3 jours |
| 1 jour | 90 jours |

Avec les paramètres de rétention des données, environ 276 Ko d'espace disque sont nécessaires pour stocker les éléments suivants pour un VDA sur une période d'un an :

- UC
- Memory
- E/S par seconde
- Données sur la latence de disque

| Nombre de machines | Stockage requis (valeur approximative) |
|---|---|
| 1 | 276 Ko |
| 1 K | 270 Mo |
| 40 K | 10,6 Go |

**Données de processus**

Les données de processus sont **désactivées** par défaut. Il est recommandé d'activer les données de processus sur un sous-ensemble de machines si nécessaire. Les paramètres de rétention des données par défaut sont les suivants :

| Granularité des données | Nombre de jours |
|---|---|
| 10 minutes | 1 jour |
| 1 heure | 7 jours |

Si les données de processus sont activées, avec les paramètres de rétention par défaut, les données de processus pourraient utiliser environ 1,5 Mo par VDA et 3 Mo par VDA Terminal Services (VDA TS) sur une période d'un an.

| Nombre de machines | Stockage requis pour VDA (valeur approximative) | Stockage requis pour VDA TS (valeur approximative) |
|---|---|---|
| 1 | 1,5 Mo | 3 Mo |
| 1 K | 1,5 Go | 3 Go |

> **Remarque :**
>
> Les chiffres fournis précédemment n'incluent pas l'espace Index. Et tous les calculs sont approximatifs et varient en fonction du déploiement.

#### Configurations facultatives

Vous pouvez modifier les paramètres de rétention par défaut en fonction de vos besoins. Toutefois, cette configuration consomme davantage de stockage. En activant les paramètres ci-dessous, vous pouvez obtenir plus de précision dans les données d'utilisation des processus. Les configurations pouvant être activées sont les suivantes :

**EnableMinuteLevelGranularityProcessUtilization**

**EnableDayLevelGranularityProcessUtilization**

Ces configurations peuvent être activées à partir de l'applet de commande PowerShell : Set-MonitorConfiguration

### Stratégies pour la détection des défaillances applicatives

Par défaut, l'onglet **Échec applicatifs** affiche uniquement les échecs applicatifs de VDA avec OS multi-session. Les paramètres de détection des défaillances applicatives peuvent être modifiés avec les stratégies de surveillance suivantes :

#### Activer la détection des défaillances applicatives

Utilisez ce paramètre pour configurer la surveillance d'échecs applicatifs pour détecter les erreurs ou les défaillances d'application (plantages et exceptions non prises en charge) ou les deux.
Désactivez la détection des défaillances applicatives en définissant **Valeur** sur **Aucun**.
La valeur par défaut pour ce paramètre est Défaillances applicatives uniquement.

#### Activer la détection des défaillances applicatives sur les VDA avec OS mono-session

Par défaut, seuls les échecs d'applications hébergées sur des VDA avec OS multi-session sont détectés. Pour contrôler les VDA avec OS mono-session, définissez la stratégie sur **Autorisé**.
La valeur par défaut est **Interdit**.

#### Liste des applications exclues de la détection des défaillances

Spécifiez une liste des applications qui ne doivent pas être contrôlées.
Par défaut, cette liste est vide.

### Stratégie de collecte de données pour la fonction Analytics

#### Collecte de données VDA pour la fonction Analytics

Utilisez la stratégie pour activer ou désactiver le service de surveillance afin qu'il collecte des mesures liées aux performances et à la sécurité des VDA pour la fonction Performance and Security Analytics. Par défaut, la stratégie est définie sur **Autorisé**. Définissez la stratégie sur **Interdit** pour arrêter la collecte de données des VDA.

#### Collecte de métadonnées en presse-papiers pour la surveillance de la sécurité

Utilisez cette stratégie pour activer ou désactiver la collecte de métadonnées en presse-papiers par Broker Service à des fins de surveillance de la sécurité, d'audit et de conformité. Cette stratégie est **activée** par défaut. Définissez la stratégie sur **Désactivé** pour arrêter la collecte de données des VDA.

#### Collecte de données diagnostiques pour le suivi des performances

Utilisez cette stratégie pour permettre au service de surveillance de collecter des données de diagnostic telles que les informations de session, l'état des services User Profile Manager/Suivi de l'expérience utilisateur, l'optimisation de Microsoft Teams et les protocoles de connexion. Cette stratégie est **activée** par défaut. Définissez la stratégie sur **Désactivé** pour arrêter la collecte de données des VDA.

### Conseils pour la planification du stockage

**Stratégie de groupe**. Si vous ne souhaitez pas surveiller les données de ressources ou de processus, vous pouvez les désactiver à l'aide de la stratégie de groupe. Pour de plus amples informations, consultez la section **Stratégie de groupe** de Créer des stratégies.

**Nettoyage des données**. Les paramètres de rétention des données par défaut peuvent être modifiés pour nettoyer les données et libérer de l'espace de stockage. Pour de plus amples informations sur les paramètres de nettoyage, consultez la section Granularité de données et rétention dans Accès aux données à l'aide de l'API.

## Paramètres de stratégie Adresse IP virtuelle

June 27, 2024

> **Important :**
>
> - Windows 10 Enterprise multi-sessions ne prend pas en charge Remote Desktop IP Virtualization (Virtual IP) et nous ne prenons pas en charge Remote Desktop IP Virtualization ni Virtual Loopback sur Windows 10 Enterprise multi-sessions.
> - Remote Desktop IP Virtualization (Virtual IP) n'est pas pris en charge sur les machines hébergées dans le cloud. Pour de plus amples informations, consultez la documentation de Microsoft.

La section **Adresse IP virtuelle** contient des paramètres de stratégie permettant de contrôler si les sessions ont leur propre adresse virtuelle de bouclage.

### Prise en charge du bouclage d'adresse IP virtuelle

Lorsque ce paramètre est activé, chaque session possède sa propre adresse virtuelle de bouclage. Lorsqu'il est désactivé, les sessions n'ont pas d'adresses de bouclage individuelles.

Par défaut, ce paramètre est désactivé.

### Liste de programmes de bouclage virtuel d'adresse IP virtuelle

Ce paramètre spécifie les exécutables d'application susceptibles d'utiliser les adresses de bouclage virtuelles. Lorsque vous ajoutez des programmes à la liste, spécifiez uniquement le nom de l'exécutable. Il n'est pas nécessaire de spécifier le chemin d'accès complet.

Par défaut, aucun exécutable n'est spécifié.

# Configurer les paramètres de redirection du port COM et LPT à l'aide du Registre

June 27, 2024

Dans les versions VDA 7.0 à 7.8, les paramètres du **port COM et LPT** sont uniquement configurables à l'aide du Registre. Pour les versions VDA antérieures à la version 7.0 et les VDA 7.9 et versions ultérieures, ces paramètres sont configurables dans Web Studio. Pour de plus amples informations, consultez la section Paramètres de stratégie de redirection de port et Paramètres de stratégie de bande passante.

Les paramètres de stratégie pour la redirection du port COM et du port LPT sont situés sous HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated sur l'image ou la machine VDA.

Pour activer la redirection des ports COM et LPT, ajoutez de nouvelles clés de Registre de type REG_DWORD, comme suit :

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

| Clé de registre | Description | Valeurs autorisées |
|---|---|---|
| AllowComPortRedirection | Autoriser ou interdire la redirection de port COM | 1 (Autoriser) ou 0 (Interdire) |
| LimitComBw | Limite de bande passante pour le canal de redirection du port COM | Valeur numérique |
| LimitComBWPercent | Limite de bande passante pour le canal de redirection du port COM sous forme de pourcentage de la bande passante totale de session | Valeur numérique comprise entre 0 et 100 |
| AutoConnectClientComPorts | Connecter automatiquement les ports COM de la machine utilisateur | 1 (Autoriser) ou 0 (Interdire) |
| AllowLptPortRedirection | Autoriser ou interdire la redirection de port LPT | 1 (Autoriser) ou 0 (Interdire) |

| Clé de registre | Description | Valeurs autorisées |
|---|---|---|
| LimitLptBw | Limite de bande passante pour le canal de redirection du port LPT | Valeur numérique |
| LimitLptBwPercent | Limite de bande passante pour le canal de redirection du port LPT sous forme de pourcentage de la bande passante totale de session | Valeur numérique comprise entre 0 et 100 |
| AutoConnectClientLptPorts | Connecter automatiquement les ports LPT de la machine utilisateur | 1 (Autoriser) ou 0 (Interdire) |

Après la configuration de ces paramètres, modifiez les catalogues de machines pour utiliser la nouvelle image principale ou la machine physique mise à jour. Les bureaux sont mis à jour avec les nouveaux paramètres lors de la fermeture de session suivante.

## Paramètres de stratégie de Connector pour Configuration Manager 2012

June 27, 2024

La section Connector pour Configuration Manager 2012 contient des paramètres de stratégie pour la configuration de l'agent Citrix Connector 7.5.

> **Important :**
>
> Les stratégies d'avertissement, de fermeture de session et de message de redémarrage s'appliquent uniquement aux déploiements de catalogues de machines avec OS multi-session qui sont gérés manuellement ou par Provisioning Services Pour ces catalogues de machines, le service Connector alerte les utilisateurs lorsqu'ils sont en attente d'une installation d'application ou de mises à jour logicielles.

Pour les catalogues gérés par MCS, utilisez Web Studio pour avertir les utilisateurs. Pour gérer des catalogues avec OS mono-session manuellement, utilisez le gestionnaire de configuration pour avertir les utilisateurs. Pour des catalogues avec OS mono-session gérés par Provisioning Services, utilisez Provisioning Services pour avertir les utilisateurs.

### Intervalle des fréquences d'avertissement

Ce paramètre définit l'intervalle entre les apparitions du message d'avertissement auprès des utilisateurs.

Les intervalles sont définis selon le format jjj.hh:mm:ss, où :

- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heures avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

Par défaut, le paramètre d'intervalle est de 1 heure (01:00:00).

### Texte du corps de la zone de message d'avertissement

Ce paramètre contient le texte modifiable du message qui avertit les utilisateurs de mises à jour logicielles ou de tâches de maintenance à venir nécessitant qu'ils ferment leur session.

Par défaut, le message est : {TIMESTAMP} Save your work. Le serveur est placé en mode déconnecté à des fins de maintenance dans {TIMELEFT}.

### Titre de la zone de message d'avertissement

Ce paramètre contient le texte modifiable de la barre de titre du message d'avertissement pour les utilisateurs.

Par défaut, le titre est Upcoming Maintenance.

### Période d'avertissement

Ce paramètre définit combien de temps avant la maintenance où le premier message d'avertissement s'affiche.

Le temps est défini selon le format jjj.hh:mm:ss, où :

- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heures avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

Par défaut, le paramètre est de 16 heures (16:00:00), ce qui indique que le premier message d'avertissement s'affiche approximativement 16 heures avant la maintenance.

### Texte du corps de la zone de message de fermeture de session forcée finale

Ce paramètre contient le texte modifiable du message alertant les utilisateurs qu'une ouverture de session forcée a commencé.

Par défaut, le message est : The server is currently going offline for maintenance (Le serveur est actuellement en mode déconnecté pour maintenance).

### Titre de la zone de message de fermeture de session forcée finale

Ce paramètre contient le texte modifiable de la barre de titre du message final de fermeture de session forcée.

Par défaut, le titre est : Notification From IT Staff (Notification du personnel informatique).

### Obliger la fermeture de session de la période de grâce

Ce paramètre définit le délai entre la notification de fermer leur session aux utilisateurs et l'implémentation de la fermeture de session forcée pour traiter la maintenance en attente.

Le temps est défini selon le format jjj.hh:mm:ss, où :

- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heures avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

Par défaut, le paramètre force logoff grace period est de 5 minutes (00:05:00).

### Texte du corps de la zone de message de fermeture de session forcée

Ce paramètre contient le texte modifiable du message demandant aux utilisateurs d'enregistrer leur travail et de fermer leur session avant de démarrer une fermeture de session forcée.

Par défaut, le message contient ce qui suit : {TIMESTAMP}Save your work and log off (Veuillez enregistrer votre travail et fermer votre session). Le serveur est placé en mode déconnecté à des fins de maintenance dans {TIMELEFT}.

### Titre de la zone de message de fermeture de session forcée

Ce paramètre contient le texte modifiable de la barre de titre du message de fermeture de session forcée.

Par défaut, le titre est : Notification From IT Staff (Notification du personnel informatique).

### Mode d'image gérée

L'agent Connector détecte automatiquement s'il est en cours d'exécution sur une machine clone gérée par Provisioning Services ou MCS. L'agent bloque de l'agent les mises à jour Configuration Manager sur les clones dont l'image est gérée et installe automatiquement les mises à jour sur l'image principale du catalogue.

Après mise à jour d'une image principale, utilisez Web Studio pour orchestrer le redémarrage des clones de catalogue MCS. L'Agent du Connector orchestre automatiquement le redémarrage des clones du catalogue PVS lors des fenêtres de maintenance Configuration Manager. Pour remplacer ce comportement afin que le logiciel soit installé sur des clones de catalogue par Configuration Manager, changez le mode Image gérée en Désactivé.

### Texte du corps de la zone de message de redémarrage

Ce paramètre contient le texte modifiable du message notifiant les utilisateurs lorsque le serveur est sur le point d'être redémarré.

Par défaut, le message est : The server is currently going offline for maintenance (Le serveur est actuellement en mode déconnecté pour maintenance).

### Intervalle de temps régulier durant lequel la tâche d'agent doit être exécutée

Ce paramètre détermine la fréquence d'exécution de la tâche d'agent Citrix Connector.

Le temps est défini selon le format jjj.hh:mm:ss, où :

- jjj représente les jours, un paramètre facultatif, avec une plage de 0 à 999.
- hh représente les heures avec une plage de 0 à 23.
- mm représente les minutes avec une plage de 0 à 59.
- ss représente les secondes avec une plage de 0 à 59.

Par défaut, le paramètre d'intervalle de temps régulier est de 5 minutes (00:05:00).

## Gérer

June 27, 2024

La gestion d'un site Citrix Virtual Apps and Desktops couvre divers éléments et tâches.

**Gestion des licences**

Une connexion valide avec le serveur de licences Citrix est requise lorsque vous créez un site. Plus tard, vous pourrez effectuer plusieurs opérations de gestion de licences à partir de Studio, y compris l'ajout de licences, la modification des types ou modèles de licences et la gestion des administrateurs de licences. Vous pourrez également accéder à la console License Administration Console à partir de Studio.

### Applications

Permet de gérer les applications dans les groupes de mise à disposition et éventuellement, les groupes d'applications.

### Zones

Dans un déploiement réparti sur différents sites géographiques, vous pouvez utiliser des zones pour que les applications et les bureaux se trouvent à proximité des utilisateurs finaux, ce qui peut améliorer les performances. Lorsque vous installez et configurez un site, tous les Controller, les catalogues de machines et les connexions hôtes se trouvent dans une zone principale. Plus tard, vous pourrez utiliser Studio pour créer des zones satellite contenant ces éléments. Une fois que votre site comporte plusieurs zones, vous pouvez indiquer dans quelle zone les catalogues de machines et les connexions hôtes créés ou les Controller ajoutés doivent être placés. Vous pouvez aussi déplacer les éléments entre les zones.

### Connexions et ressources

Si vous utilisez un hyperviseur ou un autre service pour héberger les machines qui mettent à disposition les applications et les bureaux auprès des utilisateurs, vous devez créer votre première connexion à l'hyperviseur ou à un autre service lorsque vous créez un site. Les détails de stockage et de réseau constituent les ressources de cette connexion. Plus tard, vous pourrez modifier la connexion et ses ressources, et créer des connexions supplémentaires. Vous pourrez également gérer les machines qui utilisent une connexion configurée.

### Cache d'hôte local

Le cache d'hôte local permet aux opérations de négociation de connexion d'un site de se poursuivre lorsque la connexion entre un Delivery Controller et la base de données du site échoue.

### IP virtuelle et boucle virtuelle

La fonctionnalité d'adresse IP virtuelle Microsoft fournit une application publiée avec une adresse IP unique attribuée dynamiquement à chaque session. La fonctionnalité de bouclage virtuel Citrix vous permet également de configurer des applications qui dépendent des communications avec localhost pour utiliser une adresse de bouclage virtuel unique dans la plage localhost.

### Delivery Controller

Cet article décrit les considérations et procédures lors de l'ajout et de la suppression de Controller à partir d'un site. Il décrit également comment déplacer des Controller vers une autre zone ou un autre site et comment déplacer un VDA vers un autre site.

### Enregistrement d'un VDA auprès de Delivery Controller

Avant qu'un VDA puisse effectuer la mise à disposition d'applications et de bureaux, il doit s'enregistrer (établir la communication) auprès d'un Controller. Les adresses de Controller peuvent être spécifiées de plusieurs façons, lesquelles sont décrites dans cet article. Il est d'une importance critique que les VDA obtiennent des informations actualisées au fur et à mesure que des Controller sont ajoutés, déplacés et supprimés sur le site.

### Sessions

La gestion de l'activité de session est critique pour offrir la meilleure expérience utilisateur possible. Plusieurs fonctionnalités peuvent optimiser la fiabilité des sessions, réduire les désagréments, les temps d'arrêt et la perte de productivité.

- Fiabilité de session
- Reconnexion automatique des clients
- Persistance ICA
- Contrôle de l'espace de travail
- Itinérance de session

### Utiliser la fonction de recherche dans Studio

Lorsque vous souhaitez afficher des informations sur les machines, sessions, catalogues de machines, applications ou groupes de mise à disposition dans Studio, vous pouvez utiliser la fonctionnalité de recherche flexible.

### Balises

Utilisez des balises pour identifier des éléments tels que des machines, applications, groupes et stratégies. Vous pouvez ensuite configurer certaines opérations pour qu'elles s'appliquent aux éléments avec une balise spécifique.

### IPv4/IPv6

Citrix Virtual Apps and Desktops prend en charge les déploiements IPv4 purs, IPv6 purs et double pile qui utilisent des réseaux IPv4 et IPv6 qui se chevauchent. Cet article décrit et illustre ces déploiements. Il décrit également les paramètres de stratégie Citrix qui contrôlent l'utilisation de IPv4 ou IPv6.

### Profils utilisateur

Par défaut, Citrix Profile Management est installé automatiquement lorsque vous installez un VDA. Si vous utilisez cette solution de profil, consultez cet article pour obtenir des informations générales. Pour plus d'informations, veuillez consulter la documentation de Profile Management.

#### Collecte de traces CDF (Citrix Diagnostic Facility)

L'utilitaire CDFControl est un contrôleur ou un consommateur de traçage d'événements permettant de capturer les messages de trace CDF (Citrix Diagnostic Facility) affichés à partir de divers four-

nisseurs de trace Citrix. Il est conçu pour résoudre les problèmes complexes liés à Citrix, analyser la prise en charge des filtres et collecter des données de performances.

### Citrix Insight Services

Citrix Insight Services (CIS) est une plate-forme Citrix depuis laquelle vous pouvez générer des informations d'instrumentation, de télémétrie et autres données stratégiques.

#### Citrix Scout

Citrix Scout collecte des diagnostics et effectue des contrôles d'intégrité. Vous pouvez utiliser les résultats à des fins de maintenance proactive dans votre déploiement Citrix Virtual Apps and Desktops. Citrix offre une analyse complète et automatique des collectes de diagnostics via Citrix Insight Services. Vous pouvez également utiliser Scout pour résoudre les problèmes, vous-même ou avec des instructions de l'assistance Citrix.

## Applications

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

### Introduction

Si votre déploiement utilise uniquement des groupes de mise à disposition (et aucun groupe d'applications), vous devez ajouter des applications aux groupes de mise à disposition. Si vous disposez également de groupes d'application, vous ajoutez, en règle générale, des applications aux groupes d'applications. Ces recommandations permettent de faciliter l'administration. Une application doit toujours appartenir à au moins un groupe de mise à disposition ou groupe d'applications.

Dans l'assistant Ajouter des applications, vous pouvez sélectionner un ou plusieurs groupes de mise à disposition, ou un ou plusieurs groupes d'applications, mais pas les deux. Bien que vous puissiez par la suite modifier l'association à un groupe d'applications (par exemple, transférer une application d'un groupe d'applications sur un groupe de mise à disposition), cela n'est pas recommandé pour des raisons de complexité. Gardez vos applications dans un type de groupe.

Lorsque vous associez une application à plusieurs groupes, vous risquez de rencontrer un problème de visibilité si vous ne disposez pas d'autorisations suffisantes pour afficher l'application dans tous

ces groupes. Dans de tels cas, consultez un administrateur disposant des autorisations appropriées ou demandez une extension de vos autorisations à tous les groupes auxquels l'application est associée.

Si vous publiez deux applications du même nom (peut-être de différents groupes) vers les mêmes utilisateurs, modifiez la propriété `Application name (for user)` dans Web Studio. Sinon, des noms en double s'affichent dans l'application Citrix Workspace.

Vous pouvez modifier les propriétés d'une application (paramètres) lorsque vous l'ajoutez ou ultérieurement. Vous pouvez également modifier le dossier dans lequel l'application est placée, lorsque vous ajoutez l'application, ou ultérieurement.

Pour plus de détails, consultez :

- Créer des groupes de mise à disposition
- Créer des groupes d'applications
- Balises

### Ajouter des applications

Vous pouvez ajouter des applications lorsque vous créez un groupe de mise à disposition ou un groupe d'applications. Ces procédures sont détaillées dans Créer des groupes de mise à disposition et Créer des groupes d'applications. La procédure suivante explique comment ajouter des applications après la création d'un groupe.

À savoir :

- vous ne pouvez pas ajouter d'applications aux groupes de mise à disposition Remote PC Access.
- Vous ne pouvez pas utiliser l'assistant Ajouter une application pour supprimer des applications de groupes de mise à disposition ou de groupes d'applications. Il s'agit d'une opération distincte.

Pour ajouter une ou plusieurs applications :

1. Sélectionnez **Applications** dans le volet de gauche, puis sélectionnez **Ajouter des applications** dans la barre d'actions.
2. L'assistant Ajouter des applications s'ouvre avec une page **Introduction**, que vous pouvez supprimer des lancements ultérieurs de cet assistant.
3. L'assistant vous guide à travers les pages **Groupes**, **Applications**, et **Résumé**. Lorsque vous avez terminé chaque page, cliquez sur **Suivant** jusqu'à la page **Résumé**.

Alternatives à l'étape 1 si vous souhaitez ajouter des applications à un seul groupe de mise à disposition ou groupe d'applications :

- **Pour ajouter des applications à un seul groupe de mise à disposition,** à l'étape 1, sélectionnez **Groupes de mise à disposition** dans le volet gauche de Web Studio, sélectionnez un groupe de mise à disposition dans le volet du milieu, puis sélectionnez **Ajouter des applications** dans la barre d'actions. L'assistant n'affiche pas la page **Groupes**.
- **Pour ajouter des applications à un seul groupe d'applications,** à l'étape 1, sélectionnez **Applications** dans le volet gauche de Web Studio, sélectionnez un groupe d'applications dans le volet du milieu, puis sélectionnez **Ajouter des applications** sous le nom du groupe dans la barre d'actions. L'assistant n'affiche pas la page **Groupes**.

#### Page Groupes

Cette page dresse la liste de tous les groupes de mise à disposition dans le site. Si vous avez également créé des groupes d'applications, la page dresse la liste des groupes d'applications et des groupes de mise à disposition. Vous pouvez choisir dans l'un ou l'autre des groupes, mais pas dans les deux groupes. En d'autres termes, vous ne pouvez pas ajouter d'applications à un groupe d'applications et à un groupe de mise à disposition. En général, si vous utilisez des groupes d'application, ajoutez les applications à des groupes d'applications plutôt qu'à des groupes de mise à disposition.

Lorsque vous ajoutez une application, activez la case à cocher en regard d'au moins un groupe de mise à disposition (ou un groupe d'applications, le cas échéant). Chaque application doit toujours être associée à au moins un groupe.

#### Page Applications

Cliquez sur **Ajouter** pour afficher les sources des applications.

- **À partir du menu Démarrer :** applications qui sont découvertes sur une machine dans les groupes de mise à disposition sélectionnés. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**.

  Cette source ne peut pas être sélectionnée si vous avez (1) sélectionné des groupes d'applications qui ne sont associés à aucun groupe de mise à disposition, (2) sélectionné des groupes d'applications avec des groupes de mise à disposition associés qui ne contiennent aucune machine, ou (3) sélectionné un groupe de mise à disposition ne contenant aucune machine.
- **Manuellement :** applications situées sur un VDA dans le groupe de mise à disposition ou à un autre endroit de votre réseau. La sélection de cette source ouvre une nouvelle page dans laquelle vous pouvez spécifier l'application à ajouter de la manière suivante :
  - Saisissez le chemin d'accès de l'exécutable, le répertoire de travail, les arguments de la

ligne de commande (facultatifs), et les noms affichés des administrateurs et des utilisateurs.

- Sélectionnez une application à partir d'un VDA dans le groupe de mise à disposition. Pour ce faire, cliquez sur **Parcourir**, entrez les informations d'identification pour accéder au VDA, attendez d'être connecté au VDA, puis sélectionnez une application depuis le VDA. Les propriétés de l'application sélectionnée renseignent automatiquement les champs de la page.

- **Existantes :** applications déjà ajoutées au site. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des applications découvertes. Sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**.

  Cette source ne peut pas être sélectionnée si le site ne dispose d'aucune application.

- **App-V :** applications dans des packages App-V. Lorsque vous sélectionnez cette source, une nouvelle page s'affiche dans laquelle vous pouvez sélectionner le serveur App-V ou la bibliothèque d'applications. À partir de l'écran qui s'affiche, sélectionnez les cases à cocher des applications à ajouter, puis cliquez sur **OK**. Pour plus d'informations, consultez la section Déployer et fournir des applications App-V.

  Cette source ne peut pas être sélectionnée lorsque App-V n'est pas configuré pour le site.

- **Groupe d'applications :** groupes d'applications. Lorsque vous sélectionnez cette source, une nouvelle page se lance avec une liste des groupes d'applications. (Bien que l'affichage dresse également la liste des applications de chaque groupe, vous ne pouvez sélectionner que le groupe, et non pas des applications individuelles.) Toutes les applications actuelles et futures dans les groupes sélectionnés sont ajoutées. Sélectionnez les cases à cocher des groupes d'applications à ajouter, puis cliquez sur **OK**.

  Cette source ne peut pas être sélectionnée s'il (1) n'existe aucun groupe d'applications, ou (2) si les groupes de mise à disposition sélectionnés ne prennent pas en charge les groupes d'applications (par exemple, les groupes de mise à disposition avec des machines attribuées de manière statique).

Comme indiqué dans le tableau, certaines sources dans la liste **Ajouter** ne peuvent pas être sélectionnées s'il n'existe source valide de ce type. Les sources qui ne sont pas compatibles (par exemple, vous ne pouvez pas ajouter des groupes d'applications à des groupes d'applications) ne sont pas incluses dans la liste. Les applications qui ont déjà été ajoutées aux groupes que vous avez choisis ne peuvent pas être sélectionnées.

Vous pouvez modifier les propriétés d'une application (paramètres) sur cette page ou ultérieurement.

Par défaut, les applications ajoutées sont placées dans le dossier d'application nommé `Applications`. Vous pouvez modifier l'application sur cette page ou ultérieurement. Si vous essayez d'ajouter une

application et qu'une application avec le même nom existe dans le même dossier, vous êtes invité à renommer l'application que vous ajoutez. Vous pouvez accepter le nouveau nom proposé ou refuser et renommer l'application, ou sélectionner un autre dossier. Par exemple, si `app` existe déjà dans le dossier **Applications**, et que vous essayez d'ajouter une autre application appelée `app` à ce dossier, le nouveau nom proposé sera `app_1`.

#### Page de résumé

Si vous ajoutez 10 applications ou moins, leurs noms sont répertoriés dans **Applications à ajouter**. Si vous ajoutez plus de 10 applications, le nombre total est spécifié.

Consultez les informations récapitulatives, puis cliquez sur **Terminer**.

### Modifier l'association d'un groupe d'applications

Après l'ajout d'une application, vous pouvez modifier les groupes de mise à disposition et groupes d'applications auxquels l'application est associée.

Vous pouvez faire glisser une application vers un autre groupe. Ceci est une alternative à l'utilisation des commandes dans la barre d'actions.

Si une application est associée à plus d'un groupe de mise à disposition ou plus d'un groupe d'applications, la priorité attribuée au groupe est utilisée pour spécifier l'ordre dans lequel plusieurs groupes sont vérifiés afin de trouver des applications. Par défaut, tous les groupes ont la priorité 0 (priorité la plus élevée). La charge des groupes ayant le même niveau de priorité est équilibrée.

Une application peut être associée à des groupes de mise à disposition contenant des machines partagées (non privées) qui peuvent mettre à disposition des applications. Vous pouvez également sélectionner des groupes de mise à disposition contenant des machines partagées qui mettent uniquement à disposition des bureaux, si (1) le groupe de mise à disposition contient des machines partagées et a été créé avec une version de XenDesktop 7.x antérieure à 7.9, et (2) vous disposez de l'autorisation `Edit delivery group`. Le type de groupe de mise à disposition est automatiquement converti en `desktops and applications` lorsque la boîte de dialogue des propriétés est validée.

1. Connectez-vous à Web Studio, sélectionnez **Applications** dans le volet de gauche, puis sélectionnez l'application.
2. Sélectionnez **Propriétés** dans la barre d'actions.
3. Sélectionnez la page **Groupes**.

    - Pour ajouter un groupe, cliquez sur **Ajouter** et sélectionnez **Groupes d'applications** ou **Groupes de mise à disposition**. (Si vous n'avez pas créé de groupes d'applications, la seule entrée est **Groupes de mise à disposition**). Puis sélectionnez un ou plusieurs

groupes disponibles. Les groupes qui ne sont pas compatibles avec l'application, ou qui sont déjà associés à l'application ne peuvent pas être sélectionnés.
- Pour supprimer un groupe, sélectionnez un ou plusieurs groupes, puis cliquez sur **Supprimer**. Si la suppression de l'association de groupe a pour conséquence que l'application n'est plus être associée à un groupe, vous êtes averti que l'application va être supprimée.
- Pour modifier la priorité des groupes de mise à disposition, sélectionnez le groupe, puis cliquez sur **Modifier la priorité**. Sélectionnez une valeur de priorité puis cliquez sur **OK**.

4. Lorsque vous avez terminé, cliquez sur **Appliquer** pour appliquer les modifications et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

### Dupliquer, activer/désactiver, renommer ou supprimer une application

Les actions suivantes sont disponibles :

- **Dupliquer :** il se peut que vous souhaitiez dupliquer une application pour créer une version différente avec des propriétés ou paramètres différents. Lorsque vous dupliquez une application, elle est automatiquement renommée avec un suffixe unique et placée à côté de l'original. Vous pouvez également vouloir dupliquer une application et l'ajouter à un autre groupe. (Après la duplication, la manière la plus facile de déplacer une application est de la faire glisser.)
- **Activer ou désactiver :** activer/désactiver une application ne signifie pas activer/désactiver un groupe de mise à disposition ou groupe d'applications.
- **Renommer :** vous ne pouvez renommer qu'une seule application à la fois. Si vous essayez de renommer une application et qu'une application avec le même nom existe dans le même dossier ou groupe, vous êtes invité à spécifier un nom différent.
- **Supprimer :** la suppression d'une application la supprime des groupes de mise à disposition et des groupes d'applications auxquels elle était associée, mais pas de la source utilisée pour ajouter l'application à l'origine. Supprimer une application ne signifie pas supprimer une application d'un groupe de mise à disposition ou groupe d'applications.

Pour dupliquer, activer/désactiver, renommer ou supprimer une application :

1. Sélectionnez **Applications** dans le volet de gauche.
2. Sélectionnez une ou plusieurs applications dans le panneau du milieu, puis sélectionnez la tâche appropriée dans la barre d'actions.
3. Confirmez l'action lorsque vous y êtes invité.

### Supprimer des applications d'un groupe de mise à disposition

Une application doit être associée (appartenir) à au moins un groupe de mise à disposition ou groupe d'applications. Si vous tentez de supprimer une application d'un groupe de mise à disposition qui

supprimerait l'association de cette application avec un groupe de mise à disposition ou groupe d'applications, vous êtes averti que l'application va être supprimée si vous continuez. Lorsque cela se produit, si vous souhaitez mettre à disposition cette application, vous devez l'ajouter à nouveau à partir d'une source valide.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez un groupe de mise à disposition. Dans le panneau central inférieur, dans l'onglet **Applications**, sélectionnez l'application à supprimer.
3. Sélectionnez **Retirer application** dans la barre d'actions.
4. Confirmez la suppression.

### Supprimer des applications d'un groupe d'applications

Une application doit appartenir à au moins un groupe de mise à disposition ou groupe d'applications. Si vous tentez de supprimer une application d'un groupe d'applications qui aurait pour conséquence que cette application n'appartiendrait plus à aucun groupe, vous êtes averti que l'application va être supprimée si vous continuez. Lorsque cela se produit, si vous souhaitez mettre à disposition cette application, vous devez l'ajouter à nouveau à partir d'une source valide.

1. Sélectionnez **Applications** dans le volet de gauche.
2. Sélectionnez le groupe d'applications dans le volet central, puis sélectionnez une ou plusieurs applications.
3. Sélectionnez **Retirer application du groupe d'applications** dans la barre d'actions.
4. Confirmez la suppression.

### Modifier les propriétés d'une application

Vous pouvez modifier les propriétés d'une seule application à la fois.

Pour modifier les propriétés d'une application :

1. Sélectionnez **Applications** dans le volet de gauche.
2. Sélectionnez une application, puis sélectionnez **Modifier les propriétés d'application** dans la barre d'actions.
3. Sélectionnez la page contenant la propriété que vous souhaitez modifier.
4. Lorsque vous avez terminé, cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et garder la fenêtre ouverte, ou cliquez sur **OK** pour appliquer les modifications et fermer la fenêtre.

Dans la liste suivante, la page est indiquée entre parenthèses.

| Propriété | Page |
| --- | --- |
| Catégorie/dossier dans lequel l'application s'affiche dans l'application Citrix Workspace | Mise à disposition |
| Arguments de ligne de commande ; voir Passer des paramètres aux applications publiées | Emplacement |
| Les groupes de mise à disposition et groupes d'applications dans lesquels l'application est disponible | Groupes |
| Description | Identification |
| Extensions de nom de fichier et association de type de fichier : extensions que l'application ouvre automatiquement | Association de type de fichier |
| Icône | Mise à disposition |
| Mots clés pour StoreFront | Identification |
| Limites ; voir Configurer les limites d'application | Mise à disposition |
| Nom : noms que l'utilisateur et l'administrateur voient | Identification |
| Chemin d'accès au fichier exécutable ; voir Passer des paramètres aux applications publiées | Emplacement |
| Raccourci sur le bureau de l'utilisateur : activer ou désactiver | Mise à disposition |
| Visibilité : limite les utilisateurs autorisés à voir l'application dans application Citrix Workspace. Une application non visible peut toujours être démarrée. Pour la rendre non disponible ainsi qu'invisible, ajoutez-la à un groupe différent. | Limiter la visibilité |
| Répertoire de travail | Emplacement |

Les modifications apportées aux applications peuvent ne pas prendre effet pour les utilisateurs d'applications courantes tant qu'ils n'ont pas fermé leur session.

### Configurer les limites d'application

Configurez les limites d'application pour vous aider à gérer l'utilisation des applications. Par exemple, vous pouvez utiliser les limites d'application pour gérer le nombre d'utilisateurs pouvant accéder à une application simultanément. De même, les limites d'application peuvent être utilisées pour gérer

le nombre d'instances simultanées d'applications très consommatrices de ressources. Cette limite peut vous aider à gérer les performances des serveurs et à empêcher la détérioration du service.

Cette fonctionnalité limite le nombre de démarrages d'application qui sont négociés par le Controller (par exemple, à partir de l'application Citrix Workspace et StoreFront), et non pas le nombre d'applications qui peuvent être lancées par d'autres méthodes. Par conséquent, les limites d'application aident les administrateurs à gérer l'utilisation simultanée, mais ne peuvent pas être appliquées de force dans tous les scénarios. Par exemple, les limites d'application ne peuvent pas être appliquées lorsque le Controller se trouve en mode panne.

Par défaut, il n'existe aucune limite sur le nombre d'instances d'application qui peuvent être exécutées simultanément. Il existe plusieurs paramètres de limite d'application. Vous pouvez configurer tout ou partie d'entre eux.

- Le nombre maximal d'instances simultanées de l'application par tous les utilisateurs du groupe de mise à disposition.
- Une instance de l'application par utilisateur dans le groupe de mise à disposition.
- Le nombre maximal d'instances simultanées de l'application par machine (PowerShell uniquement).

Si une limite est configurée, un message d'erreur est généré lorsqu'un utilisateur tente de démarrer une instance de l'application qui dépasse la limite configurée. Si plusieurs limites sont configurées, une erreur est signalée lorsque la première limite est atteinte.

Exemples d'utilisation des limites d'application :

- **Nombre maximal d'instances simultanées :** dans un groupe de mise à disposition, vous configurez le nombre maximal d'instances d'applications simultanées `Alpha` sur 15. Plus tard, les utilisateurs de ce groupe de mise à disposition ont 15 instances de cette application en cours d'exécution en même temps. Si un utilisateur de ce groupe de mise à disposition tente de lancer `Alpha`, un message d'erreur est généré et l'application `Alpha` n'est pas lancée car la limite d'instances d'applications simultanées (15) aurait été dépassée.
- **Une instance d'application par utilisateur :** dans un autre groupe de mise à disposition, vous activez l'option une instance par utilisateur pour l'application `Beta`. L'utilisateur Tony lance l'application `Beta` avec succès. Plus tard, alors que l'application est toujours en cours d'exécution dans la session de Tony, il tente de démarrer une autre instance de `Beta`. Un message d'erreur est généré et `Beta` n'est pas lancé car la limite d'une instance par utilisateur aurait été dépassée.
- **Nombre maximal d'instances simultanées et une instance par utilisateur :** dans un autre groupe de mise à disposition, vous configurez un nombre maximal d'instances simultanées de 10 et activez l'option une instance par utilisateur pour l'application `Delta`. Plus tard, lorsque dix utilisateurs de ce groupe de mise à disposition exécutent chacun une instance de `Delta`, les

autres utilisateurs de ce groupe de mise à disposition qui tentent de lancer `Delta` reçoivent un message d'erreur. `Delta` n'est pas démarré. Si un des dix utilisateurs de `Delta` tente de démarrer une seconde instance de cette application, il reçoit un message d'erreur et la deuxième instance ne peut pas être démarrée.

- **Nombre maximal d'instances simultanées par machine et utilisation de restrictions de balises :** l'application `Charlie` a des exigences de licence et de performance qui déterminent le nombre d'instances pouvant s'exécuter simultanément sur un serveur spécifique. Ces exigences dictent également le nombre d'instances pouvant s'exécuter simultanément sur tous les serveurs du site.

  La limite d'instances d'application par machine affecte tous les serveurs du site (et pas uniquement les machines d'un groupe de mise à disposition donné). Supposons que votre site dispose de trois serveurs. Pour l'application `Charlie`, vous configurez la limite d'instances d'application par machine sur 2. Ainsi, pas plus de six instances de l'application `Charlie` sont autorisées à se lancer à l'échelle du site. (Cela correspond à une limite de deux instances de Charlie sur chacun des trois serveurs.)

  Pour restreindre l'utilisation d'une application à certaines machines d'un groupe de mise à disposition (en plus de limiter les instances sur toutes les machines à l'échelle du site) :

  - Utilisez la fonctionnalité de balises pour ces machines.
  - Configurez le nombre maximal d'instances par machine pour cette application.

Si des applications sont lancées par d'autres méthodes que la négociation Controller (par exemple, lorsqu'un Controller se trouve en mode panne) et que les limites configurées sont dépassées, les utilisateurs ne peuvent pas lancer d'instances supplémentaires jusqu'à ce qu'ils ferment suffisamment d'instances pour ne plus dépasser la limite. Les instances qui ont dépassé la limite ne sont pas arrêtées de force. Elles seront autorisées à continuer jusqu'à ce que leurs utilisateurs les ferment.

Si vous désactivez l'itinérance de session, désactivez la limite d'application « Une seule instance par utilisateur ». Si vous activez la limite d'application « Une seule instance par utilisateur », ne configurez pas les deux valeurs qui permettent de nouvelles sessions sur de nouvelles machines. Pour plus d'informations sur l'itinérance, reportez-vous à Sessions.

Pour configurer la limite d'instances maximales par groupe de mise à disposition et la limite d'une instance par utilisateur :

1. Sélectionnez **Applications** dans le volet de gauche, puis sélectionnez une application.
2. Sélectionnez **Modifier les propriétés d'application** dans la barre d'actions.
3. Sur la page **Mise à disposition**, choisissez l'une des options ci-dessous.

   - **Autoriser l'utilisation illimitée de l'application**. Il n'existe aucune limite au nombre d'instances exécutées en même temps. Il s'agit de l'option par défaut.

- **Définir des limites pour l'application**. Il existe deux types de limite ; spécifiez-en une ou les deux.
  - Spécifier le nombre maximal d'instances pouvant être exécutées simultanément par machine
  - Limiter à une instance d'application par utilisateur

4. Cliquez sur **OK** pour appliquer la modification et fermer la boîte de dialogue ou sur **Appliquer** pour appliquer la modification et laisser la boîte de dialogue ouverte.

Pour configurer la limite d'instances maximales par machine (PowerShell uniquement) :

- Dans PowerShell (à l'aide du SDK Remote PowerShell pour les déploiements Citrix Cloud ou du SDK PowerShell pour les déploiements sur site), entrez l'applet de commande `BrokerApplication` appropriée avec le paramètre `MaxPerMachineInstances`.
- Pour plus d'informations, utilisez l'applet de commande `Get-Help`. Par exemple :

  ```
  Get-Help Set-BrokerApplication –Parameter MaxPerMachineInstances
  ```

### Passer des paramètres aux applications publiées

Utilisez la page **Emplacement** des propriétés d'une application pour entrer la ligne de commande et les paramètres à transmettre aux applications publiées.

Lorsque vous associez des types de fichier à une application publiée, les symboles `"%*"` (pourcentage et étoile entre guillemets) sont ajoutés à la fin de la ligne de commande de l'application. Ces symboles réservent l'emplacement des paramètres transmis aux machines utilisateur.

Si une application publiée ne démarre pas, vérifiez que la ligne de commandes contient les symboles appropriés. Par défaut, les paramètres fournis par les machines utilisateur sont validés lorsque les symboles `"%*"` sont ajoutés. Pour les applications publiées qui utilisent des paramètres personnalisés fournis par la machine utilisateur, les symboles `"%**"` sont ajoutés à la ligne de commande pour éviter la validation de ligne de commande. Si ces symboles n'apparaissent pas dans la ligne de commandes d'une application, vous pouvez les ajouter manuellement.

Si le chemin d'accès du fichier exécutable comprend des noms de répertoire avec des espaces, (`"C:\Program Files"`, par exemple), mettez la ligne de commandes de l'application entre guillemets afin d'indiquer que l'espace fait partie de la ligne de commandes. Pour ce faire, ajoutez des guillemets autour du chemin d'accès et des guillemets autour des symboles `%*`. Veillez à inclure un espace entre le guillemet final du chemin d'accès et le guillemet initial des symboles `%*`.

Par exemple, la ligne de commandes pour l'application publiée Windows Media Player est :

```
"C:\Program Files\Windows Media Player\mplayer1.exe""%*"
```

> **Remarque :**
>
> Le nombre maximum de caractères, arguments compris, dans la ligne de commande pour lancer des applications publiées est de 203.

### Gérer les dossiers d'applications

Par défaut, les applications que vous ajoutez aux groupes de mise à disposition sont placées dans un dossier nommé **Applications**. Vous pouvez spécifier un dossier différent lorsque vous créez le groupe de mise à disposition, lorsque vous ajoutez une application ou plus tard.

À savoir :

- Vous ne pouvez pas renommer ou supprimer le dossier Applications, mais vous pouvez déplacer toutes les applications qu'il contient vers d'autres dossiers que vous créez.
- Un nom de dossier peut contenir entre 1 et 64 caractères. Les espaces sont autorisés.
- Les dossiers peuvent être imbriqués jusqu'à cinq niveaux.
- Les dossiers n'ont pas à contenir d'applications. Les dossiers vides sont autorisés.
- Les dossiers sont répertoriés par ordre alphabétique dans Web Studio, sauf si vous les déplacez ou spécifiez un emplacement différent lorsque vous les créez.
- Vous pouvez posséder plus d'un dossier du même nom, tant que chacun possède un dossier parent différent. De même, vous pouvez posséder plus d'une application du même nom, tant que chacune se trouve dans un dossier différent.
- Vous devez disposer de l'autorisation `View Applications` pour voir les applications dans des dossiers, et vous devez posséder l'autorisation `Edit Application Properties` pour toutes les applications dans le dossier pour déplacer, renommer ou supprimer un dossier qui contient des applications.
- La plupart des procédures suivantes requièrent des actions depuis la barre d'actions de Web Studio. Éventuellement, vous pouvez utiliser les menus du bouton droit de la souris ou faire glisser l'élément. Par exemple, si vous créez ou déplacez un dossier dans un emplacement indésirable, vous pouvez le faire glisser et le déposer à l'emplacement approprié.

Pour gérer les dossiers d'applications, sélectionnez **Applications** dans le volet de gauche. Utilisez la liste ci-dessous pour plus d'informations.

- **Pour afficher tous les dossiers (mis à part les dossiers incorporés) :** cliquez sur **Afficher tout** au-dessus de la liste de dossiers.
- **Pour créer un dossier au niveau le plus élevé (non imbriqué) :** sélectionnez le dossier **Applications**. Pour placer le nouveau dossier sous un dossier existant autre que le dossier **Applications**, sélectionnez ce dossier. Sélectionnez ensuite **Créer un dossier** dans la barre d'actions Entrez un nom.

- **Pour déplacer un dossier :** sélectionnez le dossier, puis sélectionnez **Déplacer le dossier** dans la barre d'actions. Vous pouvez déplacer un seul dossier à la fois, à moins que le dossier contienne des dossiers incorporés. (Le moyen le plus simple de déplacer un dossier est de le faire glisser.)
- **Pour renommer un dossier :** sélectionnez le dossier, puis sélectionnez **Renommer le dossier** dans la barre d'actions. Entrez un nom.
- **Pour supprimer un dossier :** sélectionnez le dossier, puis sélectionnez **Supprimer le dossier** dans la barre d'actions. Lorsque vous supprimez un dossier qui contient des applications et d'autres dossiers, ces objets sont également supprimés. La suppression de l'application supprime l'attribution de l'application du groupe de mise à disposition. Elle ne supprime pas l'application de la machine.
- **Pour déplacer des applications dans un dossier :** sélectionnez une ou plusieurs applications. Sélectionnez ensuite **Déplacer l'application** dans la barre d'actions. Sélectionnez le dossier.

Vous pouvez également placer les applications que vous ajoutez dans un dossier de la page **Application** lors de la création d'un groupe de mise à disposition ou d'un groupe d'applications. Par défaut, les applications ajoutées se trouvent dans le dossier **Applications**. Cliquez sur **Modifier** pour sélectionner ou créer un dossier.

### Contrôle du lancement local des applications sur des bureaux publiés

Lorsque les utilisateurs lancent une application publiée depuis un bureau publié, vous pouvez utiliser PowerShell pour contrôler si l'application est lancée dans cette session de bureau ou en tant qu'application publiée. L'application Citrix Workspace recherche le chemin d'installation de l'application dans le registre Windows sur le VDA et, s'il est présent, lance l'instance locale de l'application. Sinon, une instance hébergée de l'application est lancée. Si vous lancez une application qui n'est pas installée sur le VDA, l'application hébergée est lancée. Pour plus d'informations, consultez la section Lancement de vPrefer.

Vous pouvez modifier cette action dans PowerShell (à l'aide du SDK Remote PowerShell dans les déploiements Citrix Cloud ou du SDK PowerShell dans les déploiements sur site).

Dans l'application `New-Broker` ou l'applet de commande `Set-BrokerApplication`, utilisez l'option `LocalLaunchDisabled`. Par exemple :

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

Par défaut, la valeur de cette option est false (`-LocalLaunchDisabled $false`). Lors du lancement d'une application publiée depuis un bureau publié, l'application est lancée dans cette session de bureau.

Si vous définissez la valeur de l'option sur true (`-LocalLaunchDisabled $true`), l'application publiée est lancée. Cela crée une session supplémentaire séparée depuis le bureau publié (à l'aide de

l'application Citrix Workspace pour Windows) vers l'application publiée.

Configuration requise et limitations :

- La valeur `ApplicationType` de l'application doit être `HostedOnDesktop`.
- Cette option est disponible uniquement via le SDK PowerShell approprié. Elle n'est actuellement pas disponible dans l'interface graphique de Web Studio.
- Cette option nécessite StoreFront 3.14 minimum, Citrix Receiver pour Windows 4.11 et Delivery Controller 7.17.

## Packages d'applications

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Microsoft propose trois technologies de packaging pour mettre à disposition des applications auprès des utilisateurs : App-V, MSIX et attachement d'application MSIX. Cet article explique comment déployer et fournir ces applications packagées à l'aide de **Web Studio > Packages d'applications** :

- Déployer et fournir des applications App-V
- Déployer et fournir des applications MSIX et des applications packagées via l'attachement d'application MSIX

### Déployer et fournir des applications App-V

Cette section contient les informations suivantes :

- Vue d'ensemble. Décrit les méthodes de gestion utilisées pour fournir et gérer les packages App-V.
- Procédures. Fournit des procédures pour le déploiement et la mise à disposition de ces packages.

### Vue d'ensemble

Cette section décrit les méthodes de gestion utilisées pour fournir et de gérer les packages App-V. Pour plus d'informations sur les composants et les concepts avec lesquels vous interagissez lors de la mise à disposition d'applications packagées App-V, consultez la documentation Microsoft : https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows.

Vous pouvez utiliser les méthodes suivantes pour fournir et gérer les packages App-V :

- **Administration double**. Les packages d'applications sont configurés et gérés sur les serveurs App-V. Citrix Virtual Apps and Desktops et les serveurs App-V fonctionnent ensemble pour fournir et gérer les packages.

  Cette méthode exige que Citrix Virtual Apps and Desktops actualise périodiquement la vue de l'instantané de l'état du serveur App-V. Cela entraîne des frais de matériel, d'infrastructure et d'administration. Les serveurs Citrix Virtual Apps and Desktops et App-V doivent rester synchronisés, en particulier pour les permissions utilisateur.

  La fonction Administration double fonctionne mieux dans les déploiements où App-V et votre environnement sont étroitement liés :

  - **App-V Management Server**. Publie et gère le cycle de vie des packages App-V et des fichiers de configuration dynamique.
  - **Composant Citrix Personalization** installé sur les machines VDA. Gère l'enregistrement du serveur de publication App-V approprié requis pour les lancements d'applications.

  Ainsi, le serveur de publication est synchronisé pour l'utilisateur au moment approprié. Le serveur de publication gère d'autres aspects du cycle de vie du package, par exemple, l'actualisation à l'ouverture de session et les groupes de connexion.

- **Administration unique**. Les packages d'applications sont stockés sur des partages réseau. Citrix Virtual Apps and Desktops fournit et gère les packages de manière indépendante.

  Cette méthode réduit les frais généraux, car les serveurs App-V et l'infrastructure de base de données ne sont pas nécessaires au déploiement.

  Avec cette méthode, vous stockez les packages App-V sur un partage réseau et téléchargez leurs métadonnées à partir de cet emplacement vers votre environnement. Le composant Citrix Personalization installé sur les machines VDA gère et fournit ensuite les applications comme suit :

  - Il traite les fichiers de configuration du déploiement et les fichiers de configuration utilisateur lors du lancement d'une application.
  - Il gère tous les aspects des cycles de vie des packages sur la machine hôte.

Vous pouvez utiliser les deux méthodes de gestion simultanément. En d'autres termes, lorsque vous

ajoutez des applications aux groupes de mise à disposition, les applications peuvent provenir de packages App-V situés sur des serveurs App-V ou sur des partages réseau.

> **Remarque :**
>
> Si vous utilisez simultanément les deux méthodes de gestion et que le package App-V contient un fichier de configuration dynamique dans les deux emplacements, le fichier du serveur App-V (Administration double) est utilisé.

#### Procédures

Pour prendre en charge la mise à disposition des applications App-V, vous devez installer le composant Citrix Personalization sur les machines VDA. Consultez Installer le composant Citrix Personalization sur les machines VDA pour obtenir plus d'informations.

Pour fournir des applications packagées App-V à vos utilisateurs, procédez comme suit :

1. Stocker les packages d'applications sur des partages réseau.
2. Charger les packages d'applications dans votre environnement
3. Ajouter des applications à des groupes de mise à disposition.
4. Pour permettre la mise à disposition automatique de packages App-V interdépendants, créez des groupes d'isolement.

Pour que Citrix Virtual Apps and Desktops reconnaisse et applique les fichiers de configuration dynamique App-V selon la méthode Administration unique, consultez ce blog Citrix.

### Déployer et fournir des applications MSIX et des applications packagées via l'attachement d'application MSIX

Cette section contient les informations suivantes :

- Vue d'ensemble. Décrit la manière dont les packages MSIX et les packages créés via l'attachement d'application MSIX sont fournis et gérés.
- Procédures. Fournit des procédures pour le déploiement et la mise à disposition de ces packages.

#### Vue d'ensemble

Citrix Virtual Apps and Desktops fournit des applications MSIX et des applications packagées via l'attachement d'application MSIX aux utilisateurs via le composant Citrix Personalization installé sur les machines VDA. Ce composant gère tous les aspects des cycles de vie des packages sur la machine hôte.

Pour plus d'informations sur MSIX et l'attachement d'application MSIX, consultez la documentation Microsoft : https://docs.microsoft.com/en-us/windows/msix/ et https://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach respectivement.

#### Procédures

Pour prendre en charge la mise à disposition des packages MSIX et des packages créés via l'attachement d'application MSIX, vous devez installer le composant Citrix Personalization sur les machines VDA. Consultez Installer le composant Citrix Personalization sur les machines VDA pour obtenir plus d'informations.

Pour fournir des applications MSIX et des applications packagées via l'attachement d'application MSIX à vos utilisateurs, procédez comme suit :

1. Stocker les packages d'applications sur des partages réseau.
2. Charger les packages d'applications dans votre environnement
3. Ajouter des applications à des groupes de mise à disposition.

### Installez le composant Citrix Personalization sur les machines VDA

Le composant Citrix Personalization gère le processus de publication des packages d'applications aux formats App-V, MSIX et aux formats crées via l'attachement d'application MSIX. Ce composant n'est pas installé par défaut lorsque vous installez un VDA. Vous pouvez l'installer pendant ou après l'installation du VDA.

Pour installer le composant lors de l'installation du VDA, utilisez l'une des méthodes suivantes :

- Dans l'assistant d'installation, accédez à la page **Composants supplémentaires**, puis activez la case à cocher **Citrix Personalization pour AppV : VDA**.
- Dans l'interface de ligne de commande, utilisez l'option **/includeadditional "Citrix Personalization pour AppV : VDA"**.

Pour installer le composant après l'installation du VDA, procédez comme suit :

1. Sur la machine VDA, accédez à **Panneau de configuration > Programmes > Programmes et fonctionnalités**, cliquez avec le bouton droit sur **Citrix Virtual Delivery Agent**, puis sélectionnez **Modifier**.
2. Dans l'assistant qui s'affiche, accédez à la page **Composants supplémentaires**, puis activez la case à cocher **Citrix Personalization for App-V - VDA**.

> **Remarque :**
>
> Le client de bureau Microsoft App-V est le composant qui exécute les applications virtuelles

> depuis les packages App-V sur les machines utilisateur. Windows 10 (1607 ou version ultérieure), Windows Server 2016 et Windows Server 2019 incluent déjà ce logiciel client App-V. Vous devez uniquement l'activer sur les machines VDA. Pour plus d'informations, consultez cet article de la documentation Microsoft : https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client.

### Stocker les packages d'applications sur des partages réseau

Après avoir configuré l'infrastructure, générez les packages d'applications et stockez-les dans un emplacement réseau, tel qu'un partage réseau UNC ou SMB ou sur un partage de fichiers Azure.

Les étapes détaillées sont les suivantes :

1. Générez des packages d'applications Reportez-vous à la documentation Microsoft pour plus d'informations.
2. Stockez les packages d'applications dans un emplacement réseau :
   - Pour la fonction **App-V Administration unique** : stockez les packages et les fichiers de configuration dynamique (App-V) correspondants sur un partage réseau UNC ou SMB ou sur un partage de fichiers Azure.
   - Pour la fonction **App-V Administration double** : publiez les packages sur le serveur de gestion App-V depuis un chemin d'accès UNC. (La publication à partir d'URL HTTP n'est pas prise en charge.)
   - Pour **les applications MSIX ou les applications packagées via l'attachement d'application MSIX** : stockez les packages sur un partage réseau UNC ou SMB ou sur un partage de fichiers Azure.
3. Assurez-vous que le VDA dispose de l'autorisation de lecture sur le chemin de stockage du package :
   - Si vous stockez des packages sur un partage réseau UNC ou SMB de votre domaine AD, accordez à la machine VDA l'autorisation de lecture sur le chemin de stockage. Pour ce faire, vous pouvez accorder explicitement au compte AD de la machine l'autorisation de lecture sur le partage ou inclure le compte dans un groupe AD disposant de cette autorisation.
   - Si vous stockez des packages sur un partage de fichiers Azure, accordez d'abord à un compte utilisateur l'autorisation de lecture sur le chemin de stockage dans Azure. Ensuite, configurez `ctxAppVService` s'exécutant sur la machine VDA pour qu'elle utilise ce compte utilisateur pour accéder au chemin de stockage du package. Consultez la section suivante pour connaître les étapes détaillées.

#### Modifier le compte d'ouverture de session de l'utilisateur

Le VDA appelle `ctxAppVService` pour accéder aux chemins de stockage du package. Par défaut, `ctxAppVService` accède aux chemins de stockage des packages à l'aide du **compte système local** de la machine. Ce type d'authentification de machine fonctionne dans les domaines AD. Toutefois, il ne fonctionne pas dans les scénarios d'intégration AD et Azure AD qui nécessitent une authentification basée sur le compte utilisateur.

Si vous stockez des packages sur un partage de fichiers Azure, remplacez le compte d'ouverture de session pour `ctxAppVService` par un compte utilisateur disposant d'une autorisation de lecture sur le chemin de stockage du package. Les étapes détaillées sont les suivantes :

1. Démarrez **Services**, cliquez avec le bouton droit sur **ctxAppVService**, puis sélectionnez **Propriétés**.
2. Dans l'onglet **Connexion**, sélectionnez **Ce compte**, entrez un compte utilisateur disposant d'une autorisation de lecture sur le chemin de stockage du package, puis saisissez deux fois le mot de passe de l'utilisateur.
3. Cliquez sur **OK**.

### Charger les packages d'applications dans votre environnement

Après avoir stocké les packages d'applications sur un emplacement réseau selon vos besoins, chargez-les sur votre environnement afin de les distribuer. Si nécessaire, utilisez l'une des méthodes suivantes :

- Chargement en bloc
- Chargement un par un

#### Préparations

Citrix Virtual Apps and Desktops utilise une machine VDA pour configurer la connexion à l'emplacement réseau pour la détection de packages. Par conséquent, créez un groupe de mise à disposition au préalable et assurez-vous qu'au moins un VDA du groupe répond aux exigences suivantes :

- Version VDA :
  - Pour découvrir les packages App-V : 2203 ou version ultérieure
  - Pour découvrir les applications MSIX et les applications packagées via l'attachement d'application MSIX : 2209 ou version ultérieure
- Composant Citrix Personalization pour App-V : installé

- Autorisation sur l'emplacement du package : lecture (consultez Étape 2 : Stocker les packages d'applications sur des partages réseau pour plus d'informations.)
- État d'alimentation : sous tension
- État : enregistré

#### Charger des packages d'applications en bloc

Charger des packages dans un emplacement réseau de votre environnement Assurez-vous que les éléments suivants sont prêts avant le chargement :

- Groupe de mise à disposition qui répond aux exigences décrites à la section Préparations
- Chemin de l'emplacement réseau

Pour charger des packages en bloc, procédez comme suit :

1. Dans le panneau gauche, sélectionnez **Packages d'applications**.
2. Dans l'onglet **Sources**, cliquez sur le bouton **Ajouter une source**. La page **Ajouter une source** s'affiche.
3. Dans le champ **Nom**, entrez un nom descriptif pour la source du package.
4. Dans le champ **Groupe de mise à disposition**, cliquez sur **Sélectionner un groupe de mise à disposition**. Sélectionnez ensuite un groupe de mise à disposition qui répond aux exigences décrites à la section Préparations, puis cliquez sur **OK**.
5. Dans le champ **Type d'emplacement**, sélectionnez **Serveur Microsoft App-V** ou **Partage réseau** en fonction de l'endroit où vous stockez les packages, puis définissez les paramètres correspondants :
   - Si vous sélectionnez **Serveur Microsoft App-V**, entrez les informations suivantes :
     - URL du serveur de gestion. Exemple : `http://appv-server.example.com`
     - Informations de connexion de l'administrateur du serveur d'administration.
     - URL et numéro de port du serveur de publication. Exemple : `http://appv-server.example.com:3330`
   - Si vous avez sélectionné **Partage réseau**, spécifiez les informations suivantes :
     - Entrez le chemin UNC du partage réseau. Exemple : `\\Package-Server\apps\`
     - Sélectionnez les types de packages que vous souhaitez charger. Les options incluent App-V, MSIX et Attachement d'applications MSIX.
     - Spécifiez s'il faut rechercher des packages dans les sous-dossiers.
6. Cliquez sur **Ajouter une source**.

   La page Ajouter une source se ferme et la nouvelle source ajoutée apparaît dans la liste des sources. Citrix Virtual Apps and Desktops charge les packages dans votre environnement à l'

aide d'un VDA du groupe de mise à disposition. Une fois le chargement terminé, le champ État indique *Importation réussie*. Les packages correspondants apparaissent dans l'onglet **Packages**.

> **Remarque :**
>
> Pour rechercher les mises à jour des packages dans un emplacement source et les importer dans votre environnement, sélectionnez l'emplacement dans la liste des sources et cliquez sur **Rechercher mises à jour des packages**.

#### Charger les packages d'application un par un

Chargez un package d'application depuis un partage réseau vers votre environnement. Avant le chargement, assurez-vous que les éléments suivants sont prêts :

- Groupe de mise à disposition qui répond aux exigences décrites à la section Préparations
- Chemin de l'emplacement réseau

Pour charger un package vers votre environnement, procédez comme suit :

1. Dans le panneau gauche, sélectionnez **Packages d'applications**.
2. Dans l'onglet **Packages**, cliquez sur le bouton **Ajouter un package**. La page **Ajouter un package** s'affiche.
3. Dans le champ **Groupe de mise à disposition**, cliquez sur **Sélectionner un groupe de mise à disposition**. Sélectionnez ensuite un groupe de mise à disposition qui répond aux exigences décrites à la section Préparations, puis cliquez sur **OK**.
4. Dans le champ **Chemin complet du package**, entrez un chemin d'accès selon vos besoins :
   - Pour charger plusieurs packages à la fois, entrez leurs chemins complets, séparés par des points-virgules (`;`). Exemple : `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - Pour charger tous les packages présents sur un partage réseau, entrez le chemin de stockage. Exemple : \package-Server\apps\
5. Cliquez sur **Ajouter un package**.

   Le package de l'application apparaît dans l'onglet **Packages**.

### Ajouter des applications à des groupes de mise à disposition

Une fois qu'un package d'applications est entièrement chargé, ajoutez ses applications à un ou plusieurs groupes de mise à disposition selon vos besoins. Ainsi, les utilisateurs associés à ces

groupes de mise à disposition peuvent accéder aux applications.

Pour ajouter une ou plusieurs applications d'un package à plusieurs groupes de mise à disposition, procédez comme suit :

1. Dans le panneau gauche, sélectionnez **Packages d'applications**.
2. Dans l'onglet **Packages**, sélectionnez un package selon vos besoins.
3. Dans la barre d'actions, cliquez sur **Ajouter des groupes de mise à disposition**. La page Groupes de mise à disposition s'affiche.
4. Sélectionnez une ou plusieurs applications dans le package selon vos besoins, puis cliquez sur **Suivant**. Les groupes de mise à disposition avec le type *Applications* s'affiche.
5. Dans la liste des groupes de mise à disposition, sélectionnez les groupes auxquels vous souhaitez attribuer les applications, puis cliquez sur **Suivant**.
   **Remarque :** si vous avez sélectionné un package MSIX ou un package créé via l'attachement d'application MSIX, seuls les groupes de mise à disposition dont le niveau fonctionnel est 2106 ou supérieur sont affichés dans la liste.
6. Cliquez sur **Terminer**.

Vous pouvez également ajouter des applications packagées à un groupe de mise à disposition dans les cas suivants :

- Création d'un groupe de mise à disposition. Pour plus d'informations, consultez la section Créer des groupes de mise à disposition.
- Modification de groupes de mise à disposition ou d'applications existants. Pour plus d'informations, consultez la section Ajouter des applications.

## (Facultatif) Créez des groupes d'isolement pour les packages App-V

Vous pouvez créer des groupes d'isolement pour permettre la mise à disposition automatique de packages App-V interdépendants.

> **Remarque :**
>
> Les groupes d'isolement sont pris en charge pour la méthode App-V Administration unique. Si vous utilisez la méthode App-V Administration double, vous pouvez atteindre le même objectif en créant des *groupes de connexions* dans l'infrastructure Microsoft App-V. Pour plus d'informations, consultez cet article de la documentation Microsoft : https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file.

### À propos des groupes d'isolement

Un groupe d'isolement est un ensemble de packages d'applications interdépendants qui doivent s'exécuter dans le même sandbox Windows pour créer un environnement virtuel. Les groupes d'isole-

ment Citrix App-V sont similaires mais pas identiques aux groupes de connexions App-V. Un groupe d'isolement comprend deux types de packages :

- Packages d'applications de type **Explicite**. Applications soumises à des exigences de licence spécifiques. Vous pouvez restreindre ces applications à une plage spécifique d'utilisateurs en les ajoutant à des groupes de mise à disposition.
- Packages d'applications de type **Automatique**. Applications toujours disponibles pour tous les utilisateurs, qu'ils soient ajoutés ou non à des groupes de mise à disposition.

Par exemple, l'application app-a requiert JRE 1.7 pour s'exécuter. Vous pouvez créer un groupe d'isolement qui contient app-a (marqué comme *Explicite*) et JRE 1.7 (marqué comme *Automatique*). Ajoutez ensuite le package App-V pour app-a à un ou plusieurs groupes de mise à disposition. Lorsqu'un utilisateur démarre l'application app-a, JRE 1.7 est automatiquement déployé.

Lorsqu'un utilisateur démarre une application App-V marquée comme *Explicite* dans un groupe d'isolement, Citrix Virtual Apps and Desktops vérifie l'autorisation d'accès de l'utilisateur à l'application dans les groupes de mise à disposition. Si l'utilisateur est autorisé à accéder à l'application, tous les packages d'applications de type *Automatique* du même groupe d'isolement sont mis à la disposition de l'utilisateur.

Il n'est pas nécessaire d'ajouter les packages de type *Automatique* à un groupe de mise à disposition. S'il existe un autre package d'applications de type *Explicite* dans le groupe d'isolement, ce package n'est mis à la disposition de l'utilisateur que s'il se trouve dans le même groupe de mise à disposition.

Pour plus d'informations sur les groupes d'isolement, consultez ce blog Citrix.

**Créer un groupe d'isolement App-V** Créez un groupe d'isolement et ajoutez-y des packages d'applications interdépendants. Les étapes détaillées sont les suivantes :

1. Dans l'onglet **Groupes d'isolement**, cliquez sur **Ajouter un groupe d'isolement**.
2. Entrez un nom et une description pour le groupe d'isolement. Tous les packages d'applications de votre environnement apparaissent dans la liste **Packages disponibles**.
3. Dans la liste **Packages disponibles**, sélectionnez une application selon vos besoins, puis cliquez sur la flèche droite. Les applications sélectionnées s'affichent dans la liste **Packages en groupe d'isolement**.
4. Dans le champ **Déploiement**, sélectionnez **Explicite** ou **Automatique** pour l'application.
5. Répétez les étapes 2 à 3 pour ajouter d'autres packages.
6. Pour modifier l'ordre des packages dans la liste, cliquez sur la flèche vers le haut ou vers le bas.
7. Cliquez sur **Enregistrer**.

> **Remarque :**
>
> Les configurations de groupes d'isolement entraînent la création de groupes de connexions App-

> V sur le VDA. Les scénarios de déploiement peuvent devenir complexes. Le client App-V prend en charge les packages qui ne se trouvent que dans un seul groupe de connexion actif à la fois. Nous vous recommandons d'éviter d'ajouter le même package à deux groupes d'isolement différents qui sont ajoutés au même groupe de mise à disposition.

## Publiez des applications packagées sur des VDA de bureau à session unique ou partagés

Vous pouvez désormais fournir des packages App-V, MSIX et MSIX App Attach à vos sessions VDA de bureau à session unique ou partagée directement via des groupes de mise à disposition. Vous pouvez accéder aux applications packagées sur votre VDA de bureau lors de la connexion en fonction des autorisations d'accessibilité définies pour les applications.

### Avantages

- Applications disponibles sur le VDA lors de la connexion et non mises en service à la demande via Workspace ou StoreFront.
- Temps de lancement amélioré lors de l'accès aux applications packagées.
- Facilite la maintenance des applications packagées de manière autonome, indépendamment de l'image de base du VDA.

### Considérations

- Cette option n'est disponible pour les VDA à session unique que via le SDK PowerShell approprié. Il n'est actuellement pas disponible dans le workflow Web Studio. La publication sur des bureaux partagés peut être effectuée à l'aide du SDK PowerShell ou de la manière existante via le workflow Web Studio. Pour en savoir plus sur la procédure existante, voir Ajouter des applications aux groupes de mise à disposition.
- Les applications doivent faire partie d'un groupe de mise à disposition.

### Avant de commencer

- Assurez-vous que les applications packagées sont signées et disponibles sur le site de partage de fichiers ou UNC. Pour en savoir plus, voir Stocker les packages d'applications sur des partages réseau.
- Installez le composant Citrix Personalization sur les machines VDA.

### Procédure

Pour fournir des applications packagées aux VDA de bureau, procédez comme suit :

1. Importez des packages d'applications dans Web Studio.
2. Publiez le package BrokerApplication.
3. Limitez la visibilité des applications sur le Web Studio.

### Importer des packages d'applications dans Web Studio

1. Ouvrez un navigateur Web. Entrez `https://<address of the server hosting Web Studio>/Citrix/Studio`.
2. Créez un groupe de mise à disposition. Pour plus d'informations, consultez la section Créer des groupes de mise à disposition.
3. Importez les packages d'applications dans Web Studio. Pour en savoir plus, voir Charger des packages d'applications en masse.

### Publiez l'application packagée sur BrokerApplication

Si vous publiez sur un VDA multisession (partagé) ou sur un VDA d'application à session unique, la procédure de publication reste inchangée. Pour en savoir plus, voir Ajouter des applications aux groupes de mise à disposition.
Si vous publiez sur un VDA de bureau à session unique, procédez comme suit :

Exécutez la commande PowerShell suivante sur le Delivery Controller :

1. Pour récupérer les commandes présentes dans le package :

   ```
   Import-Module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
   ```

   > **Remarque :**
   >
   > La version de `App-V package discovery module` qui prend en charge cette fonctionnalité se trouve dans l'ISO Citrix Virtual Apps and Desktops (versions 2311 ou supérieures) sur le chemin ci-dessus.

2. Pour récupérer les ID de groupe de mise à disposition et d'application packagés pertinents, procédez comme suit :

   ```
   Get-BrokerDesktopGroup | Format-Table Uid, Name
   Get-AppLibAppVApplication | Format-Table Uid, Name
   ```

3. Pour publier les packages et créer les configurations BrokerMachineConfigurations appropriées, procédez comme suit :

   ```
   Publish-PackagedApplication -AppLibararyApplicationUid <AppLibararyApplica
   .Uid > -DesktopGroupUid <DesktopGroup.Uid>
   ```

4. Pour synchroniser les configurations Broker, qui sont ensuite envoyées à l'agent Broker sur VDA, procédez comme suit :

   ```
   Update-DesktopGroupMachineConfigurations -DesktopGroupUid <
   DesktopGroup.Uid>
   ```

   > **Remarque :**
   >
   > Assurez-vous d'exécuter la commande PowerShell `Update-DesktopGroupMachineConfigurati` après avoir publié ou supprimé des applications packagées d'un VDA.

#### Limiter la visibilité des applications sur Web Studio

Par défaut, toutes les applications packagées attribuées au groupe de mise à disposition desservant leur VDA sont disponibles sur leur session de bureau. Vous pouvez contrôler la visibilité des applications packagées sur les VDA de bureau en définissant la visibilité des applications pour des utilisateurs ou des groupes spécifiques sur le Web Studio. Pour gérer la visibilité des applications packagées, voir Modifier les propriétés de l'application.

## Applications de la plate-forme Windows universelle

June 27, 2024

Pour plus d'informations sur les applications UWP (Plateforme Windows universelle), consultez la documentation Microsoft suivante :

- Qu'est-ce qu'une application UWP ?
- Gestionnaire de packages Windows

### Configuration requise et limitations

Citrix Virtual Apps and Desktops prend en charge l'utilisation d'applications UWP avec des VDA sur les machines Windows suivantes :

- Windows 10 et versions ultérieures
- Windows Server 2016 et versions ultérieures

Les VDA doivent être à la version minimale 7.11.

Les fonctionnalités suivantes de Citrix Virtual Apps and Desktops ne sont pas prises en charge ou sont limitées lors de l'utilisation d'applications UWP :

- L'association de type de fichier n'est pas prise en charge.
- Local App Access n'est pas pris en charge.
- Aperçu dynamique : si les applications exécutées dans la session se chevauchent, l'aperçu affiche l'icône par défaut. Les API Win32 utilisées pour l'aperçu dynamique ne sont pas prises en charge dans les applications UWP.
- Centre de maintenance à distance : les applications UWP peuvent utiliser le Centre de maintenance pour afficher les messages dans la session. Ces messages ne sont actuellement pas redirigés vers le terminal pour être affichés à l'utilisateur.

Le lancement d'applications UWP et d'applications non UWP à partir du même serveur n'est pas pris en charge. Placez plutôt les applications UWP et non UWP dans des groupes de mise à disposition ou des groupes d'applications distincts.

Toutes les applications UWP installées sur la machine étant énumérées, Citrix recommande de désactiver l'accès des utilisateurs au Windows Store. Ceci empêche les applications UWP installées par un utilisateur d'être accessibles par un autre utilisateur.

Durant le chargement de version test, l'application UWP est installée sur la machine et elle est disponible pour d'autres utilisateurs. Lorsqu'un autre utilisateur lance l'application, celle-ci est installée et le système d'exploitation met à jour sa base de données AppX pour indiquer qu'elle a été installée par cet utilisateur.

Une fermeture de session appropriée lancée à partir d'une application UWP publiée qui a été lancée dans une fenêtre fixe ou transparente peut empêcher la fermeture de la session VDA et fermer de force la session l'utilisateur. Dans ce cas, plusieurs processus restant dans la session VDA empêchent sa fermeture correcte. Pour résoudre ce problème, déterminez le processus qui empêche la fermeture de la session VDA et ajoutez-le à la valeur de la clé de registre « LogoffCheckSysModules », en suivant les instructions de l'article CTX891671.

Les noms d'affichage des applications et les descriptions des applications UWP peuvent ne pas porter le nom correct. Modifiez et corrigez ces propriétés lors de l'ajout des applications au groupe de mise à disposition.

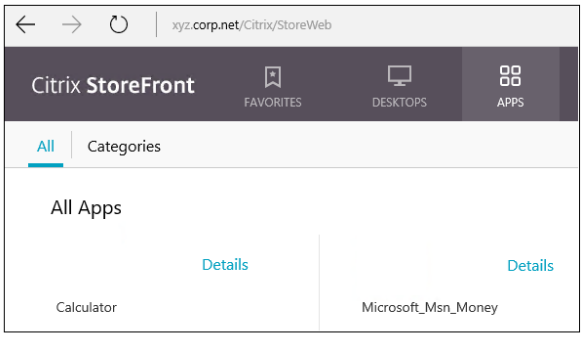
Consultez les Problèmes connus afin de prendre connaissance de problèmes supplémentaires.

Actuellement, plusieurs applications UWP ont des icônes blanches avec transparence activée, et par conséquent l'icône n'est pas visible sur l'arrière-plan blanc de StoreFront. Pour éviter ce problème, vous pouvez modifier l'arrière-plan. Par exemple, sur la machine StoreFront, modifiez le fichier `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`. À la fin du fichier, ajoutez

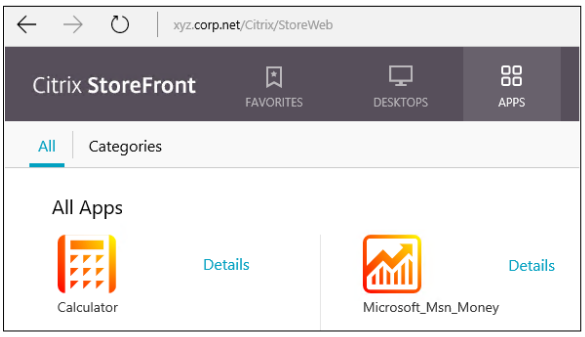
```
.storeapp-icon { background-image: radial-gradient( circle at top
```

`right, yellow, red ); }`. L'image suivante illustre l'arrière-plan avant et après pour cet exemple.




Before




After

Sur Windows Server 2016 et les versions ultérieures, le Gestionnaire de serveur peut également se lancer lorsqu'une application UWP est lancée. Pour éviter ce problème, vous pouvez désactiver le démarrage automatique du Gestionnaire de serveur lors de l'ouverture de session avec la clé de registre `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`. Pour plus de détails, consultez https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/.

### Installer et publier des applications UWP

La prise en charge des applications UWP est activée par défaut.

Pour installer une ou plusieurs applications UWP sur des VDA (ou une image principale), utilisez l'une des méthodes suivantes :

- Effectuez une installation en mode déconnecté à partir du Windows Store d'entreprise, à l'aide d'un outil tel que Deployment Image Servicing and Management (DISM) pour déployer les applications sur l'image de bureau. Pour plus d'informations, consultez la section Gestionnaire de packages Windows.
- Chargez la version test des applications. Pour plus d'informations, consultez la section Side-loading d'applications métier (LOB) sur des appareils clients Windows.
- Installez les applications UWP pour chaque utilisateur cible directement depuis le Windows Store pour les entreprises.

Pour ajouter (publier) une ou plusieurs applications UWP dans Citrix Virtual Apps ou Citrix Virtual Desktops :

1. Une fois que les applications UWP sont installées sur la machine, ajoutez les applications UWP à un groupe de mise à disposition ou un groupe d'applications. Vous pouvez le faire lorsque vous créez un groupe ou ultérieurement. Sur la page **Applications**, dans le menu **Ajouter**, sélectionnez **Depuis le menu Démarrer**.

2. Lorsque la liste des applications s'affiche, sélectionnez les applications UWP que vous souhaitez publier.
3. Continuez avec l'assistant ou fermez la boîte de dialogue d'édition.

Pour désactiver l'utilisation des applications universelles sur un VDA, ajoutez le paramètre de registre **EnableUWASeamlessSupport** dans `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` et définissez-le sur **0**.

### Désinstaller des applications UWP

Lorsque vous désinstallez une application UWP avec une commande telle que `Remove-AppXPackage`, l'élément est désinstallé uniquement pour les administrateurs. Pour supprimer l'application sur les machines des utilisateurs qui ont lancé et utilisé l'application, exécutez la commande de suppression sur chaque machine. Vous ne pouvez pas désinstaller le package AppX de toutes les machines des utilisateurs à l'aide d'une seule commande.

## Autoscale

June 27, 2024

Autoscale fournit une solution cohérente et hautes performances pour gérer de manière proactive vos machines. Elle vise à équilibrer les coûts et l'expérience des utilisateurs.

Autoscale permet une gestion proactive de l'alimentation de toutes les machines avec OS multi-session et mono-session enregistrées dans un groupe de mise à disposition.

Les fonctionnalités Autoscale sont les suivantes :

- Paramètres basés sur le calendrier et sur la charge
- Délai d'expiration de session dynamique
- Autoscaling des machines balisées (cloud bursting)
- Notifications de fermeture de la session utilisateur

### Plateformes d'hébergement VDA prises en charge

Autoscale prend en charge toutes les plates-formes prises en charge par Citrix Virtual Apps and Desktops. Cela inclut différentes plates-formes d'infrastructure, notamment XenServer, Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere et bien d'autres. Pour obtenir la liste complète des plates-formes prises en charge, consultez la section Configuration système requise pour Citrix Virtual Apps and Desktops.

> **Remarque :**
>
> Lorsque vous ajoutez des connexions hôtes de cloud public à votre déploiement, vous avez besoin d'une licence de droits hybrides. Pour plus d'informations sur la licence de droits hybrides, consultez Transition et échange (TTU) avec droits hybrides. Pour plus d'informations sur l'ajout d'une licence, consultez Créer un site.

### Charges de travail prises en charge

Autoscale prend en charge les groupes de mise à disposition OS multi-session et OS mono-session. Il y a trois interfaces utilisateur :

- Interface utilisateur Autoscale pour groupes de mise à disposition OS multi-session (anciennement groupes de mise à disposition RDS)
- Interface utilisateur Autoscale pour groupes de mise à disposition aléatoires (regroupés) OS mono-session (anciennement groupes de mise à disposition VDI regroupés)
- Interface utilisateur Autoscale pour groupes de mise à disposition statiques OS mono-session (anciennement groupes de mise à disposition VDI statiques)

Pour plus d'informations sur les interfaces utilisateur pour les différents groupes de mise à disposition, reportez-vous à la section Interfaces utilisateur Autoscale.

### Avantages

La fonctionnalité Autoscale offre les avantages suivants :

- Fournit un mécanisme unique et cohérent pour gérer l'alimentation des machines dans un groupe de mise à disposition.
- Assure la disponibilité et contrôle les coûts avec une gestion de l'alimentation des machines basée sur la charge ou sur des calendriers, ou une combinaison des deux.
- Pour surveiller des indicateurs tels que les économies de coûts et l'utilisation de la capacité, et pour activer les notifications, utilisez Director.

### Regardez une vidéo de 2 minutes

La vidéo suivante fournit un aperçu rapide de Autoscale.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

# Prise en main de Autoscale

June 27, 2024

Autoscale fonctionne au niveau du groupe de mise à disposition. Il gère de manière proactive l'alimentation des machines d'un groupe de mise à disposition en fonction des horaires que vous définissez.

Autoscale s'applique à tous les types de groupes de mise à disposition :

- OS statique mono-session
- OS aléatoire mono-session
- OS aléatoire multi-session

Cet article décrit les concepts de base liés à Autoscale et explique comment activer et configurer Autoscale pour un groupe de mise à disposition.

## Concepts de base

Avant de commencer, découvrez les concepts de base suivants pour Autoscale :

- Calendriers
- Tampon de capacité
- Indice de charge

### Calendriers

Autoscale allume et éteint les machines d'un groupe de mise à disposition selon un calendrier que vous avez défini.

Un calendrier inclut le nombre de machines actives pour chaque tranche horaire, avec des heures de pointe et des heures creuses définies.

Les paramètres de calendrier varient selon le type de groupe de mise à disposition. Pour plus d'informations, consultez :

- Groupes de mise à disposition des OS multi-sessions
- Groupes de mise à disposition aléatoires OS mono-session
- Groupes de mise à disposition statiques OS mono-session

#### Tampon de capacité

Le tampon de capacité est utilisé pour ajouter de la capacité de réserve à la demande actuelle afin de tenir compte des augmentations dynamiques de charge. Il y a deux scénarios à connaître :

- Pour les groupes de mise à disposition OS multi-session, le tampon de capacité est défini comme un pourcentage de la capacité totale du groupe de mise à disposition en termes d'indice de charge.
- Pour les groupes de mise à disposition OS mono-session, le tampon de capacité est défini comme un pourcentage du nombre total de machines dans le groupe de mise à disposition.

#### Indice de charge

> **IMPORTANT :**
>
> L'index de charge s'applique uniquement aux groupes de mise à disposition multi-session.

L'indice de charge détermine la probabilité qu'une machine reçoive des demandes de connexions utilisateur. Il est calculé à l'aide des paramètres de **stratégie Citrix Load Management** configurés pour les ouvertures de session simultanées, la session, l'UC, le disque et l'utilisation de la mémoire.

L'indice de charge est compris entre 0 et 10 000. Par défaut, une machine est considérée à pleine charge lorsqu'elle héberge 250 sessions.

- Le chiffre « 0 » indique une machine déchargée. Une machine dont la valeur d'indice de charge est 0 est à une charge de base.
- Le chiffre « 10 000 » indique une machine entièrement chargée qui ne peut plus exécuter de sessions.

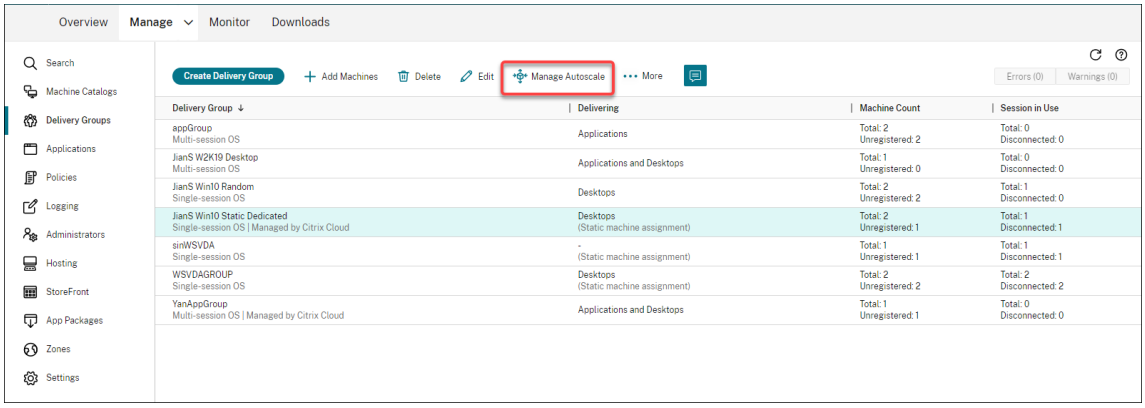
### Activer Autoscale pour un groupe de mise à disposition

Par défaut, Autoscale est désactivé lorsque vous créez un groupe de mise à disposition. Pour activer et configurer Autoscale pour un groupe de mise à disposition à l'aide de Web Studio, procédez comme suit :

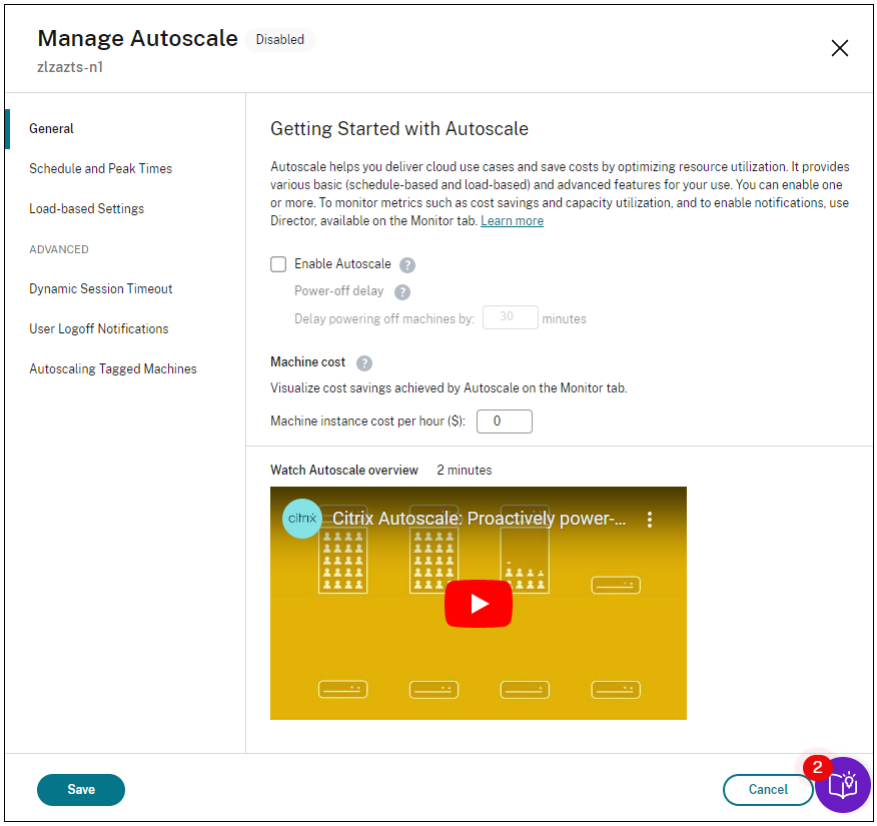
Vous pouvez également utiliser des commandes PowerShell pour activer et configurer Autoscale pour un groupe de mise à disposition. Pour plus d'informations, consultez la section Commandes SDK PowerShell de Broker.

1. Sélectionnez **Groupes de mise à disposition** dans le volet de gauche.
2. Sélectionnez le groupe de mise à disposition que vous souhaitez gérer, puis cliquez sur **Gérer Autoscale**.




3. Sur la page **Gérer Autoscale**, activez la case à cocher **Activer Autoscale** pour activer la fonctionnalité. Une fois que vous avez activé Autoscale, les options de la page sont activées.




4. Pour modifier les paramètres par défaut en fonction des besoins de votre organisation, définissez les paramètres suivants :

   - Définir des calendriers
   - Pour éteindre les machines inactives plus efficacement, utilisez Délai d'expiration de session dynamique et Notifications de fermeture de session
   - Pour gérer l'alimentation d'un sous-ensemble de machines du groupe de mise à disposition, utilisez Autoscaling des machines balisées.

Pour désactiver Autoscale, désélectionnez la case **Autoscale**. Les options de la page deviennent grises pour indiquer que la fonction Autoscale est désactivée pour le groupe de mise à disposition sélectionné.

> **Important :**
>
> - Si vous désactivez Autoscale, toutes les machines gérées par Autoscale restent dans l'état dans lequel elles se trouvent au moment de la désactivation.
> - Une fois que vous avez désactivé Autoscale, les machines en état de vidage sont retirées de l'état de vidage. Pour plus d'informations sur l'état de vidage, reportez-vous à la section État de drainage.

### Surveiller les indicateurs

Après avoir activé Autoscale pour un groupe de mise à disposition, vous pouvez surveiller les indicateurs suivants des machines gérées par Autoscale dans Director.

- Utilisation de machine
- Estimation des économies
- Notifications d'alerte pour les machines et les sessions
- État de machine
- Tendances du calculateur de charge

> **Remarque :**
>
> Lorsque vous activez initialement Autoscale pour un groupe de mise à disposition, l'affichage des données de surveillance pour ce groupe de mise à disposition peut prendre quelques minutes.
> Les données de surveillance restent disponibles si Autoscale est activé, puis désactivé pour le groupe de mise à disposition. Autoscale collecte les données de surveillance à intervalles de 5 minutes.

Pour plus d'informations sur les mesures, consultez la rubrique Surveiller les machines gérées par Autoscale.

### À savoir

Autoscale fonctionne au niveau du groupe de mise à disposition. Il est configuré par groupe de mise à disposition. Il gère uniquement les machines du groupe de mise à disposition sélectionné.

### Capacité et enregistrement d'une machine

Autoscale inclut uniquement les machines enregistrées auprès du site lors de la détermination de la capacité. Les machines sous tension non enregistrées ne peuvent pas accepter les demandes de session. Par conséquent, elles ne sont pas incluses dans la capacité globale du groupe de mise à disposition.

### Montée en charge sur plusieurs catalogues de machines

Dans certains sites, plusieurs catalogues de machines peuvent être associés à un seul groupe de mise à disposition. Autoscale met sous tension de façon aléatoire les machines de chaque catalogue afin de répondre aux besoins de calendrier ou de session.

Par exemple, un groupe de mise à disposition dispose de deux catalogues de machines : le catalogue A a trois machines sous tension et le catalogue B a une machine sous tension. Si Autoscale doit mettre sous tension une machine supplémentaire, elle peut effectuer la mise sous tension à partir du catalogue A ou du catalogue B.

### Provisioning de machines et demande de session

Le catalogue de machines associé au groupe de mise à disposition doit disposer de suffisamment de machines à mettre sous tension et hors tension lorsque la demande augmente et diminue. Si la demande de sessions dépasse le nombre total de machines enregistrées dans le groupe de mise à disposition, Autoscale garantit que toutes les machines enregistrées sont sous tension. Cependant, **Autoscale ne fournit pas de machines supplémentaires**.

### Considérations relatives à la taille des instances

Vous pouvez optimiser vos coûts si vous dimensionnez correctement vos instances dans des clouds publics. Nous vous recommandons de provisionner des instances plus petites à condition qu'elles correspondent à vos besoins en termes de performances et de capacité de charge de travail.

Les instances plus petites hébergent moins de sessions utilisateur que les instances de plus grande taille. Par conséquent, Autoscale place les machines dans l'état de drainage beaucoup plus rapidement car il faut moins de temps pour que la dernière session utilisateur soit déconnectée. Autoscale éteint donc plus rapidement les instances plus petites, réduisant ainsi les coûts.

### État de drainage

Autoscale tente de réduire le nombre de machines sous tension dans le groupe de mise à disposition en fonction de la taille du pool et du tampon de capacité configurés.

Autoscale le fait en mettant les machines excédentaires avec le moins de sessions en « état de vidage » et en les mettant hors tension lorsque toutes les sessions sont déconnectées. Ce comportement se produit lorsque la demande de sessions diminue et que le calendrier nécessite moins de machines que celles qui sont sous tension.

Autoscale place les machines excédentaires en « état de vidage » une par une :

- Si au moins deux machines ont le même nombre de sessions actives, Autoscale vide la machine qui a été mise sous tension pendant le délai de mise hors tension spécifié.

  Cela évite de placer les machines récemment mises sous tension dans l'état de vidage, car ces machines sont plus susceptibles d'avoir le moins de sessions.
- Si au moins deux machines ont été mises sous tension pendant le délai de mise hors tension spécifié, Autoscale vide ces machines une par une au hasard.

Les machines en état de vidage n'hébergent plus les lancements de nouvelle session et attendent que les sessions existantes soient déconnectées. Une machine devient candidate à l'arrêt uniquement lorsque toutes les sessions sont déconnectées. Toutefois, s'il n'y a pas de machines immédiatement disponibles pour les lancements de session, Autoscale préfère diriger les lancements de session vers une machine en état de vidage plutôt que de mettre une machine sous tension.

Une machine est retirée de l'état de vidage lorsque l'une des conditions suivantes est remplie :

- La machine est éteinte.
- Autoscale est désactivé pour le groupe de mise à disposition auquel appartient la machine.
- Autoscale utilise la machine pour répondre aux exigences de planification ou de charge. Ce cas se produit lorsque la planification (scalabilité basée sur la planification) ou la demande actuelle (scalabilité basée sur la charge) nécessite plus de machines qu'il n'y en a de disponibles.

> **Important :**
>
> S'il n'y a pas de machines immédiatement disponibles pour les lancements de session, Autoscale préfère diriger les lancements de session vers une machine en état de vidage plutôt que de mettre une machine sous tension. Une machine en état de vidage qui héberge un lancement de session reste en état de vidage.

Pour savoir quelles machines sont en état de vidage, utilisez la commande PowerShell `Get-BrokerMachine`. Par exemple : `Get-BrokerMachine -DrainingUntilShutdown $true`. Vous pouvez également utiliser la console Gérer. Voir Afficher les machines en état de drainage.

**Afficher les machines en état de drainage**

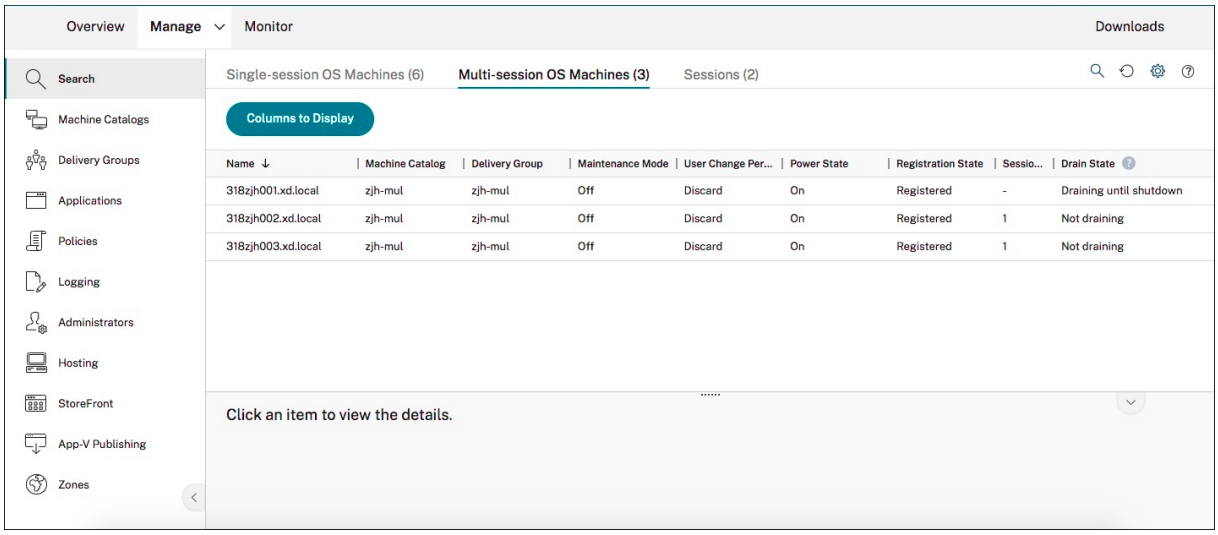
> **Remarque :**
>
> Cette fonctionnalité s'applique uniquement aux machines multi-session.

Dans Web Studio, vous pouvez afficher les machines qui sont en état de drainage, ce qui vous permet de savoir quelles machines sont sur le point de s'arrêter. Effectuez les étapes suivantes :

1. Accédez au nœud **Recherche**, puis cliquez sur **Colonnes à afficher**.
2. Dans la fenêtre **Colonnes à afficher**, activez la case à cocher **État de drainage**.
3. Cliquez sur **Enregistrer** pour quitter la fenêtre **Colonnes à afficher**.

La colonne **État de drainage** peut afficher les informations suivantes :

- **Drainage jusqu'à l'arrêt**. S'affiche lorsque les machines sont en état de drainage jusqu'à ce qu'elles soient arrêtées.
- **Pas de drainage**. Apparaît lorsque les machines ne sont pas encore en état de drainage.




### Informations supplémentaires

Pour plus d'informations sur la fonctionnalité Autoscale, consultez la section Citrix Autoscale sur Tech Zone.

## Paramètres basés sur le calendrier et sur la charge

June 27, 2024

### Comment Autoscale gère les machines

Autoscale allume et éteint les machines en fonction du calendrier sélectionné. Autoscale vous permet de définir plusieurs calendriers qui incluent des jours spécifiques de la semaine et d'ajuster le nombre de machines disponibles pendant ces périodes. Si vous savez qu'un certain groupe d'utilisateurs est susceptible de consommer les ressources de machine à un moment donné pendant des jours spécifiques, Autoscale vous permet de proposer une expérience optimisée. Notez que ces machines seront sous tension pendant la période définie par le calendrier, qu'il y ait ou non des sessions en cours d'exécution sur elles.

> **Remarque :**
>
> Autoscale prend en charge toute machine dont l'alimentation est gérée.

Le calendrier est basé sur le **fuseau horaire** du groupe de mise à disposition. Pour modifier le fuseau horaire, vous pouvez modifier les paramètres utilisateur dans un groupe de mise à disposition. Pour de plus amples informations, consultez la section Gérer les groupes de mise à disposition.

Autoscale a deux calendriers par défaut : les *jours de la semaine* (du lundi au vendredi) et le *week-end* (le samedi et le dimanche). Par défaut, le programme **Jours ouvrés** maintient une machine sous tension de 7h00 à 18h30 pendant les heures de pointe et aucune pendant les heures creuses. Le tampon de capacité par défaut est réglé à 10% pendant les heures de pointe et pendant les heures creuses. Par défaut, le programme **Weekend** ne garde pas de machines sous tension.

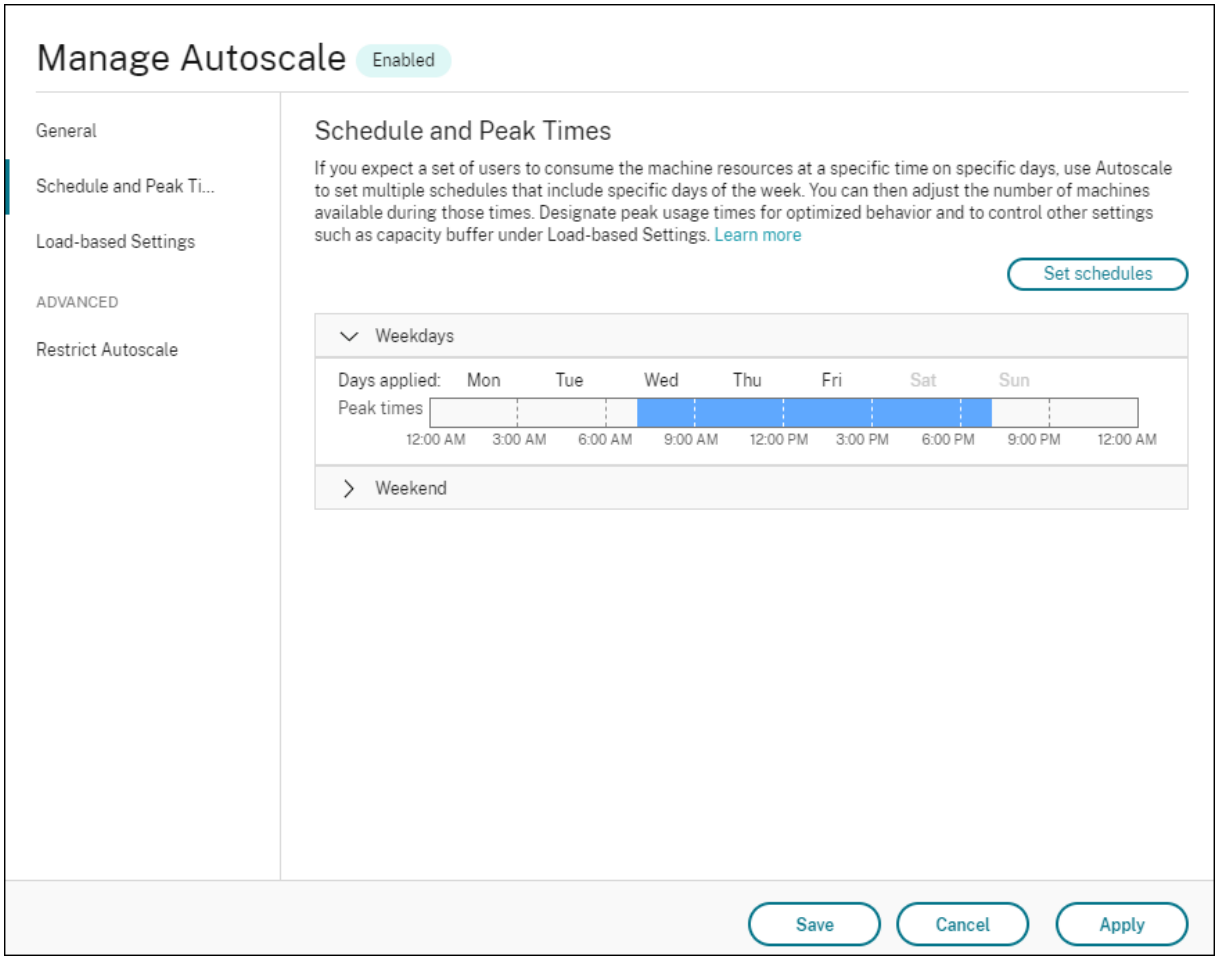
> **Remarque :**
>
> Autoscale traite uniquement les machines enregistrées sur le site comme faisant partie de la capacité disponible dans les calculs qu'il effectue. « Enregistré » signifie que la machine est disponible ou déjà utilisée. Cela garantit que seules les machines qui acceptent les sessions utilisateur sont incluses dans la capacité du groupe de mise à disposition.

### Interfaces utilisateur

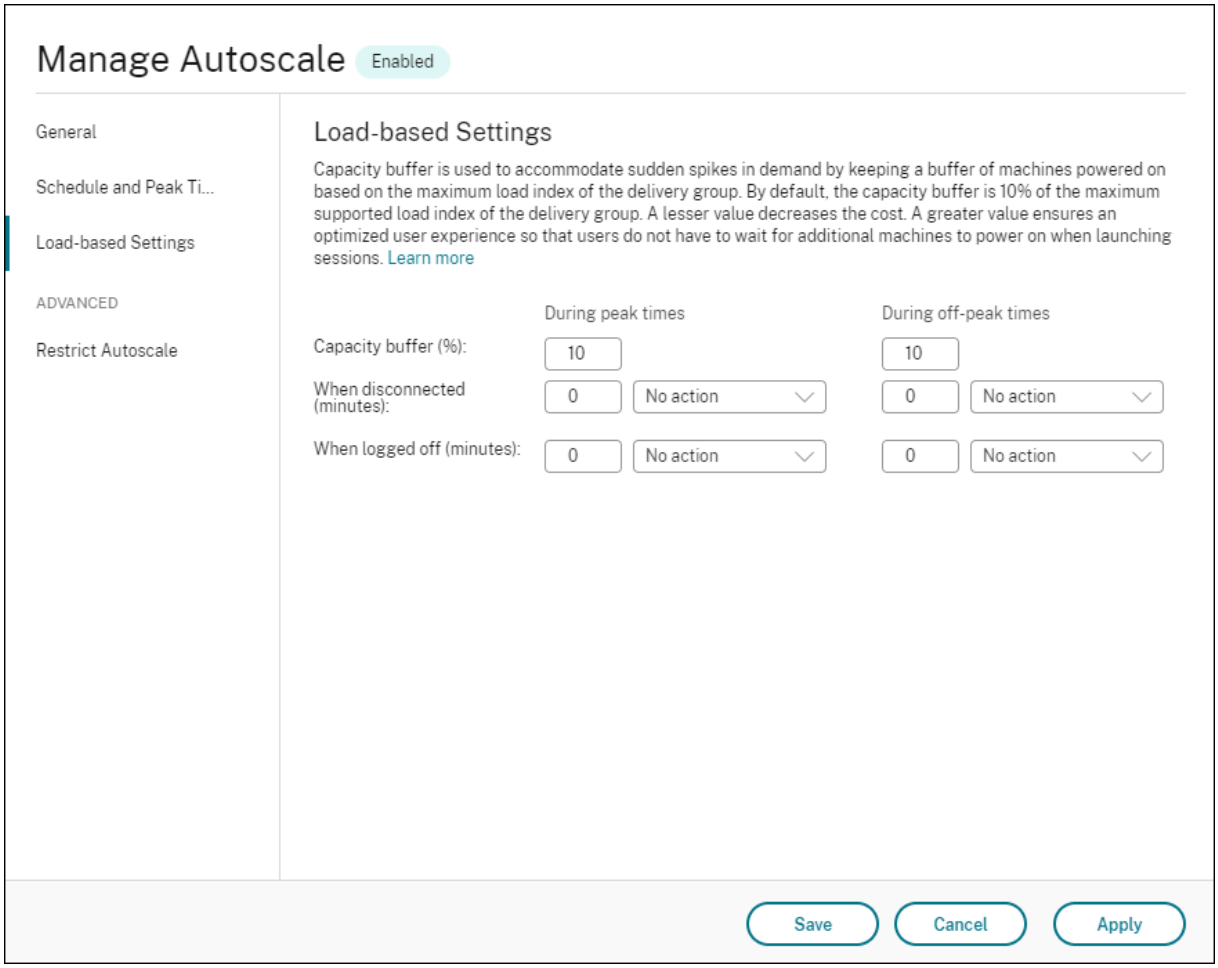
Il existe trois types d'interfaces utilisateur.

Interface utilisateur pour *groupes de mise à disposition statiques OS mono-session* :

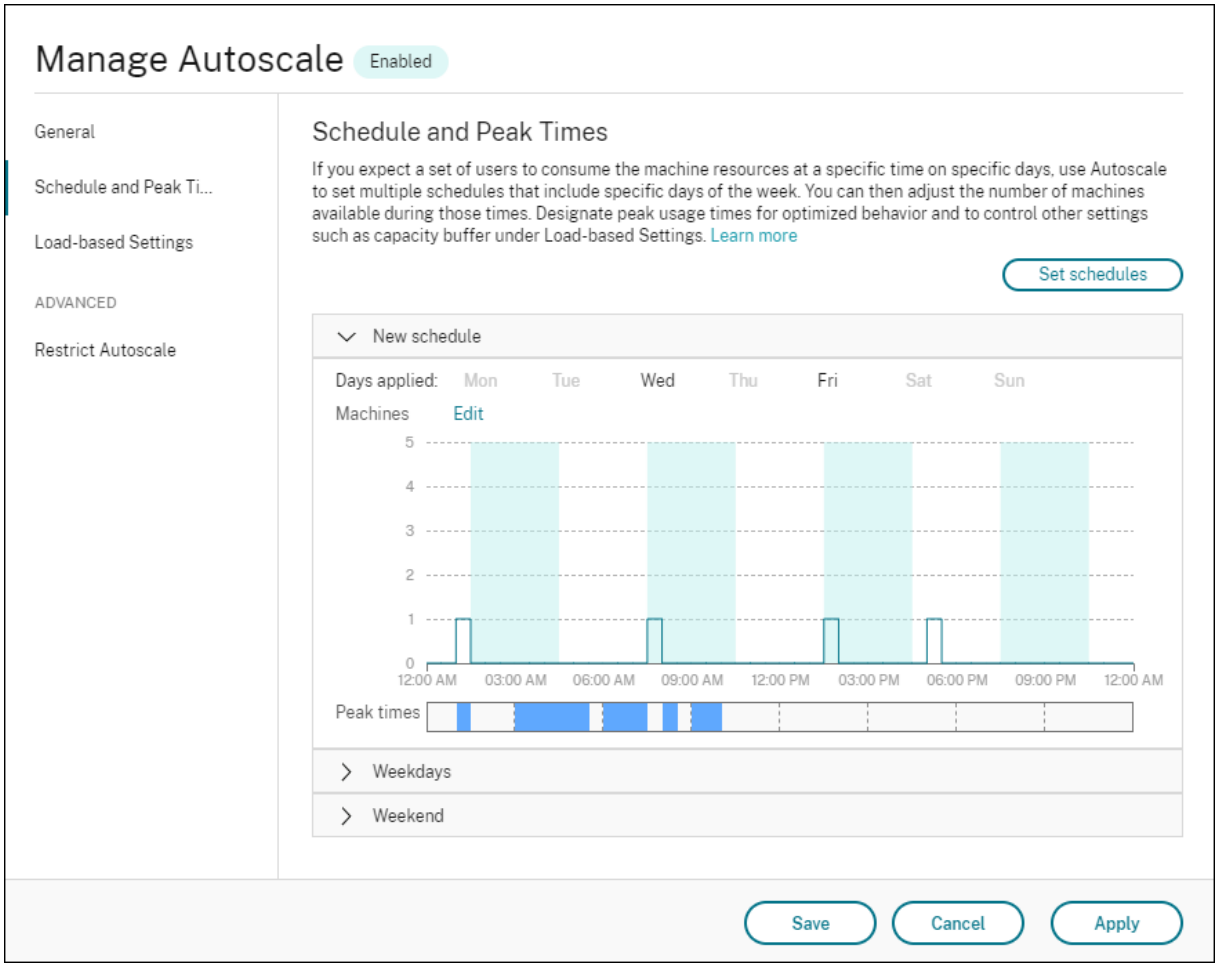


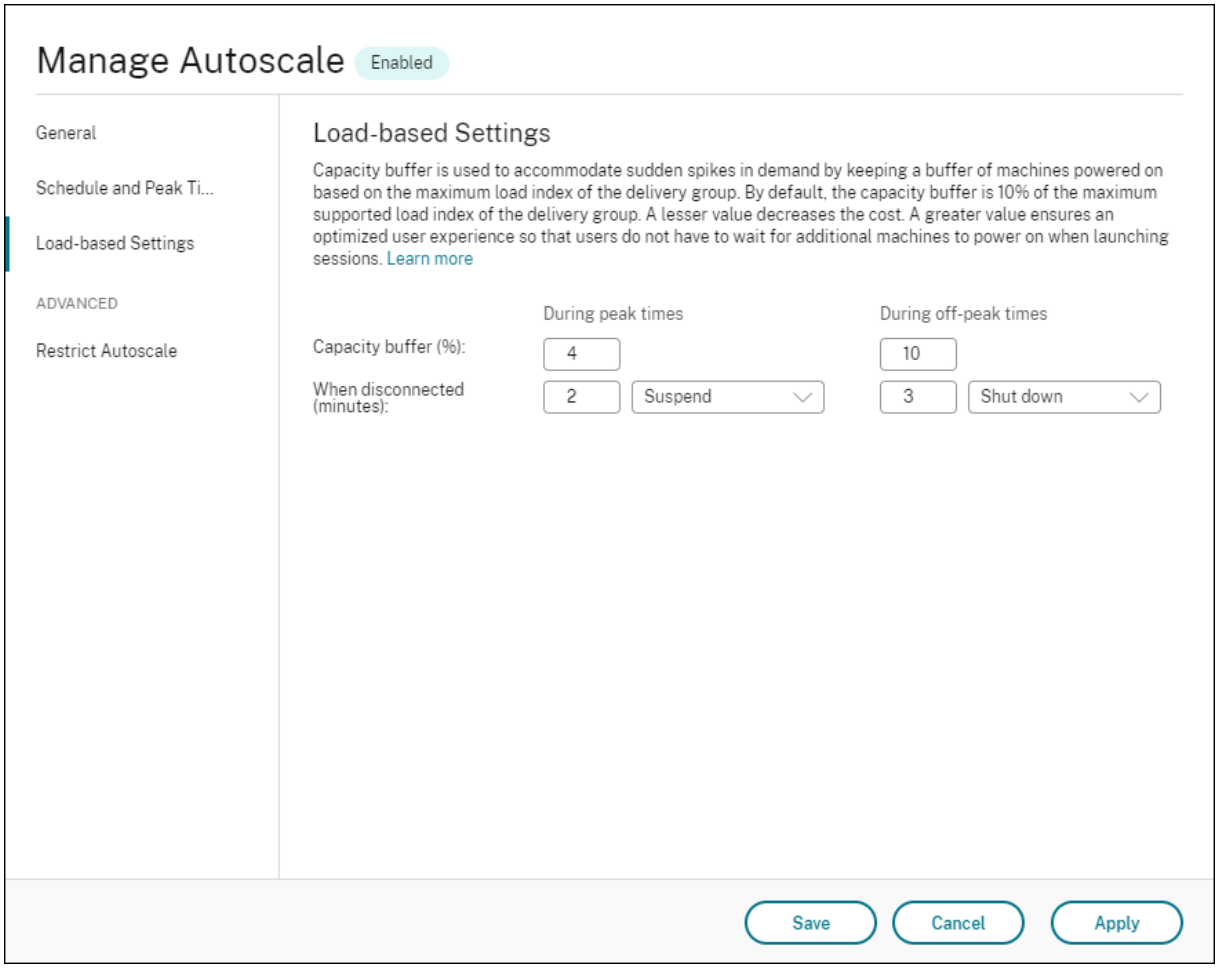



Interface utilisateur Autoscale pour *groupes de mise à disposition aléatoires OS mono-session* :

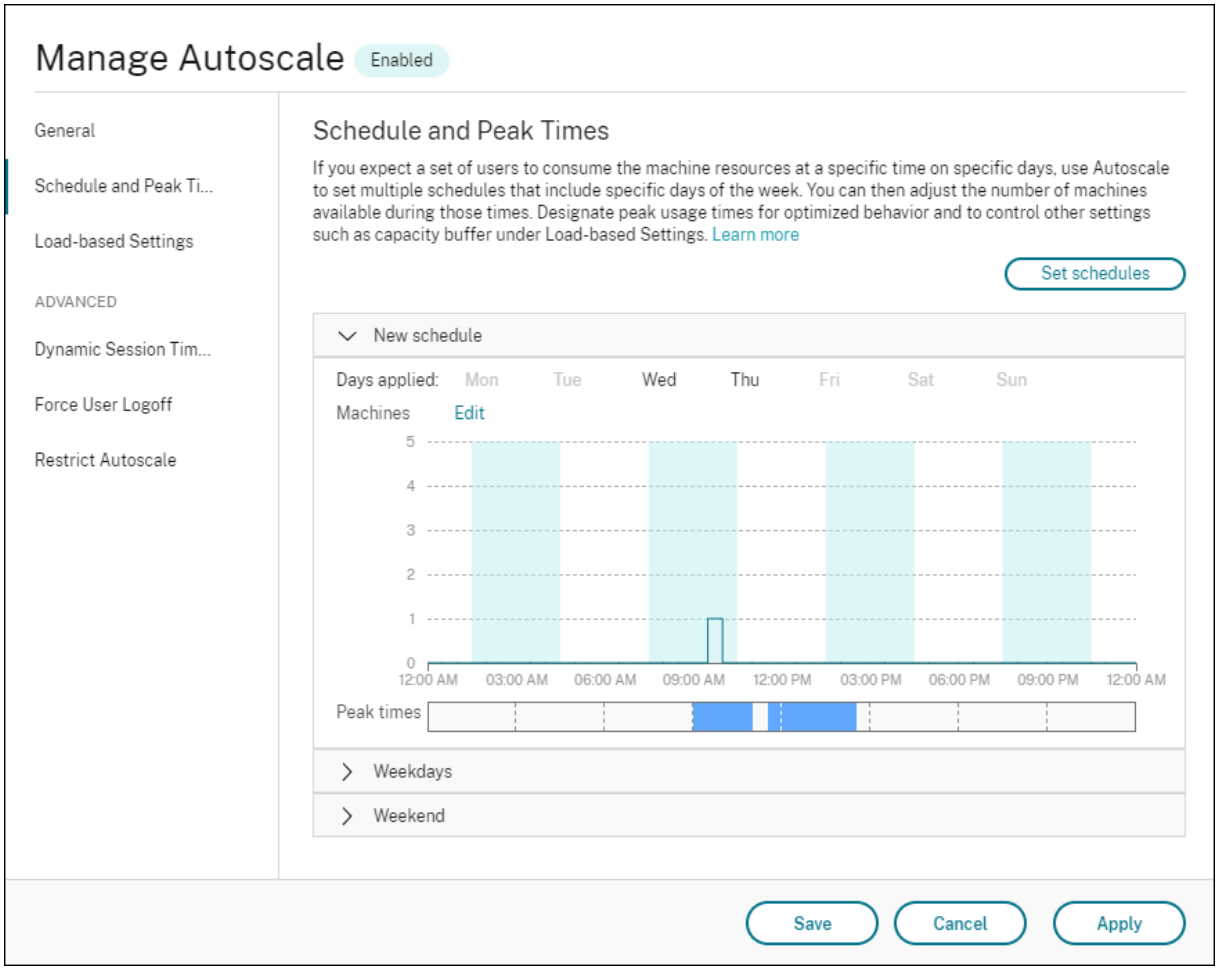


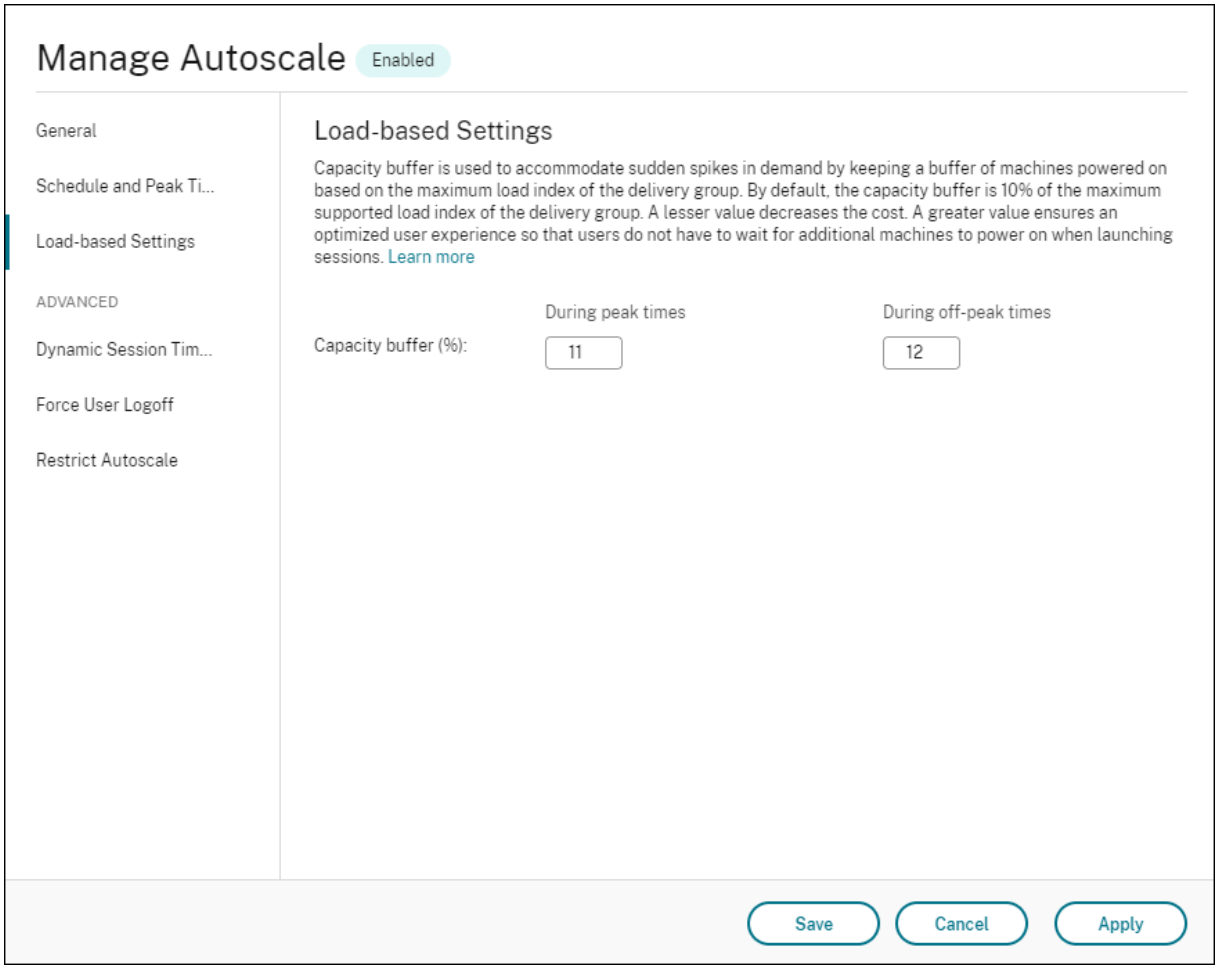



Interface utilisateur Autoscale pour *groupes de mise à disposition OS multi-session* :






### Paramètres basés sur le calendrier

**Calendrier Autoscale**. Permet d'ajouter, de modifier, de sélectionner et de supprimer des planifications.

**Jours appliqués**. Met en surbrillance les jours que vous avez appliqués au calendrier sélectionné. Les jours restants sont grisés.

**Modifier**. Permet d'affecter les machines à chaque heure ou demi-heure. Vous pouvez affecter les machines par nombres et par pourcentages.

> **Remarque :**
>
> - Cette option est disponible uniquement dans les interfaces utilisateur Autoscale pour les groupes de mise à disposition aléatoires OS multi-session et OS mono-session.
> - L'histogramme en regard de **Modifier** représente le nombre ou le pourcentage de machines exécutées dans différents créneaux horaires.
> - Vous pouvez **affecter des machines** à chaque créneau horaire en cliquant sur **Modifier**

au-dessus des **heures de pointe**. En fonction de l'option sélectionnée dans le menu de la fenêtre **Machines à démarrer**, vous pouvez affecter les machines par nombres ou par pourcentages.
- Pour les groupes de mise à disposition OS multi-session, vous pouvez définir le nombre minimum de machines en cours d'exécution séparément par incréments granulaires de 30 minutes chaque jour. Pour les groupes de mise à disposition aléatoires OS mono-session, vous pouvez définir le nombre minimum de machines en cours d'exécution séparément par incréments granulaires de 60 minutes chaque jour.

Pour définir vos propres calendriers, suivez ces étapes :

1. Sur la page **Planification et heures de pointe** de la fenêtre **Gérer Autoscale**, cliquez sur **Définir planifications**.
2. Dans la fenêtre **Modifier calendriers Autoscale**, sélectionnez les jours à appliquer à chaque calendrier. Vous pouvez également supprimer des calendriers, le cas échéant.
3. Cliquez sur **Terminé** pour enregistrer les programmes et revenir à la page **Planification et heures de pointe**.
4. Sélectionnez le calendrier applicable et configurez-le au besoin.
5. Cliquez sur **Appliquer** pour quitter la fenêtre **Gérer Autoscale** ou configurez les paramètres sur d'autres pages.

**Important :**

- Autoscale ne permet pas à un même jour de se chevaucher dans des calendriers différents. Par exemple, si vous sélectionnez Lundi dans le calendrier2 après avoir sélectionné Lundi dans le calendrier1, Lundi est automatiquement effacé dans le calendrier1.
- Un nom de calendrier n'est pas sensible à la casse.
- Un nom de calendrier ne doit pas être vide ou contenir uniquement des espaces.
- Autoscale autorise les espaces vides entre les caractères.
- Un nom de calendrier ne doit pas contenir les caractères suivants : \ / ; : # . * ? = < > | [ ] ( ) { } “ “.
- Autoscale ne prend pas en charge les noms de calendrier dupliqués. Entrez un nom différent pour chaque calendrier.
- Autoscale ne prend pas en charge les calendriers vides. Cela signifie que les calendriers sans sélection de jours ne sont pas enregistrés.

**Remarque :**

Les jours inclus dans le calendrier sélectionné sont mis en surbrillance, tandis que ceux qui ne sont pas inclus sont grisés.

### Paramètres basés sur la charge

**Heures de pointe**. Permet de définir les heures de pointe pour les jours que vous avez appliqués dans le calendrier sélectionné. Pour ce faire, cliquez avec le bouton droit sur le graphique à barres horizontales. Après avoir défini les heures de pointe, les heures restantes non définies par défaut sont les heures creuses. Par **défaut**, le créneau horaire de 7h00 à 19h00 est défini comme heures de pointe pour les jours inclus dans le calendrier sélectionné.

> **Important :**
>
> - Pour les groupes de mise à disposition OS mono-session, le graphique à barres des heures de pointe est utilisé pour le tampon de capacité.
> - Pour les groupes de mise à disposition OS mono-session, le graphique à barres des heures de pointe est utilisé pour le tampon de capacité et contrôle les actions à déclencher après la fermeture de session et/ou la déconnexion.
> - Vous pouvez définir les heures de pointe pour les jours inclus dans une planification à un niveau granulaire de 30 minutes pour les groupes de mise à disposition OS multi-session et OS mono-session. Vous pouvez également utiliser la commande New-BrokerPowerTimeScheme PowerShell à la place. Pour plus d'informations, consultez la section Commandes SDK PowerShell de Broker.

**Tampon de capacité**. Permet de conserver un tampon des machines sous tension. Une valeur moindre diminue le coût. Une valeur supérieure garantit une expérience utilisateur optimisée car les utilisateurs n'ont pas à attendre que des machines supplémentaires soient mises sous tension lors du lancement des sessions. Par défaut, le tampon de capacité est de 10 % pour les heures de pointe et les heures creuses. Si vous définissez le tampon de capacité sur 0 (zéro), les utilisateurs devront peut-être attendre que des machines supplémentaires soient mises sous tension lors du lancement des sessions. Autoscale vous permet de déterminer le tampon de capacité séparément pour les heures de pointe et les heures creuses.

### Paramètres divers

> **Conseil :**
>
> - Vous pouvez choisir de configurer les divers paramètres à l'aide du SDK Broker PowerShell. Pour plus d'informations, consultez la section Commandes SDK PowerShell de Broker.
> - Pour comprendre les commandes SDK associées aux paramètres Après déconnexion et Après fermeture de session, voir https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy.

**Après déconnexion**. Permet de spécifier combien de temps une machine déconnectée et verrouillée reste sous tension après la déconnexion d'une session avant qu'elle ne soit suspendue ou arrêtée.

Si une valeur temporelle est spécifiée, la machine est suspendue ou arrêtée lorsque le temps de déconnexion spécifié est écoulé, en fonction de l'action que vous avez configurée. Par défaut, aucune action n'est affectée aux machines déconnectées. Vous pouvez définir des actions séparément pour les heures de pointe et les heures creuses. Pour ce faire, cliquez sur la flèche vers le bas, puis sélectionnez l'une des options suivantes dans le menu :

- **Aucune action**. Si cette option est sélectionnée, la machine reste sous tension après la fermeture de session. Autoscale n'effectue pas d'action.
- **Suspendre**. Si cette option est sélectionnée, Autoscale met en pause la machine sans l'arrêter lorsque le temps de déconnexion spécifié est écoulé. L'option suivante devient disponible une fois que vous avez sélectionné **Suspendre**.
  - **Quand aucune reconnexion après (minutes)** Les machines suspendues restent disponibles pour les utilisateurs déconnectés lorsqu'ils se reconnectent, mais ne sont pas disponibles pour les nouveaux utilisateurs. Pour que les machines soient à nouveau disponibles pour gérer toutes les charges de travail, arrêtez-les. Spécifiez le délai d'expiration, en minutes, après lequel Autoscale les arrête.
- **Arrêter**. Si cette option est sélectionnée, Autoscale arrête la machine lorsque le temps de déconnexion spécifié est écoulé.

> **Remarque :**
>
> Cette option est disponible uniquement dans les interfaces utilisateur Autoscale pour les groupes de mise à disposition aléatoires et statiques OS mono-session.

**Après une fin de session**. Permet de spécifier combien de temps une machine reste sous tension après la fin d'une session avant qu'elle ne soit suspendue ou arrêtée. Si une valeur temporelle est spécifiée, la machine est suspendue ou arrêtée lorsque le temps de fin de session spécifié est écoulé, en fonction des actions que vous avez configurées. Par défaut, aucune action n'est affectée aux machines à session terminée. Vous pouvez définir des actions séparément pour les heures de pointe et les heures creuses. Pour ce faire, cliquez sur la flèche vers le bas, puis sélectionnez l'une des options suivantes dans le menu :

- **Aucune action**. Si cette option est sélectionnée, la machine reste sous tension après la fermeture de session. Autoscale n'effectue pas d'action.
- **Suspendre**. Si cette option est sélectionnée, Autoscale met en pause la machine sans l'arrêter lorsque le temps de fin de session spécifié est écoulé.
- **Arrêter**. Si cette option est sélectionnée, Autoscale arrête la machine lorsque le temps de fin de session spécifié est écoulé.

> **Remarque :**
>
> Cette option est disponible uniquement dans l'interface utilisateur Autoscale pour les groupes de mise à disposition statiques OS mono-session.

### Gestion de l'alimentation des machines avec OS mono-session qui passent à une période différente avec des sessions déconnectées

> **Important :**
>
> - Cette amélioration s'applique uniquement aux machines avec OS mono-session avec sessions déconnectées. Elle ne s'applique pas aux machines avec OS mono-session avec sessions fermées.
> - Pour que cette amélioration prenne effet, vous devez activer Autoscale pour le groupe de mise à disposition applicable. Sinon, les actions de stratégie de déconnexion d'alimentation ne sont pas déclenchées lors de la transition.

Dans les versions antérieures, une machine avec OS mono-session en transition vers une période où une action (action de déconnexion = « **Suspend** » ou « **Shutdown** ») était requise restait sous tension. Ce scénario se produisait si la machine était déconnectée pendant une période (heures de pointe ou heures creuses) pendant laquelle aucune action (action de déconnexion = « **Nothing** ») n'était requise.

À partir de cette version, Autoscale suspend ou met hors tension la machine lorsque le temps de déconnexion spécifié est écoulé, en fonction de l'action de déconnexion configurée pour la période suivante.

Par exemple, vous configurez les stratégies d'alimentation suivantes pour un groupe de mise à disposition OS mono-session :

- Définissez `PeakDisconnectAction` sur « Nothing »
- Définissez `OffPeakDisconnectAction` sur « Shutdown »
- Définissez « OffPeakDisconnectTimeout » sur 10

> **Remarque :**
>
> Pour plus d'informations sur la stratégie d'alimentation d'action de déconnexion, reportez-vous aux sections https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy et https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Dans les versions antérieures, une machine avec OS mono-session avec une session déconnectée pendant les heures de pointe restait sous tension lorsqu'elle passait des heures de pointe aux heures creuses. À partir de cette version, les actions de stratégie `OffPeakDisconnectAction`

et `OffPeakDisconnectTimeout` sont appliquées à la machine avec mono-session lors de la transition. Par conséquent, la machine est mise hors tension 10 minutes après sa transition vers les heures creuses.

Si vous souhaitez revenir au comportement précédent (autrement dit, n'effectuer aucune action sur les machines qui passent d'heures de pointe à heures creuses ou inversement avec des sessions déconnectées), effectuez l'une des opérations suivantes :

- Définissez la valeur de Registre « LegacyPeakTransitionDisconnectedBehaviour » sur 1 (true ; active le comportement précédent). Par défaut, la valeur est 0 (false, qui déclenche la déconnexion des actions de stratégie d'alimentation lors de la transition).
  - Chemin : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Nom : LegacyPeakTransitionDisconnectedBehaviour
  - Type : REG_DWORD
  - Données : 0x00000001 (1)
- Configurez le paramètre à l'aide de la commande PowerShell `Set-BrokerServiceConfigurationDa` . Par exemple :
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Une machine doit répondre aux critères suivants avant que des actions de stratégie d'alimentation puissent lui être appliquées lors de la transition :

- A une session déconnectée.
- N'a aucune action d'alimentation en attente.
- Appartient à un groupe de mise à disposition OS mono-session qui effectue une transition vers une période différente.
- A une session qui se déconnecte pendant une certaine période (heures de pointe ou heures creuses) et effectue une transition vers une période où une action d'alimentation est affectée.

### Fonctionnement du tampon de capacité

Le tampon de capacité est utilisé pour ajouter de la capacité de réserve à la demande actuelle afin de tenir compte des augmentations dynamiques de charge. Il y a deux scénarios à connaître :

- Pour les groupes de mise à disposition OS multi-session, le tampon de capacité est défini comme un pourcentage de la capacité totale du groupe de mise à disposition en termes d'indice de charge. Pour plus d'informations sur l'indice de charge, reportez-vous à la section Indice de charge.

- Pour les groupes de mise à disposition OS mono-session, le tampon de capacité est défini comme un pourcentage de la capacité totale du groupe de mise à disposition en termes de nombre de machines.

> **Remarque :**
>
> Dans les scénarios où vous limitez Autoscale aux machines balisées, le tampon de capacité est défini comme un pourcentage de la capacité totale des machines balisées du groupe de mise à disposition en termes d'indice de charge.

Autoscale vous permet de définir le tampon de capacité séparément pour les heures de pointe et les heures creuses. Une valeur moindre dans le champ de tampon de capacité réduit le coût, car Autoscale permet de réduire la capacité de réserve. Une valeur supérieure garantit une expérience utilisateur optimisée car les utilisateurs n'ont pas à attendre que des machines supplémentaires soient mises sous tension lors du lancement des sessions. Par défaut, le tampon de capacité est de 10 %.

> **Important :**
>
> Le tampon de capacité entraîne la mise sous tension des machines lorsque la capacité totale de réserve tombe à un niveau inférieur à « X » pour cent de la capacité totale du groupe de mise à disposition. Ainsi, le pourcentage requis de capacité inutilisée est réservé.

### Groupes de mise à disposition des OS multi-sessions

#### Quand les machines sont-elles mises sous tension ?

> **Important :**
>
> Si un calendrier est sélectionné, Autoscale allume toutes les machines configurées pour être sous tension selon le calendrier. Autoscale maintient ce nombre spécifié de machines sous tension pendant toute la période du calendrier, quelle que soit la charge.

Lorsque le nombre de machines sous tension dans le groupe de mise à disposition ne peut plus répondre au tampon requis pour appliquer la capacité de tampon en termes d'indice de charge, Autoscale allume des machines supplémentaires. Par exemple, supposons que votre groupe de mise à disposition dispose de 20 machines et que 3 machines sont programmées pour être mises sous tension dans le cadre d'une montée en charge planifiée avec un tampon de capacité de 20 %. 4 machines seront sous tension lorsqu'il n'y aura pas de charge. Cela est dû au fait qu'un index de charge de 4 x 10 k est nécessaire pour le tampon ; par conséquent, au moins 4 machines doivent être sous tension. Ce cas peut se produire pendant les périodes de pointe, l'augmentation de la charge sur les machines, le lancement de nouvelles sessions, et lorsque vous ajoutez de nouvelles machines au groupe de mise à disposition. Notez que Autoscale allume uniquement les machines répondant aux critères suivants :

- Les machines ne sont pas en mode de maintenance.
- L'hyperviseur sur lequel les machines sont en cours d'exécution n'est pas en mode de maintenance.
- Les machines sont actuellement hors tension.
- Les machines n'ont aucune action d'alimentation en attente.

#### Quand les machines sont-elles mises hors tension ?

> **Important :**
>
> - Si un calendrier est sélectionné, Autoscale éteint les machines en fonction du calendrier.
> - Autoscale ne met pas hors tension les machines configurées pour être mises sous tension pendant la période du calendrier.

Lorsqu'il y a suffisamment de machines pour prendre en charge le nombre ciblé de machines sous tension (y compris le tampon) pour le groupe de mise à disposition, Autoscale éteint les machines supplémentaires. Ce cas peut se produire pendant les heures creuses, la diminution de la charge sur les machines et les déconnexions de session, et lorsque vous supprimez des machines du groupe de mise à disposition. Autoscale éteint uniquement les machines répondant aux critères suivants :

- Les machines et l'hyperviseur sur lesquels les machines sont en cours d'exécution ne sont pas en mode de maintenance.
- Les machines sont actuellement sous tension.
- Les machines sont enregistrées comme étant disponibles ou en attente d'enregistrement après le démarrage.
- Les machines n'ont pas de session active.
- Les machines n'ont aucune action d'alimentation en attente.
- Les machines satisfont au délai de mise hors tension spécifié. Cela signifie que les machines ont été mises sous tension pendant au moins « X » minutes, où « X » est le délai de mise hors tension spécifié pour le groupe de mise à disposition.

#### Exemple de scénario

Supposons que vous ayez le scénario suivant :

- **Configuration du groupe de mise à disposition**. Le groupe de mise à disposition dont Autoscale doit gérer l'alimentation contient 10 machines (M1 à M10).
- **Configuration Autoscale**

  - Le tampon de capacité est défini sur 10 %.
  - Aucune machine n'est incluse dans le calendrier sélectionné.

Le scénario est exécuté dans l'ordre suivant :

1. Aucun utilisateur ne se connecte.
2. Les sessions utilisateur augmentent.
3. D'autres sessions utilisateur démarrent.
4. La charge de session utilisateur diminue en raison de la fin de session.
5. La charge de session utilisateur diminue encore jusqu'à ce que la charge de session soit gérée uniquement par des ressources locales.

Voir ci-dessous pour plus de détails sur le fonctionnement de Autoscale dans le scénario ci-dessus.

- Pas de charge utilisateur (état initial)
  - Une machine (par exemple, M1) est sous tension. La machine est sous tension en raison du tampon de capacité configuré. Dans ce cas, 10 (nombre de machines) x 10 000 (indice de charge) x 10 % (tampon de capacité configuré) est égal à 10 000. Par conséquent, une machine est sous tension.
  - La valeur de l'indice de charge de la machine sous tension (M1) correspond à une charge de base (l'indice de charge est égal à 0).
- Le premier utilisateur ouvre une session
  - La session est dirigée pour être hébergée sur la machine M1.
  - L'indice de charge de la machine sous tension M1 augmente et la machine M1 ne correspond plus à une charge de base.
  - Autoscale commence à allumer une machine supplémentaire (M2) pour répondre à la demande en raison du tampon de capacité configuré.
  - La valeur de l'indice de charge de la machine M2 correspond à une charge de base.
- Les utilisateurs augmentent la charge
  - Les sessions sont équilibrées entre les machines M1 et M2. En conséquence, l'indice de charge des machines sous tension (M1 et M2) augmente.
  - La capacité totale de réserve est encore supérieure à 10 000 en termes d'indice de charge.
  - La valeur de l'indice de charge de la machine M2 ne correspond plus à une charge de base.
- D'autres sessions utilisateur démarrent.
  - Les sessions sont équilibrées entre les machines (M1 et M2). En conséquence, l'indice de charge des machines sous tension (M1 et M2) augmente encore.

  - Lorsque la capacité totale de réserve tombe à un niveau inférieur à 10 000 en termes d'indice de charge, Autoscale commence à allumer une machine supplémentaire (M3) pour répondre à la demande en raison du tampon de capacité configuré.
  - La valeur de l'indice de charge de la machine M3 est à une charge de base.

- Encore plus de sessions utilisateur démarrent
  - Les sessions sont équilibrées entre les machines (M1 à M3). En conséquence, l'indice de charge des machines sous tension (M1 à M3) augmente.
  - La capacité totale de réserve est supérieure à 10 000 en termes d'indice de charge.
  - La valeur de l'indice de charge de la machine M3 n'est plus à une charge de base.

- La charge de session utilisateur diminue en raison de la fin de session
  - Une fois que les utilisateurs ont mis fin à leurs sessions ou que les sessions inactives dépassent le délai, la capacité libérée sur les machines M1 à M3 est réutilisée pour héberger des sessions démarrées par d'autres utilisateurs.
  - Lorsque la capacité totale de réserve augmente à un niveau supérieur à 10 000 en termes d'indice de charge, Autoscale met l'une des machines (par exemple, M3) à l'état de vidage. Par conséquent, les sessions lancées par d'autres utilisateurs ne sont plus dirigées vers cette machine. Par exemple, la charge de l'utilisateur final augmente à nouveau ou d'autres machines deviennent les moins chargées.

- La charge de session utilisateur continue de diminuer
  - Une fois que toutes les sessions de la machine M3 sont terminées et que le délai de mise hors tension spécifié expire, Autoscale éteint la machine M3.
  - Une fois que plus d'utilisateurs mettent fin à leurs sessions, la capacité libérée sur les machines (M1 et M2) est réutilisée pour héberger des sessions démarrées par d'autres utilisateurs.
  - Lorsque la capacité totale de réserve augmente à un niveau supérieur à 10 000 en termes d'indice de charge, Autoscale met l'une des machines (par exemple, M2) à l'état de vidage. Par conséquent, les sessions lancées par d'autres utilisateurs ne sont plus dirigées vers cette machine.

- La charge de session utilisateur continue de diminuer jusqu'à ce qu'il n'y ait pas de session
  - Une fois que toutes les sessions de la machine M2 sont terminées et que le délai de mise hors tension spécifié expire, Autoscale éteint la machine M2.
  - La valeur d'indice de charge de la machine sous tension (M1) correspond à une charge de base. Autoscale ne met pas la machine M1 en état de vidage en raison du tampon de capacité configuré.

> **Remarque :**
>
> Pour les groupes de mise à disposition OS multi-session, toutes les modifications apportées au bureau sont perdues lorsque les utilisateurs mettent fin aux sessions. Toutefois, s'ils sont configurés, les paramètres spécifiques à l'utilisateur restent dans le profil utilisateur.

### Groupes de mise à disposition aléatoires OS mono-session

Le tampon de capacité est utilisé pour répondre aux pics soudains de la demande en conservant un tampon de machines sous tension en fonction du nombre total de machines dans le groupe de mise à disposition. Par défaut, le tampon de capacité représente 10 % du nombre total de machines dans le groupe de mise à disposition.

Si le nombre de machines (y compris le tampon de capacité) dépasse le nombre total de machines actuellement sous tension, des machines supplémentaires sont mises sous tension pour répondre à la demande. Si le nombre de machines (y compris le tampon de capacité) est inférieur au nombre total de machines actuellement sous tension, les machines excédentaires sont arrêtées ou suspendues, selon les actions que vous avez configurées.

#### Exemple de scénario

Supposons que vous ayez le scénario suivant :

- **Configuration du groupe de mise à disposition**. Le groupe de mise à disposition dont Autoscale doit gérer l'alimentation contient 10 machines (M1 à M10).
- **Configuration Autoscale**
  - Le tampon de capacité est défini sur 10 %.
  - Aucune machine n'est incluse dans le calendrier sélectionné.

Le scénario est exécuté dans l'ordre suivant :

1. Aucun utilisateur ne se connecte.
2. Les sessions utilisateur augmentent.
3. D'autres sessions utilisateur démarrent.
4. La charge de session utilisateur diminue en raison de la fin de session.
5. La charge de session utilisateur diminue encore jusqu'à ce que la charge de session soit gérée uniquement par des ressources locales.

Voir ci-dessous pour plus de détails sur le fonctionnement de Autoscale dans le scénario ci-dessus.

- Pas de charge utilisateur (état initial)

  - Une machine (M1) est sous tension. La machine est sous tension en raison du tampon de capacité configuré. Dans ce cas, 10 (nombre de machines) x 10 % (tampon de capacité configuré) est égal à 1. Par conséquent, une machine est sous tension.

- Un premier utilisateur ouvre une session
  - La première fois qu'un utilisateur ouvre une session pour utiliser un bureau, l'utilisateur se voit attribuer un bureau depuis un groupe de bureaux hébergés sur des machines sous tension. Dans ce cas, l'utilisateur se voit attribuer un bureau à partir de la machine M1.
  - Autoscale commence à allumer une machine supplémentaire (M2) pour répondre à la demande en raison du tampon de capacité configuré.
- Un deuxième utilisateur ouvre une session
  - L'utilisateur est affecté à un bureau de la machine M2.
  - Autoscale commence à allumer une machine supplémentaire (M3) pour répondre à la demande en raison de la mémoire tampon de capacité configurée.
- Un troisième utilisateur ouvre une session
  - L'utilisateur se voit attribuer un bureau à partir de la machine M3.
  - Autoscale commence à allumer une machine supplémentaire (M4) pour répondre à la demande en raison de la mémoire tampon de capacité configurée.
- Un utilisateur se déconnecte
  - Une fois qu'un utilisateur se déconnecte ou que le bureau de l'utilisateur expire, la capacité libérée (par exemple, M3) est disponible en tant que tampon. En conséquence, Autoscale commence à éteindre la machine M4 car le tampon de capacité est configuré sur 10 %.
- Plus d'utilisateurs se déconnectent jusqu'à ce qu'il n'y ait aucun utilisateur
  - Une fois que plus d'utilisateurs se sont déconnectés, Autoscale éteint des machines (par exemple, M2 ou M3).
  - Même s'il n'y a plus d'utilisateurs, Autoscale n'éteint pas la machine restante (par exemple, M1) car cette machine est réservée en tant que capacité de réserve.

> **Remarque :**
>
> Pour les groupes de mise à disposition aléatoires OS mono-session, toutes les modifications apportées au bureau sont perdues lorsque les utilisateurs mettent fin aux sessions Toutefois, s'ils sont configurés, les paramètres spécifiques à l'utilisateur restent dans le profil utilisateur.

### Groupes de mise à disposition statiques OS mono-session

Le tampon de capacité est utilisé pour répondre aux pics soudains de la demande en conservant un tampon de machines non affectées sous tension en fonction du nombre total de machines non affectées dans le groupe de mise à disposition. Par défaut, le tampon de capacité représente 10 % du nombre total de machines non affectées dans le groupe de mise à disposition.

> **Important :**
>
> Une fois toutes les machines du groupe de mise à disposition affectées, le tampon de capacité ne joue plus de rôle dans la mise sous tension ou hors tension des machines.

Si le nombre de machines (y compris le tampon de capacité) dépasse le nombre total de machines actuellement sous tension, des machines supplémentaires non affectées sont mises sous tension pour répondre à la demande. Si le nombre de machines (y compris le tampon de capacité) est inférieur au nombre total de machines actuellement sous tension, les machines excédentaires sont mises hors tension ou suspendues, selon les actions que vous avez configurées.

Pour les groupes de mise à disposition statiques OS mono-session, Autoscale :

- Met les machines attribuées sous tension pendant les heures de pointe et hors tension pendant les heures creuses uniquement lorsque la propriété `AutomaticPowerOnForAssigned` du groupe de mise à disposition OS mono-session applicable est définie sur true.
- Met automatiquement sous tension une machine pendant les heures de pointe si elle est hors tension et si la propriété `AutomaticPowerOnForAssignedDuringPeak` du groupe de mise à disposition auquel elle appartient est définie sur true.

Pour comprendre le fonctionnement du tampon de capacité avec les machines attribuées, tenez compte des points suivants :

- Le tampon de capacité ne fonctionne que lorsque le groupe de mise à disposition contient au moins une machine qui n'est pas attribuée.
- Si le groupe de mise à disposition n'a pas de machines non attribuées (toutes les machines du groupe de mise à disposition sont attribuées), le tampon de capacité ne joue plus de rôle dans la mise sous tension ou hors tension des machines.
- La propriété `AutomaticPowerOnForAssignedDuringPeak` détermine si les machines attribuées sont sous tension pendant les heures de pointe. Si elle est définie sur true, Autoscale maintient les machines sous tension pendant les heures de pointe. Autoscale les alimentera également même si elles sont mises hors tension.

#### Exemple de scénario

Supposons que vous ayez le scénario suivant :

- **Configuration du groupe de mise à disposition**. Le groupe de mise à disposition dont Autoscale doit gérer l'alimentation contient 10 machines (M1 à M10).
- **Configuration Autoscale**
  - Les machines M1 à M3 sont affectées et les machines M4 à M10 ne sont pas affectées.
  - Le tampon de capacité est défini sur 10 % pour les heures de pointe et les heures creuses.
  - Selon le calendrier sélectionné, Autoscale gère les machines entre 09h00 et 18h00.

Voir ci-dessous pour plus de détails sur le fonctionnement de Autoscale dans le scénario ci-dessus.

- Début du calendrier —09h00
  - Autoscale allume les machines M1 à M3.
  - Autoscale allume une machine supplémentaire (par exemple, M4) en raison du tampon de capacité configuré. La machine M4 n'est pas affectée.
- Un premier utilisateur ouvre une session
  - La première fois qu'un utilisateur ouvre une session pour utiliser un bureau, l'utilisateur se voit attribuer un bureau depuis un groupe de bureaux hébergés sur des machines sous tension non affectées. Dans ce cas, l'utilisateur se voit attribuer un bureau à partir de la machine M4. Les ouvertures de session suivantes de cet utilisateur se connectent au bureau qui a été affecté lors de la première utilisation.
  - Autoscale commence à allumer une machine supplémentaire (par exemple, M5) pour répondre à la demande en raison du tampon de capacité configuré.
- Un deuxième utilisateur ouvre une session
  - Un bureau est affecté à l'utilisateur à partir des machines sous tension non affectées. Dans ce cas, l'utilisateur se voit attribuer un bureau à partir de la machine M5. Les ouvertures de session suivantes de cet utilisateur se connectent au bureau qui a été affecté lors de la première utilisation.
  - Autoscale commence à allumer une machine supplémentaire (par exemple, M6) pour répondre à la demande en raison de la mémoire tampon de capacité configurée.
- Les utilisateurs se déconnectent
  - Alors que les utilisateurs se déconnectent de leur bureau ou que le délai d'attente des ordinateurs de bureau est écoulé, Autoscale maintient les machines M1 à M5 sous tension entre 09h00 et 18h00. Lorsque ces utilisateurs se connectent la prochaine fois, ils se connectent au même bureau que celui qui a été affecté lors de la première utilisation.
  - La machine non assignée M6 attend de fournir un bureau à un utilisateur entrant non affecté.
- Fin du calendrier —18h00

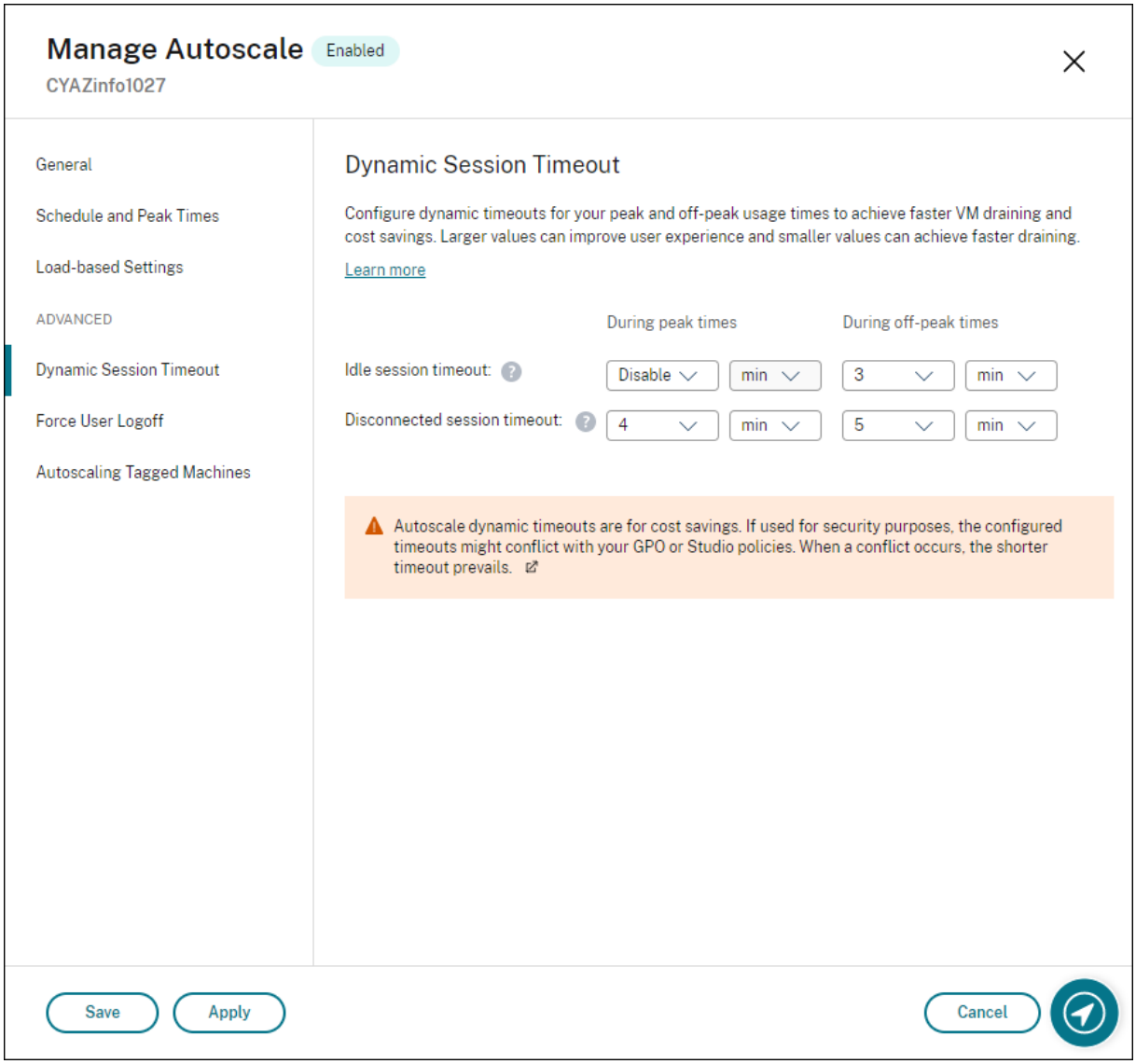
- À 18h00, Autoscale éteint les machines M1 à M5.
- Autoscale maintient la machine non affectée M6 sous tension en raison du tampon de capacité configuré. Cette machine attend de fournir un bureau à un utilisateur entrant non affecté.
- Dans le groupe de mise à disposition, les machines M6 à M10 sont des machines non affectées.

## Délai d'expiration de session dynamique

June 27, 2024

Cette fonctionnalité vous permet de configurer des délais d'expiration pour les sessions déconnectées et inactives aux heures de pointe et aux heures creuses afin d'accélérer le drainage de la machine et de réaliser des économies. Cette fonctionnalité s'applique aux machines avec OS mono-session et multi-session. Un VDA signale les temps d'inactivité pour les sessions inactives depuis plus de 10 minutes. Ainsi, les délais d'expiration de sessions dynamiques ne pourront pas déconnecter les sessions inactives dans les 10 premières minutes d'inactivité. Une valeur inférieure supprime les sessions persistantes plus tôt, réduisant ainsi les coûts.

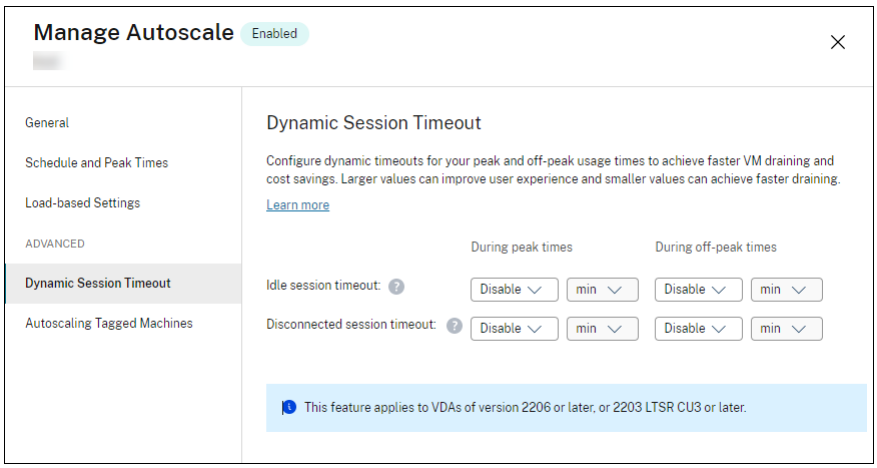
 




**Remarque :**

- Cette fonctionnalité est toujours disponible pour les groupes de mise à disposition avec OS multi-session.
- Pour les groupes de mise à disposition d'OS mono-session, cette fonctionnalité s'applique aux VDA de version 2206 CR ou ultérieure, ou 2203 LTSR CU3 ou ultérieure. Assurez-vous que ces VDA se sont enregistrés auprès de Citrix Cloud au moins une fois. Lorsque cette option n'est pas disponible, l'interface utilisateur suivante s'affiche :




- Les délais d'expiration dynamiques Autoscale permettent de réaliser des économies. S'ils sont utilisés à des fins de sécurité, les délais configurés peuvent entrer en conflit avec vos stratégies GPO ou console Gérer. En cas de conflit, le délai d'expiration le plus court prévaut.

**Délai d'expiration de session**. Active ou désactive une horloge qui détermine la durée pendant laquelle une connexion utilisateur ininterrompue est maintenue si aucune entrée utilisateur n'est effectuée. Lorsque l'horloge expire, la session est placée dans l'état déconnecté et le paramètre **Délai d'expiration de session déconnectée** s'applique. Si le paramètre **Délai d'expiration de session déconnectée** est désactivé, la session n'est pas fermée.

**Important :**

- Si vous spécifiez une valeur inférieure ou égale à 10 minutes (600 secondes), Autoscale déconnecte les sessions concernées après 10 minutes d'inactivité. En effet, Autoscale repose sur les temps d'inactivité de session signalés par les VDA. Les VDA signalent les temps d'inactivité uniquement pour les sessions inactives pendant plus de 10 minutes.
- Une session inactive sera toujours placée dans un état déconnecté si l'utilisateur est actif au cours des 5 dernières minutes suivant l'expiration du délai d'inactivité de la session.

**Délai d'expiration de session déconnectée**. Active ou désactive une horloge permettant de déterminer la durée pendant laquelle un bureau déconnecté reste verrouillé avant fermeture de la session. Si ce paramètre est activé, la session déconnectée est fermée à l'expiration de l'horloge.

## Autoscaling des machines balisées (cloud bursting)

June 27, 2024

> **Remarque :**
>
> Cette fonctionnalité était auparavant appelée Limiter Autoscale.

## Introduction

Autoscale permet de gérer l'alimentation d'un sous-ensemble de machines d'un groupe de mise à disposition. Pour ce faire, appliquez une balise à une ou plusieurs machines, puis configurez Autoscale pour gérer l'alimentation des machines balisées uniquement.

Cette fonctionnalité peut être utile dans les cas d'utilisation de poussée sur le cloud : vous souhaitez utiliser les ressources locales (ou des instances de cloud public réservées) pour gérer les charges de travail avant que les ressources basées sur le cloud répondent à une demande supplémentaire (c'est-à-dire, une poussée de charges de travail). Pour permettre aux machines locales (ou aux instances réservées) de répondre d'abord aux charges de travail, vous devez utiliser la restriction de balise ainsi que la préférence de zone.

La restriction de balise spécifie les machines qui seront gérées par Autoscale. La préférence de zone spécifie les machines de la zone préférée pour gérer les demandes de lancement de l'utilisateur. Pour plus d'informations, veuillez consulter la section Balises et Préférence de zone.

Pour activer Autoscale sur certaines machines balisées, vous pouvez utiliser la console Gérer ou PowerShell.

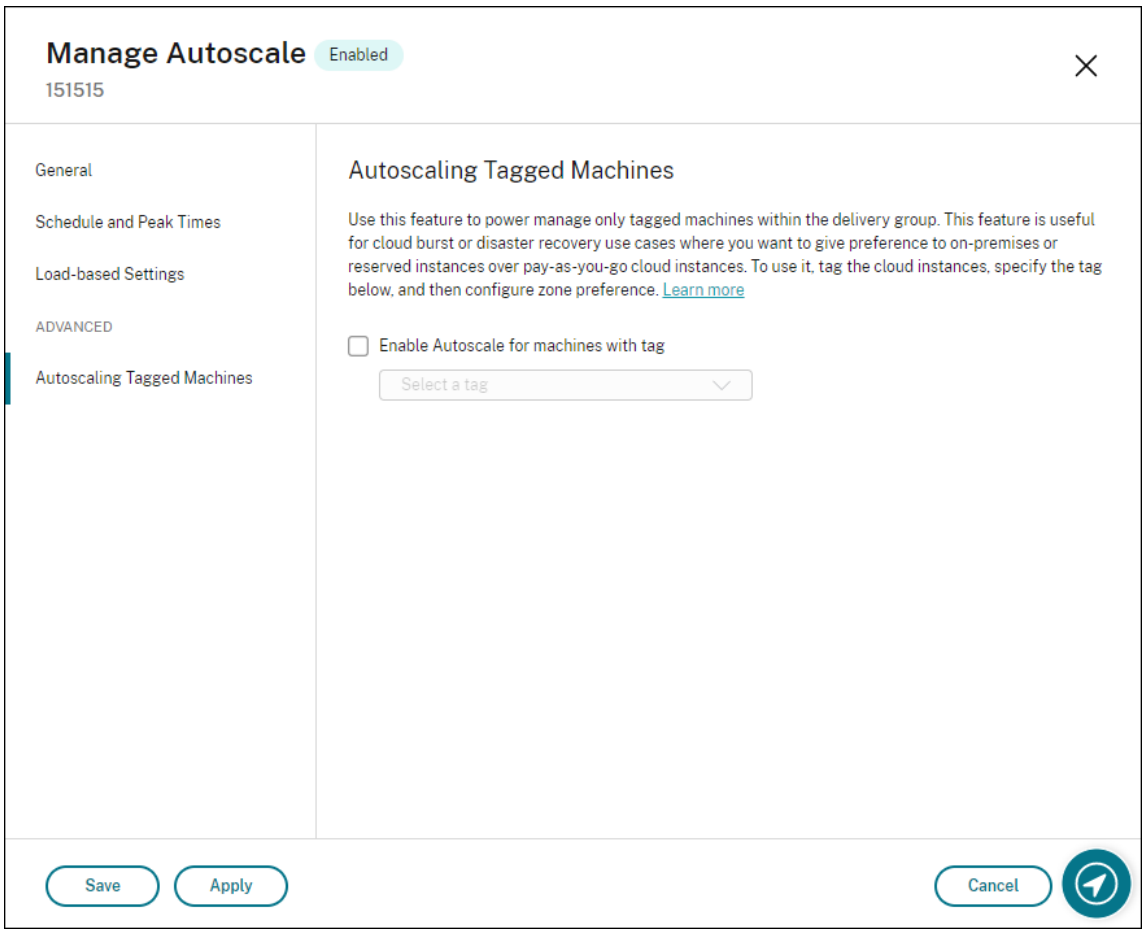
## Utiliser la console Gérer pour activer Autoscale sur certaines machines balisées

Pour activer Autoscale sur certaines machines balisées, procédez comme suit :

1. Créez une balise et appliquez cette balise aux machines applicables dans le groupe de mise à disposition. Pour plus d'informations, consultez la rubrique Gérer les balises et restrictions de balise.
2. Sélectionnez le groupe de mise à disposition, puis ouvrez l'Assistant **Gérer Autoscale**.
3. Dans la page **Autoscaling des machines balisées**, sélectionnez **Activer Autoscale pour les machines avec balise**, sélectionnez une balise dans la liste, puis cliquez sur **Appliquer** pour enregistrer vos modifications.

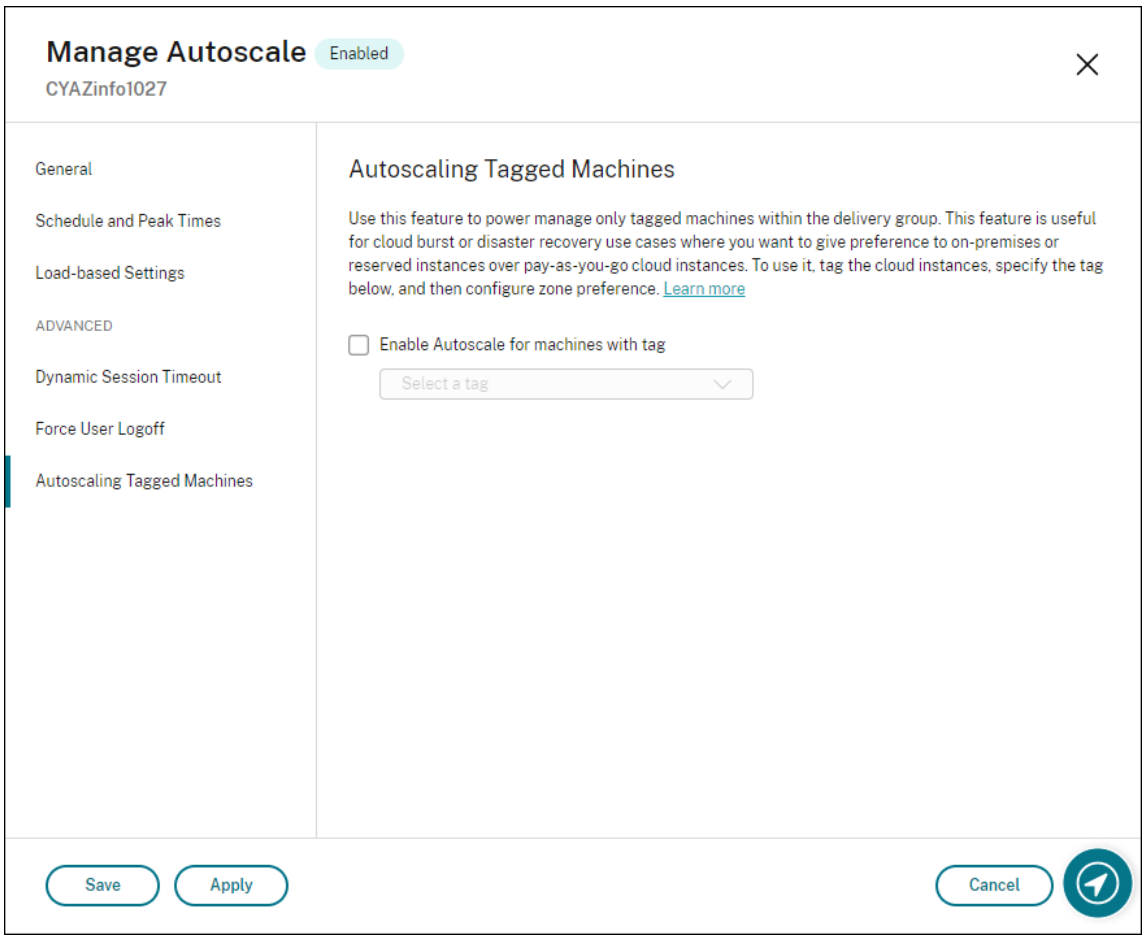
   Interface utilisateur pour les groupes de mise à disposition *statiques* et *aléatoires* des OS mono-session :




Interface utilisateur pour les *groupes de mise à disposition des OS multi-session* :




> **Avertissement :**
>
> - Activer Autoscale sur des machines associées à une balise spécifique peut entraîner la mise à jour automatique de l'histogramme afin de refléter le nombre de machines correspondant à la balise. Sur la page **Planification et heures de pointe**, vous pouvez affecter manuellement des machines à chaque créneau horaire si nécessaire.
> - Vous ne pouvez pas supprimer une balise qui est utilisée sur des machines balisées. Pour supprimer la balise, vous devez d'abord supprimer la restriction de balise.

Après avoir appliqué la restriction de balise, vous pouvez la supprimer du groupe de mise à disposition. Pour ce faire, accédez à la page **Gérer Autoscale > Autoscaling des machines balisées**, puis désactivez **Activer Autoscale pour les machines avec balise**.

> **Avertissement :**
>
> - Si vous supprimez la balise des machines applicables sans désélectionner **Activer Autoscale pour les machines avec balise**, vous pouvez recevoir un avertissement lorsque vous ouvrez l'Assistant **Gérer Autoscale**. Lorsque la balise est supprimée des machines,

> il est possible qu'Autoscale n'ait plus de machines à gérer car la balise spécifiée dans Autoscale est devenue invalide. Pour effacer l'avertissement, accédez à la page **Autoscaling des machines balisées**, supprimez la balise non valide, puis cliquez sur **Appliquer** pour enregistrer vos modifications.

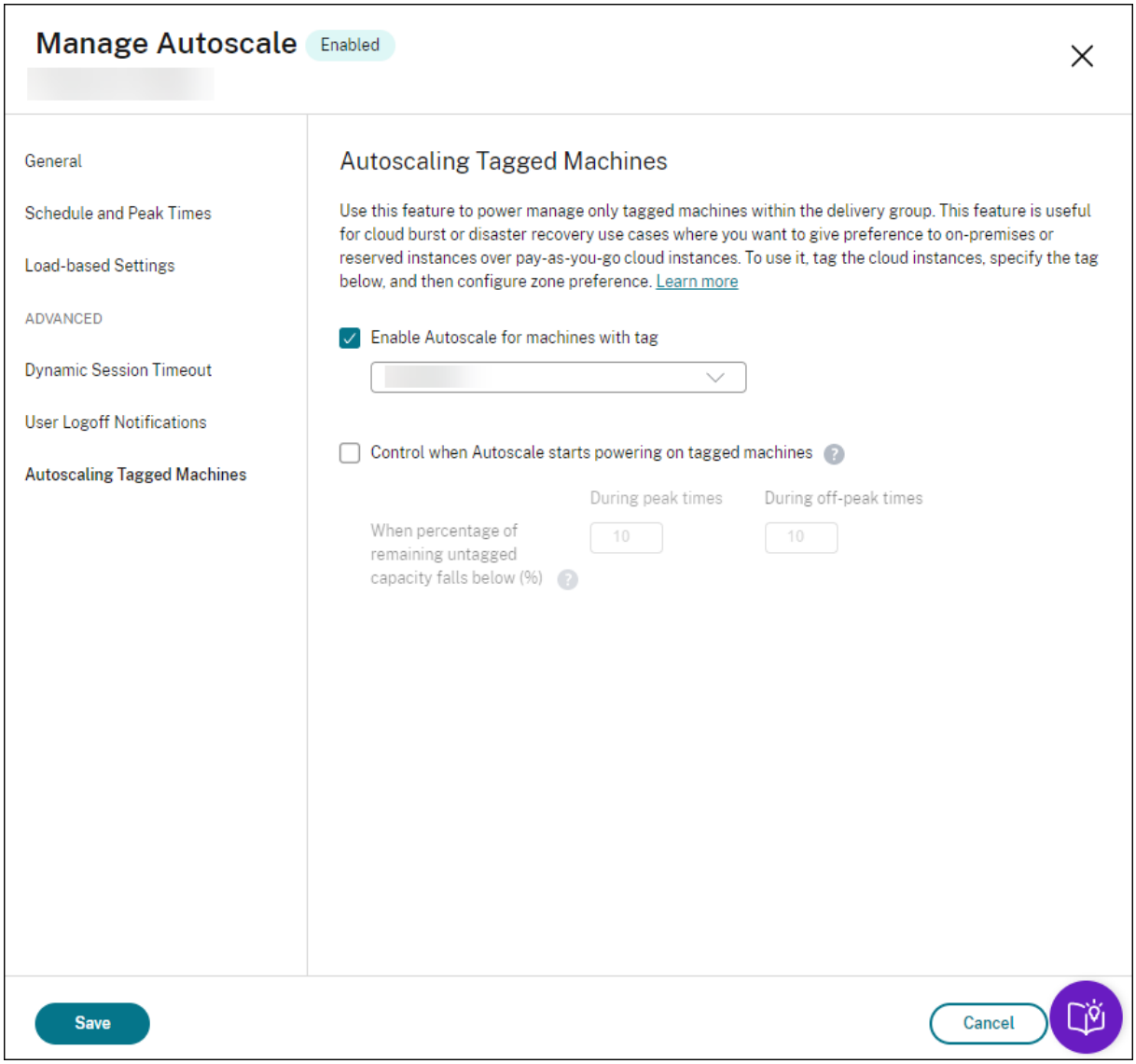
#### Contrôler le moment où Autoscale met les ressources sous tension

Vous pouvez également contrôler le moment où Autoscale démarre la mise sous tension des machines balisées en fonction de l'utilisation de machines non balisées. Cela vous permet d'optimiser davantage la consommation de vos charges de travail balisées ou de cloud public.

Pour ce faire, procédez comme suit :

1. Sur la page **Autoscaling des machines balisées**, sélectionnez **Contrôler le moment où Autoscale démarre la mise sous tension des machines balisées**.
2. Saisissez le pourcentage d'utilisation de la machine non balisée que vous souhaitez atteindre pendant les heures de pointe et les heures creuses, puis cliquez sur **Appliquer**. Valeurs prises en charge : 0 à 100.




**Conseil :**

Le pourcentage contrôle le moment où Autoscale démarre la mise sous tension des machines balisées. Lorsque le pourcentage tombe en dessous du seuil (par défaut, 10 %), Autoscale commence à mettre sous tension les machines balisées. Lorsque le pourcentage dépasse le seuil, Autoscale passe en mode hors tension. Lorsque vous saisissez le pourcentage, considérez deux scénarios :

- Pour les groupes de mise à disposition avec OS mono-session : la valeur est définie comme un pourcentage du nombre total de machines non balisées en état d'inactivité. Exemple : vous disposez de 10 machines OS mono-session non balisées. Lorsqu'il ne reste qu'une seule machine sans session, Autoscale commence à allumer une machine balisée.
- Pour les groupes de mise à disposition avec OS multi-session : la valeur est définie comme

> un pourcentage de la capacité totale (en termes d'indice de charge) de machines non balisées disponibles. Exemple : vous disposez de 10 machines OS multi-session non balisées. Lorsqu'elles sont chargées à 90 %, Autoscale commence à allumer une machine balisée.

### Utiliser PowerShell pour activer Autoscale sur certaines machines balisées

Pour utiliser directement le SDK PowerShell, procédez comme suit :

1. **Créez une balise.** Utilisez la commande New-Brokertag PowerShell pour créer une balise.
   - Par exemple : `$managed = New-BrokerTag Managed`. Dans ce cas, la balise s'appelle « Managed ». Pour plus d'informations sur la commande PowerShell New-Brokertag, voir https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/.
2. **Appliquez la balise aux machines**. Utilisez la commande PowerShell Get-Brokermachine pour appliquer la balise aux machines d'un catalogue pour lesquelles Autoscale doit gérer l'alimentation.
   - Par exemple : `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`. Dans ce cas, le catalogue s'appelle « cloud ».
   - Pour plus d'informations sur la commande PowerShell Get-Brokermachine, voir https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/.

   > **Remarque :**
   >
   > Vous pouvez ajouter de nouvelles machines au catalogue après avoir appliqué la balise. La balise n'est *PAS* appliquée automatiquement à ces nouvelles machines.

3. **Ajoutez des machines balisées au groupe de mise à disposition dont Autoscale doit gérer l'alimentation.** Utilisez la commande PowerShell Get-BrokerDesktopGroup pour ajouter une restriction de balise au groupe de mise à disposition qui contient les machines (en d'autres termes, « restreindre les lancements aux machines avec la balise X »).
   - Par exemple : `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. Dans ce cas, l'UID du groupe de mise à disposition est 1.
   - Pour plus d'informations sur la commande PowerShell Get-BrokerDesktopGroup, voir https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Après avoir appliqué la restriction de balise, vous pouvez la supprimer du groupe de mise à disposition. Pour ce faire, utilisez la commande PowerShell Get-BrokerDesktopGroup.

Exemple : `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $null`. Dans ce cas, l'UID du groupe de mise à disposition est 1.

> **Remarque :**
>
> Les machines non balisées redémarrent automatiquement après que les utilisateurs les ont éteintes. Ce comportement garantit qu'elles deviennent disponibles pour gérer les charges de travail plus tôt. Il peut être activé ou désactivé par groupe de bureaux à l'aide de la propriété `AutomaticRestartForUntaggedMachines` de `Set-BrokerDesktopGroup` Pour plus d'informations, consultez https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

### Exemple de scénario

Supposons que vous ayez le scénario suivant :

- **Configuration du catalogue de machines**. Il existe deux catalogues de machines (C1 et C2).
  - Le catalogue C1 contient 5 machines (M1 à M5) locales dans les déploiements locaux.
  - Le catalogue C2 contient 5 machines (M6 à M10) distantes dans les déploiements cloud.
- **Restriction de balise**. Une balise nommée « Cloud » est créée et appliquée aux machines M6 à M10 dans le catalogue C2.
- **Configuration de zone**. Deux zones (Z1 et Z2) sont créées.
  - La zone Z1 contenant le catalogue C1 correspond aux déploiements locaux.
  - La zone Z2 contenant le catalogue C2 correspond aux déploiements cloud.
- **Configuration du groupe de mise à disposition**.
  - Le groupe de mise à disposition contient 10 machines (M1 à M10), 5 machines du catalogue C1 (M1 à M5) et 5 du catalogue C2 (M6 à M10).
  - Les machines M1 à M5 sont mises sous tension manuellement et restent sous tension tout au long de la planification.
- **Configuration Autoscale**
  - Le tampon de capacité est défini sur 10 %.
  - Autoscale ne gère l'alimentation que des machines avec la balise « Cloud ». Dans ce cas, Autoscale gère l'alimentation des machines cloud M6 à M10.
- **Configuration des applications ou bureaux publiés**. Les préférences de zone sont configurées pour les bureaux publiés (par exemple), où la zone Z1 est préférée à la zone Z2 pour une demande de lancement utilisateur.

  - La zone Z1 est configurée comme zone préférée (zone de base) pour les bureaux publiés.

Le scénario est exécuté dans l'ordre suivant :

1. Aucun utilisateur ne se connecte.
2. Les sessions utilisateur augmentent.
3. Les sessions utilisateur continuent à augmenter jusqu'à ce que toutes les machines locales disponibles soient consommées.
4. D'autres sessions utilisateur démarrent.
5. Les sessions utilisateur diminuent en raison de fermetures de session.
6. Les sessions utilisateur continuent à diminuer jusqu'à ce que la charge de session soit gérée uniquement par des ressources locales.

Voir ci-dessous pour plus de détails sur le fonctionnement de Autoscale dans le scénario ci-dessus.

- Pas de charge utilisateur (état initial)
  - Les machines locales M1 à M5 sont toutes sous tension.
  - Une machine dans le cloud (par exemple, M6) est sous tension. La machine est sous tension en raison du tampon de capacité configuré. Dans ce cas, 10 (nombre de machines) x 10 000 (indice de charge) x 10 % (tampon de capacité configuré) est égal à 10 000. Par conséquent, une machine est sous tension.
  - La valeur de l'indice de charge de toutes les machines sous tension (M1 à M6) correspond à une charge de base (l'indice de charge est égal à 0).
- Des utilisateurs se connectent
  - Les sessions sont dirigées pour être hébergées sur les machines M1 à M5 via la préférence de zone configurée et la charge est équilibrée sur ces machines locales.
  - La valeur d'indice de charge des machines sous tension (M1 à M5) augmente.
  - La valeur d'indice de charge de la machine sous tension (M6) correspond à une charge de base.
- Les utilisateurs augmentent la charge et consomment toutes les ressources locales
  - Les sessions sont dirigées pour être hébergées sur les machines M1 à M5 via la préférence de zone configurée et la charge est équilibrée sur ces machines locales.
  - La valeur d'indice de charge de toutes les machines sous tension (M1 à M5) a atteint 10 000.
  - La valeur d'indice de charge de la machine sous tension (M6) reste sur une charge de base.
- Un utilisateur de plus se connecte
  - La session dépasse la préférence de zone et est dirigée pour être hébergée sur la machine cloud M6.

  - La valeur d'indice de charge de toutes les machines sous tension (M1 à M5) a atteint 10 000.
  - La valeur d'indice de charge de la machine sous tension (M6) augmente et ne correspond plus à une charge de base. Lorsque la capacité totale de réserve tombe à un niveau inférieur à 10 000 en termes d'indice de charge, Autoscale commence à allumer une machine supplémentaire (M7) pour répondre à la demande en raison du tampon de capacité configuré. Notez que la mise sous tension de la machine M7 peut prendre un certain temps. Il peut donc y avoir un délai avant que la machine M7 soit prête.

- Plus d'utilisateurs se connectent
  - Les sessions sont dirigées pour être hébergées sur la machine M6.
  - La valeur d'indice de charge de toutes les machines sous tension (M1 à M5) a atteint 10 000.
  - L'indice de charge de la machine M6 sous tension augmente encore, mais la capacité totale de réserve est supérieure à 10 000 en termes d'indice de charge.
  - La valeur d'indice de charge de la machine sous tension (M7) reste sur une charge de base.
- Encore plus d'utilisateurs se connectent
  - Une fois la machine M7 prête, les sessions sont dirigées pour être hébergées sur les machines M6 et M7 et la charge est équilibrée sur ces machines.
  - La valeur d'indice de charge de toutes les machines sous tension (M1 à M5) a atteint 10 000.
  - La valeur de l'indice de charge de la machine M7 n'est plus à une charge de base.
  - La valeur d'indice de charge des machines sous tension (M6 et M7) augmente.
  - La capacité totale de réserve est encore supérieure à 10 000 en termes d'indice de charge.
- La charge de session utilisateur diminue en raison de la fin de session
  - Une fois que les utilisateurs ont mis fin à leurs sessions ou que les sessions inactives dépassent le délai, la capacité libérée sur les machines M1 à M7 est réutilisée pour héberger des sessions démarrées par d'autres utilisateurs.
  - Lorsque la capacité totale de réserve augmente à un niveau supérieur à 10 000 en termes d'indice de charge, Autoscale met l'une des machines cloud (M6 à M7) à l'état de vidage. Par conséquent, les sessions lancées par d'autres utilisateurs ne sont plus dirigées vers cette machine (par exemple, M7) à moins que de nouvelles modifications ne se produisent ; par exemple, la charge de l'utilisateur augmente de nouveau ou d'autres machines cloud deviennent moins chargées.
- La charge de session utilisateur diminue encore jusqu'à ce qu'une ou plusieurs machines cloud ne soient plus nécessaires
  - Une fois que toutes les sessions de la machine M7 sont terminées et que le délai de mise hors tension spécifié expire, Autoscale éteint la machine M7.

  - La valeur d'indice de charge de toutes les machines sous tension (M1 à M5) peut tomber à un niveau inférieur à 10 000.
  - La valeur d'indice de charge de la machine sous tension (M6) diminue.

- La session utilisateur diminue encore jusqu'à ce qu'aucune machine cloud ne soit nécessaire
  - Même s'il n'y a pas de session utilisateur sur la machine M6, Autoscale ne l'éteint pas car elle sert de capacité de réserve.
  - Autoscale maintient la machine cloud restante (M6) sous tension en raison du tampon de capacité configuré. Cette machine attend de fournir un bureau à un utilisateur entrant.
  - Les sessions ne sont pas dirigées pour être hébergées sur la machine M6 tant que les machines locales ont une capacité disponible.

## Notifications de fermeture de session utilisateur (anciennement Forcer fermeture de la session utilisateur)

June 27, 2024

> **Important :**
>
> Cette fonction est disponible uniquement dans l'interface utilisateur Autoscale pour les groupes de mise à disposition multi-session basés sur les applications.

Pour optimiser les économies, la fonction Autoscale vous permet de forcer la fermeture des sessions persistantes. Cette procédure vous permet d'envoyer une notification personnalisée aux utilisateurs, ainsi qu'une période de grâce après laquelle les sessions sont forcées à être déconnectées. Cette procédure est exécutée uniquement sur les machines en mode de drainage, et non pour toutes les machines sous tension. Pour éviter toute perte de données potentielle causée par la fermeture forcée des sessions utilisateur, vous pouvez configurer cette fonctionnalité pour n'envoyer que des rappels de fermeture de session sans forcer la fermeture de la session utilisateur.

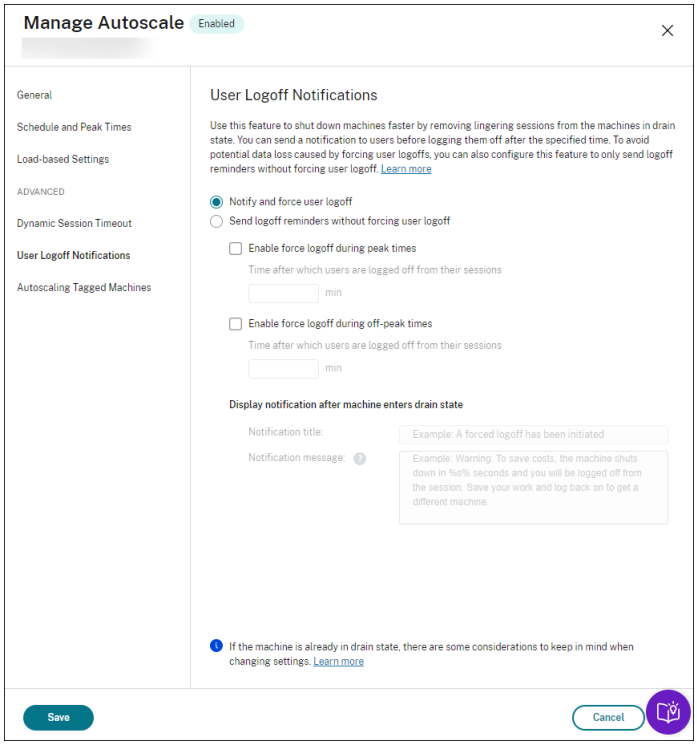
Vous disposez des deux options suivantes :

- **Notifier et forcer fermeture de la session utilisateur**
- **Envoyer des rappels de fermeture de session sans forcer l'utilisateur à se déconnecter**

### Notifier et forcer fermeture de la session utilisateur

Si cette option est sélectionnée, Autoscale déconnecte les utilisateurs de leurs sessions après les heures spécifiées ci-dessous.




**Activer déconnexion forcée pendant les heures de pointe**. Si cette option est sélectionnée, Autoscale déconnecte ces utilisateurs de leurs sessions pendant les heures de pointe lorsque le délai spécifié s'est écoulé.

**Activer déconnexion forcée pendant les heures creuses**. Si cette option est sélectionnée, Autoscale déconnecte ces utilisateurs de leurs sessions pendant les heures creuses lorsque le délai spécifié s'est écoulé.

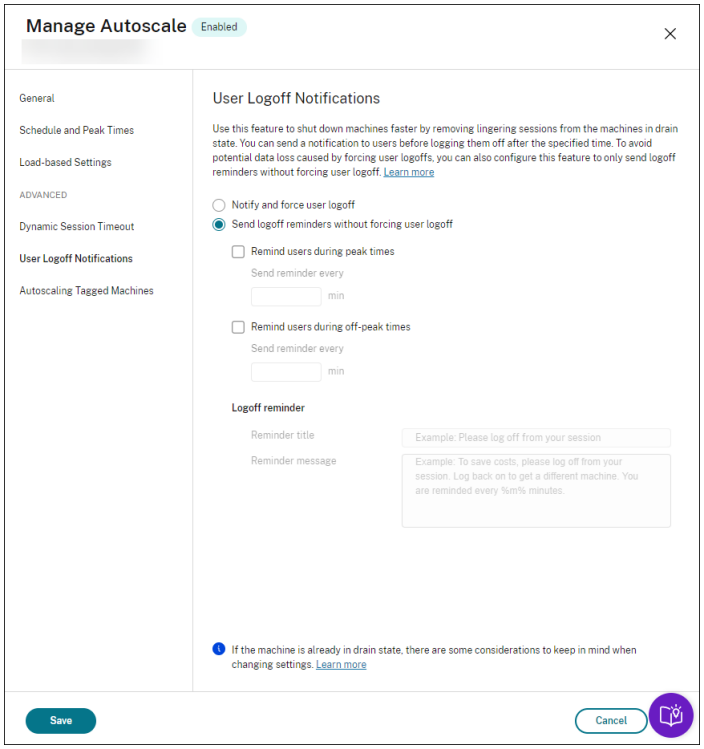
**Afficher une notification lorsque la machine passe à l'état de drainage**. Vous permet d'envoyer des notifications aux utilisateurs lorsque leur machine passe à l'état de drainage.

- **Titre de la notification**. Permet de spécifier un titre de la notification à envoyer aux utilisateurs. Exemple : `A forced logoff has been initiated.`
- **Message de notification**. Permet de spécifier le contenu de la notification à envoyer aux utilisateurs. Vous pouvez utiliser %s% ou %m% comme variables pour indiquer le délai spécifié dans le message. Pour exprimer le délai en secondes, utilisez %s%. Pour exprimer le délai en minutes, utilisez %m%. Exemple : `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine.`

### Envoyer des rappels de fermeture de session sans forcer l'utilisateur à se déconnecter

Si cette option est sélectionnée, les utilisateurs reçoivent un rappel leur demandant de se déconnecter de leur machine une fois que celle-ci est passée à l'état de drainage. Ce rappel peut être configuré pour être envoyé à l'intervalle spécifié ci-dessous.




**Envoyer un rappel aux utilisateurs pendant les heures de pointe**. Si cette option est sélectionnée, les utilisateurs reçoivent un rappel les invitant à se déconnecter de leurs sessions aux heures de pointe toutes les X minutes (X indique le délai spécifié).

**Envoyer un rappel aux utilisateurs pendant les heures creuses**. Si cette option est sélectionnée, les utilisateurs reçoivent un rappel les invitant à se déconnecter de leurs sessions aux heures creuses toutes les X minutes (X indique le délai spécifié).

**Rappel de fermeture de session**. Vous permet de configurer le rappel envoyé aux utilisateurs lorsque leur machine passe à l'état de drainage.

- **Titre du rappel**. Vous permet de spécifier un titre pour le rappel à envoyer aux utilisateurs. Exemple : `Please log off from your session`.
- **Message de rappel**. Vous permet de spécifier un message à envoyer aux utilisateurs. Exemple : `Please log off from your session and log back on to save costs`.

### Considérations

Si la machine est déjà en état de drainage, tenez compte des points suivants lors de la modification des paramètres :

- Si vous remplacez le paramètre **Envoyer des rappels de fermeture de session sans forcer l'utilisateur à se déconnecter** par **Notifier et forcer fermeture de la session utilisateur**, le nouveau paramètre prend effet immédiatement.
- Si vous remplacez le paramètre **Notifier et forcer fermeture de la session utilisateur** par **Envoyer des rappels de fermeture de session sans forcer l'utilisateur à se déconnecter**, le nouveau paramètre ne prendra effet que la prochaine fois que la machine passe à l'état de drainage. L'utilisateur est encore obligé de fermer la session.

## Commandes SDK PowerShell de Broker

June 27, 2024

Vous pouvez configurer Autoscale pour les groupes de mise à disposition à l'aide du Kit de développement logiciel (SDK) Broker PowerShell. Pour configurer Autoscale à l'aide des commandes PowerShell, vous devez utiliser le SDK PowerShell version 7.21.0.12 ou ultérieure. Pour plus d'informations sur les SDK PowerShell, consultez SDK et API.

### Set-BrokerDesktopGroup

Désactive ou active un BrokerDesktopGroup existant ou modifie ses paramètres. Pour plus d'informations sur cette applet de commande, voir https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

#### Exemples

Consultez les exemples suivants pour plus de détails sur l'utilisation des applets de commande PowerShell.

Activer Autoscale

- Supposons que vous souhaitiez activer Autoscale pour le groupe de mise à disposition dont le nom est « MyDesktop ». Utilisez la commande PowerShell `Set-BrokerDesktopGroup`. Par exemple :

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-AutoscalingEnabled
  $true
```

Configurer le tampon de capacité séparément pour les heures de pointe et les heures creuses

- Supposons que vous souhaitiez définir le tampon de capacité sur 20 % pour les heures de pointe et 10 % pour les heures creuses pour un groupe de mise à disposition dont le nom est « MyDesktop ». Utilisez la commande PowerShell `Set-BrokerDesktopGroup`. Par exemple :

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent
  20 -OffPeakBufferSizePercent 10
```

Configurer le paramètre de **délai d'expiration après déconnexion**

- Supposons que vous souhaitiez définir la valeur du **délai d'expiration après déconnexion** sur 60 minutes pour les heures de pointe et 30 minutes pour les heures creuses pour un groupe de mise à disposition dont le nom est « MyDesktop ». Utilisez la commande PowerShell `Set-BrokerDesktopGroup`. Par exemple :

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout
  60 -OffPeakDisconnectTimeout 30
```

Configurer le paramètre de **délai d'expiration après fermeture de session**

- Supposons que vous souhaitiez définir la valeur de **délai d'expiration après fermeture de session** sur 60 minutes pour les heures de pointe et 30 minutes pour les heures de pointe pour un groupe de mise à disposition dont le nom est « MyDesktop ». Utilisez la commande PowerShell `Set-BrokerDesktopGroup`. Par exemple :

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout
  60 -OffPeakLogOffTimeout 30
```

Configurer le paramètre de **délai de mise hors tension**

- Supposons que vous souhaitiez définir le délai de mise hors tension sur 15 minutes pour un groupe de mise à disposition dont le nom est « MyDesktop ». Utilisez la commande PowerShell `Set-BrokerDesktopGroup`. Par exemple :

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PowerOffDelay 15
```

Configurer une période pendant laquelle le délai de mise hors tension n'est pas appliqué

- Supposons que vous vouliez que le délai de mise hors tension soit appliqué après que 30 minutes se sont écoulées pour un groupe de mise à disposition dont le nom est « MyDesktop ». Utilisez la commande PowerShell `Set-BrokerDesktopGroup`. Par exemple :

```
- C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoSh
  30.
```

Configurer le paramètre de **coût des instances de machine**

- Supposons que vous souhaitiez définir le coût des instances de machine par heure sur 0,2 dollars pour un groupe de mise à disposition dont le nom est « MyDesktop ». Utilisez la commande PowerShell `Set-BrokerDesktopGroup`. Par exemple :

  ```
  - PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2
  ```

### New-BrokerPowerTimeScheme

Crée un BrokerPowerTimeScheme pour un groupe de mise à disposition. Pour plus d'informations, consultez https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/.

#### Exemple

Supposons que vous souhaitiez créer un schéma de temps d'alimentation pour un groupe de mise à disposition dont la valeur UID est 3. Le nouveau schéma couvre le week-end, le lundi et le mardi. Le créneau horaire de 8h00 à 18h30 est défini comme heures de pointe pour les jours inclus dans le schéma. Pour les périodes de pointe, la taille du pool (le nombre de machines maintenues sous tension) est de 20. Pour les heures creuses, il est de 5. Vous pouvez utiliser la commande PowerShell `Set-BrokerDesktopGroup`. Par exemple :

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week'-DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

### Paramètres des délais d'expiration des sessions dynamiques

Les applets de commande du SDK Broker PowerShell suivantes ont été étendues pour les délais d'expiration des sessions dynamiques en prenant en charge plusieurs nouveaux paramètres :

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

Ces paramètres incluent :

- **DisconnectPeakIdleSessionAfterSeconds** - Représente le délai en secondes après lequel une session inactive est déconnectée pendant les heures de pointe. Cette propriété a une valeur par défaut de 0, ce qui indique la désactivation de son comportement associé pendant les heures de pointe. Une valeur supérieure à 0 active son comportement pour le groupe de mise à disposition pendant les heures de pointe uniquement.
- **DisconnectOffPeakIdleSessionAfterSeconds** - Représente le délai en secondes après lequel une session inactive est déconnectée pendant les heures creuses. La valeur par défaut de cette propriété est 0, ce qui indique la désactivation de son comportement associé pendant les heures creuses. Une valeur supérieure à 0 active le comportement associé au groupe de mise à disposition pendant les heures creuses uniquement.
- **LogoffPeakDisconnectedSessionAfterSeconds** - Représente le délai en secondes après lequel une session déconnectée est terminée pendant les heures de pointe. La valeur par défaut de cette propriété est 0, ce qui indique la désactivation de son comportement associé pendant les heures de pointe. Une valeur supérieure à 0 active le comportement associé au groupe de mise à disposition pendant les heures de pointe uniquement.
- **LogoffOffPeakDisconnectedSessionAfterSeconds** - Représente le délai en secondes après lequel une session déconnectée est terminée pendant les heures creuses. La valeur par défaut de cette propriété est 0, ce qui indique la désactivation de son comportement associé pendant les heures creuses. Une valeur supérieure à 0 active le comportement associé au groupe de mise à disposition pendant les heures creuses uniquement.

#### Exemple

Supposons que vous souhaitiez définir le délai d'expiration de la session inactive à 3 600 secondes pendant les heures de pointe pour un groupe de mise à disposition dont le nom est « MyDesktop ». Utilisez la commande PowerShell `Set-BrokerDesktopGroup`. Par exemple :

- ```
  C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte
    3600
  ```

Déconnecte les sessions inactives depuis plus d'une heure en période creuse pour le groupe de bureaux dont le nom est « MyDesktop ».

## Citrix Insight Services

June 27, 2024

 
  ```

Citrix Insight Services (CIS) est une plate-forme Citrix depuis laquelle vous pouvez générer des informations d'instrumentation, de télémétrie et autres données stratégiques. Ses fonctionnalités d'instrumentation et de télémétrie permettent aux utilisateurs techniques (clients, partenaires et techniciens) de diagnostiquer et de résoudre les problèmes ainsi que d'optimiser leurs environnements. Pour plus d'informations sur CIS et son fonctionnement, veuillez consulter le site https://cis.citrix.com(informations d'identification de compte Citrix requises).

Toutes les informations chargées sur Citrix sont utilisées à des fins de dépannage et de diagnostic, ainsi que pour améliorer la qualité, la fiabilité et les performances des produits, sous réserve de ce qui suit :

- la politique Citrix Insight Services sur https://cis.citrix.com/legal
- la déclaration de confidentialité Citrix sur https://www.cloud.com/privacy-policy

Cette version de Citrix Virtual Apps and Desktops prend en charge les technologies suivantes.

- Analyses de l'installation et de la mise à niveau de Citrix Virtual Apps and Desktops
- Programme d'amélioration de l'expérience du client Citrix (CEIP)
- Citrix Call Home
- Citrix Scout

En supplément à CIS et Citrix Analytics (et séparément) : les données Google Analytics sont automatiquement collectées (et chargées plus tard) lorsque vous installez (ou mettez à niveau) Studio. Après l'installation de Studio, vous pouvez modifier ce paramètre avec la clé de Registre HKLM\Software\Citrix\DesktopStudio\GAEnabled. La valeur 1 active la collecte et le chargement, 0 désactive la collecte et le chargement.

### Installer et mettre à niveau les outils d'analyse

Lorsque vous utilisez le programme d'installation du produit complet pour déployer et mettre à niveau les composants Citrix Virtual Apps and Desktops, des informations anonymes sur le processus d'installation sont collectées et stockées sur la machine sur laquelle vous installez/mettez à niveau le composant. Ces données sont utilisées pour aider Citrix à améliorer l'expérience de ses clients avec l'installation.

Les informations sont stockées localement sous %ProgramData%\Citrix\CTQs.

Le chargement automatique de ces données est activé par défaut dans les interfaces graphique et de ligne de commande du programme d'installation du produit entier.

- Vous pouvez changer la valeur par défaut dans un paramètre de registre. Si vous modifiez le paramètre de registre avant l'installation ou la mise à niveau, cette valeur est utilisée lorsque vous utilisez le programme d'installation du produit entier.

- Vous pouvez remplacer le paramètre par défaut si vous installez ou mettez à niveau à l'aide de l'interface de ligne de commande en spécifiant une option avec la commande.

**Contrôle des téléchargements automatiques :**

- Paramètre de registre qui contrôle le chargement automatique des outils d'analyse d'installation et de mise à niveau (valeur par défaut=1) :
  - Emplacement : HKLM:\Software\Citrix\MetaInstall
  - Nom : SendExperienceMetrics
  - Valeur : 0=désactivé, 1=activé
- L'applet de commande PowerShell suivante désactive le chargement automatique des outils d'analyse d'installation et de mise à niveau :

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
    SendExperienceMetrics -PropertyType DWORD -Value 0
<!--NeedCopy-->
```

- Pour désactiver les chargements automatiques à l'aide de la commande XenDesktopServerSetup.exe ou XenDesktopVDASetup.exe, spécifiez l'option /`disableexperiencemetrics` .

  Pour activer les chargements automatiques à l'aide de la commande XenDesktopServerSetup.exe ou XenDesktopVDASetup.exe, spécifiez l'option /`sendexperiencemetrics`.

## Programme d'amélioration de l'expérience du client Citrix

Lorsque vous choisissez de participer au Programme d'amélioration de l'expérience utilisateur (CEIP), des informations d'utilisation et des statistiques anonymes sont envoyées à Citrix pour nous aider à améliorer la qualité et les performances des produits Citrix. Pour plus d'informations, consultez https://www.citrix.com/fr-fr/community/cx/ceip-fr.html.

### Inscription lors de la création ou de la mise à niveau du site

Vous êtes automatiquement inscrit au programme CEIP lorsque vous créez un site (lorsque vous installez le premier Delivery Controller). Le premier chargement de données se produit approximativement sept jours après la création du site.

Vous pouvez mettre fin à votre participation à tout moment après la création du site. Sélectionnez le nœud **Paramètres** dans le volet gauche de Web Studio et désactivez le paramètre **Programme d'amélioration de l'expérience cliente Citrix**.

Lorsque vous mettez à niveau un déploiement de Citrix Virtual Apps and Desktops :

- Si vous mettez à niveau à partir d'une version qui ne prend pas en charge le programme CEIP, le système vous demandera si vous souhaitez y prendre part.
- Si vous mettez à niveau à partir d'une version qui prend en charge le programme CEIP et que la participation a été activée, CEIP est activé dans le site mis à niveau.
- Si vous mettez à niveau à partir d'une version qui prend en charge le programme CEIP et que la participation a été désactivée, CEIP est désactivé dans le site mis à niveau.
- Si vous mettez à niveau à partir d'une version qui prend en charge le programme CEIP et que la participation est inconnue, le système vous demande si vous souhaitez y prendre part.

Les informations collectées sont anonymes, de façon à ce qu'elles ne puissent pas être consultées après leur chargement auprès de Citrix Insight Services.

#### Inscription lors de l'installation d'un VDA

Par défaut, vous êtes automatiquement inscrit au programme CEIP lorsque vous installez un VDA Windows. Vous pouvez modifier cette valeur par défaut dans un paramètre de registre. Si vous modifiez le paramètre de registre avant d'installer le VDA, cette valeur est utilisée.

Paramètre de registre qui contrôle l'inscription automatique dans CEIP (valeur par défaut=1) :

Emplacement : HKLM: \Software\Citrix\Telemetry\CEIP
Nom : Enabled
Valeur : 0 = désactivé, 1 = activé

Par défaut, la propriété `Enabled` est masquée dans le registre. Si elle n'est pas spécifiée, la fonctionnalité de chargement automatique est activée.

L'applet de commande PowerShell suivante désactive l'inscription au programme CEIP :

```
1 New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
     Enabled -PropertyType DWORD -Value 0
2 <!--NeedCopy-->
```

Les points de données d'exécution collectés sont périodiquement écrits sous forme de fichiers dans un dossier de sortie (par défaut %programdata%/Citrix/VdaCeip).

Le premier chargement de données se produit approximativement sept jours après l'installation du VDA.

#### Inscription lors de l'installation d'autres produits et composants

Vous pouvez également participer au programme CEIP lorsque vous installez des produits, composants et technologies Citrix, tels que Citrix Provisioning, AppDNA, le serveur de licences Citrix, l'application Citrix Workspace pour Windows, le serveur d'impression universelle et l'enregistrement

de session. Consultez la documentation respective de chaque composant pour de plus amples informations sur l'installation et les valeurs de participation par défaut.

## Citrix Call Home

Lors de l'installation de certains composants et fonctionnalités de Citrix Virtual Apps and Desktops, vous aurez la possibilité de participer à Citrix Call Home. Call Home collecte des données de diagnostic, puis charge périodiquement des paquets de télémétrie contenant ces données directement à Citrix Insight Services (via HTTPS sur le port 443 par défaut) à des fins d'analyse et de résolution des problèmes.

Dans Citrix Virtual Apps and Desktops, Call Home s'exécute en tant que service d'arrière-plan sous le nom Service de télémétrie Citrix. Pour plus d'informations, voir https://www.citrix.com/community/cx/call-home-fr.html.

La fonction de planification de Call Home est également disponible dans Citrix Scout. Pour plus d'informations, consultez Citrix Scout.

### Quelles informations sont collectées

Le traçage Citrix Diagnostic Facility (CDF) consigne les informations qui peuvent être utiles pour la résolution des problèmes. Call Home collecte un sous-ensemble des traces CDF qui peut être utile lors de la résolution des problèmes courants, par exemple, les enregistrements de VDA et le lancement d'application/bureau. Cette technologie est appelée traçage permanent (AOT). Les journaux AOT sont enregistrés sur le disque dans C:\Users\CitrixTelemetryService\Appdata\Local\CitrixAOT.

Call Home ne recueille pas d'autres informations de Suivi d'événements pour Windows (ETW), et ne peut pas être configuré pour le faire.

Call Home recueille également d'autres informations, telles que :

- Registres créés par Citrix Virtual Apps and Desktops sous `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Informations Infrastructure de gestion Windows (WMI) sous l'espace de noms de Citrix.
- Liste des processus en cours d'exécution.
- Vidages sur incident des processus Citrix qui sont stockés dans %PROGRAM DATA%\Citrix\CDF.
- Informations sur l'installation et la mise à niveau. Cela peut inclure le journal du metainstaller complet du produit, les journaux de MSI défaillants, la sortie de l'analyseur des journaux MSI, les journaux StoreFront, les journaux de vérification de compatibilité des licences et les résultats des tests de mise à niveau préliminaires du site.

Les informations de trace sont compressées lorsqu'elles sont collectées. Le Citrix Telemetry Service conserve un maximum de 10 Mo d'informations de traçage récentes comprimées, pendant une période maximale de huit jours.

- La compression des données permet à Call Home de limiter l'encombrement sur le VDA.
- Les traces sont stockées dans la mémoire pour éviter des opérations d'entrées/sortie sur les machines provisionnées.
- Le tampon de suivi utilise un mécanisme circulaire pour conserver les traces en mémoire.

Call Home collecte les points de données clés répertoriés dans Points de données clés Call Home.

#### Configurer et gérer : résumé

Vous pouvez vous inscrire à Call Home lors de l'utilisation de l'assistant d'installation du produit complet ou plus tard, à l'aide d'applets de commande PowerShell. Si vous vous inscrivez, par défaut, des diagnostics sont collectés et chargés vers Citrix tous les dimanches à environ 3 h 00, heure locale. Le chargement est aléatoire avec un intervalle de deux heures depuis l'heure spécifiée. Cela signifie qu'un chargement avec la programmation par défaut se produit entre 3h00 et 5h00.

Si vous ne souhaitez pas charger d'informations de diagnostic à intervalles réguliers (ou si vous souhaitez changer une planification), vous pouvez toujours utiliser les applets de commande PowerShell pour collecter et charger manuellement les diagnostics ou les stocker localement.

Si vous avez opté pour le chargement de données Call Home à intervalles réguliers et que vous chargez manuellement des informations de diagnostic sur Citrix, vous devez fournir les informations d'identification d'accès au compte Citrix ou Citrix Cloud. Citrix échange les informations d'identification contre un jeton de chargement qui est utilisé pour identifier le client et charger les données. Les informations d'identification ne sont pas enregistrées.

Lorsqu'un chargement se produit, une notification est envoyée par e-mail à l'adresse associée au compte Citrix.

Si vous activez Call Home lorsque vous installez un composant, vous pouvez le désactiver ultérieurement.

#### Logiciel requis

- La machine doit exécuter PowerShell 3.0 ou version ultérieure.
- Le Service de télémétrie Citrix doit être en cours d'exécution sur la machine.
- La variable système `PSModulePath` doit être définie sur le chemin d'installation de la télémétrie, par exemple, C:\Program Files\Citrix\Telemetry Service\.

#### Activer Call Home lors de l'installation de composants

**Lors de l'installation ou la mise à niveau de VDA :** lorsque vous installez ou mettez à niveau un VDA à l'aide de l'interface graphique du programme d'installation du produit entier, il vous est demandé si vous souhaitez participer à Call Home. Il existe deux options :

- Participer au programme Call Home
- Je ne veux pas participer au programme Call Home

Si vous mettez à niveau un VDA et êtes déjà inscrit à Call Home, cette page de l'assistant n'apparaît pas.

**Lors de l'installation ou la mise à niveau de Controller :** lorsque vous installez ou mettez à niveau un Delivery Controller à l'aide de l'interface graphique, il vous est demandé si vous souhaitez participer à Call Home. Il existe trois options :

Lorsque vous installez un Controller, vous ne pouvez pas configurer d'informations sur la page Call Home de l'assistant d'installation si le serveur possède un objet de stratégie de groupe Active Directory dans lequel le paramètre de stratégie « Ouvrir une session en tant que service » est activé. Pour plus d'informations, veuillez consulter l'article CTX218094.

Si vous mettez un Controller à niveau et êtes déjà inscrit à Call Home, vous n'êtes pas invité à participer.

#### Applets de commande PowerShell

L'aide de PowerShell fournit une syntaxe complète, y compris des descriptions des applets de commande et des paramètres qui ne sont pas utilisés dans ces cas d'utilisation courants.

Pour utiliser un serveur proxy pour les chargements, reportez-vous à la section Configurer un serveur proxy.

- **Activer des chargements programmés :** les collectes de diagnostics sont automatiquement chargées vers Citrix. Si vous n'entrez pas d'applets de commande supplémentaires pour un programme personnalisé, le programme par défaut est utilisé.

  ```
  $cred = Get-Credential
  Enable-CitrixCallHome -Credential $cred
  <!--NeedCopy-->
  ```

  Pour confirmer que les chargements programmés sont activés, entrez `Get-CitrixCallHomeGet-CitrixCallHome`. Si cette option est activée, le retour est `IsEnabled=True` et `IsMasterImage=False`.

- **Activer des chargements programmés pour des machines créées à partir d'une image principale :** l'activation de chargements programmés dans une image principale vous évite d'avoir à configurer chaque machine qui est créée dans le catalogue de machines.

  ```
  Enable-CitrixCallHome -Credential $cred -MasterImage
  ```

  Pour confirmer que les chargements programmés sont désactivés, entrez **Get-CitrixCallHome**. Si cette option est activée, le retour est `IsEnabled=True` et `IsMasterImage=True`.

- **Créer un calendrier personnalisé :** créez une planification quotidienne ou hebdomadaire pour les collectes de diagnostics et les chargements.

  ```
  $timespan = New-TimeSpan –Hours hours -Minutes minutes
  Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek day
      -UploadFrequency {
  Daily|Weekly }

  <!--NeedCopy-->
  ```

**Exemples :**

Les applets de commande suivantes créent un programme qui collecte et charge les données à 22:20 chaque soir. Le paramètre Heures utilise une horloge de 24 heures. Lorsque la valeur du paramètre `UploadFrequency` est Daily, le paramètre `DayOfWeek` est ignoré, s'il est spécifié.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
<!--NeedCopy-->
```

Pour confirmer le programme, entrez `Get-CitrixCallHomeSchedule`. Dans l'exemple précédent, la valeur suivante est renvoyée : `StartTime=22:20:00, DayOfWeek=Sunday (ignored), Upload Frequency=Daily`.

Les applets de commande suivantes créent un programme qui collecte et charge les données à 22:20 chaque mercredi soir.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -
    UploadFrequency Weekly
<!--NeedCopy-->
```

Pour confirmer le programme, entrez `Get-CitrixCallHomeSchedule`. Dans l'exemple précédent, la valeur suivante est renvoyée : `StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`.

### Désactiver Call Home

Vous pouvez désactiver Call Home à l'aide d'une applet de commande PowerShell ou via Citrix Scout.

Les journaux AOT sont collectés et enregistrés sur le disque, même lorsque les chargements programmés Call Home sont désactivés. (Lorsque les chargements programmés sont désactivés, les journaux AOT ne sont pas automatiquement téléchargés vers Citrix.) Vous pouvez désactiver la collecte et le stockage local des journaux AOT.

**Désactiver Call Home avec PowerShell** Après avoir exécuté l'applet de commande suivante, les données de diagnostic ne seront pas téléchargées automatiquement vers Citrix. (Vous pouvez toujours charger des données de diagnostic à l'aide de Citrix Scout ou d'applets de commande PowerShell de télémétrie.)

```
Disable-CitrixCallHome
```

Pour confirmer la désactivation de Call Home, entrez `Get-CitrixCallHome`. Si cette option est désactivée, le retour est `IsEnabled=False` et `IsMasterImage=False`.

**Désactiver une planification de collecte à l'aide de Citrix Scout** Pour désactiver une planification de collecte de diagnostics à l'aide de Citrix Scout, suivez les instructions de la section Planifier des collectes. À l'étape 3, cliquez sur **Désactivé** pour annuler la planification des machines sélectionnées.

**Désactiver la collecte des journaux AOT** Après avoir exécuté l'applet de commande suivante (avec le champ `Enabled` réglé sur **`false`**), les journaux AOT ne sont pas collectés.

```
Enable-CitrixTrace -Listen'{ "trace":{ "enabled":false,"persistDirectory
":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds
":300 } } '
```

Le paramètre `Listen` contient des arguments au format JSON.

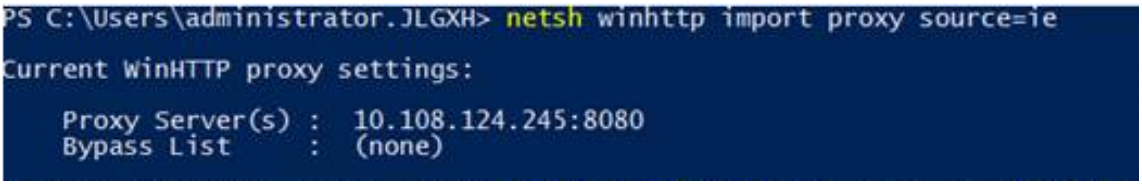
### Configurer un serveur proxy pour les chargements effectués par Call Home

Effectuez les tâches suivantes sur la machine où Call Home est activé. Les diagrammes de la procédure suivante contiennent l'adresse et le port du serveur 10.158.139.37:3128. Vos informations seront différentes.

1. Ajoutez les informations du serveur proxy dans votre navigateur. Dans Internet Explorer, sélectionnez **Options Internet > Connexions > Paramètres LAN**. Sélectionnez **Utiliser un serveur proxy pour le réseau local**, puis entrez le numéro d'adresse et le port du serveur proxy.

2. Dans PowerShell, exécutez `netsh winhttp import proxy source=ie`.




3. À l'aide d'un éditeur de texte, modifiez le fichier de configuration TelemetryService.exe, qui se trouve dans C:\Program Files\Citrix\Telemetry Service. Ajoutez les informations affichées dans la zone rouge.


4. Redémarrez le service de télémétrie.

Exécutez les applets de commande Call Home dans PowerShell.

#### Collecter et charger manuellement des informations de diagnostic

Vous pouvez utiliser le site Web CIS pour charger des packages d'informations de diagnostic sur CIS. Vous pouvez également utiliser les applets de commande PowerShell pour collecter et charger des informations de diagnostic sur CIS.

Pour charger un package à l'aide du site Web CIS :

1. Connectez-vous à Citrix Insight Services à l'aide des informations d'identification de votre compte Citrix.
2. Sélectionnez **My Workspace**.
3. Sélectionnez **Healthcheck**, puis accédez à l'emplacement de vos données.

CIS prend en charge plusieurs applets de commande PowerShell qui gèrent le chargement de données. Cette documentation couvre les applets de commande pour deux cas courants :

- Utilisez l'applet de commande `Start-CitrixCallHomeUpload` pour collecter et charger manuellement un package d'informations de diagnostic sur CIS. (Le package n'est pas enregistré localement).
- Utilisez l'applet de commande `Start-CitrixCallHomeUpload` pour collecter manuellement des données et stocker un package d'informations de diagnostic localement. Cela vous permet d'afficher un aperçu des données. Ensuite, utilisez l'applet de commande `Send-CitrixCallHomeBundle` pour charger manuellement une copie de ce package sur CIS. (Les données que vous avez enregistrées à l'origine restent locales).

L'aide de PowerShell fournit une syntaxe complète, y compris des descriptions des applets de commande et des paramètres qui ne sont pas utilisés dans ces cas d'utilisation courants.

Lorsque vous entrez une applet de commande pour charger des données sur CIS, vous êtes invité à confirmer le chargement. Si l'applet de commande expire avant que le chargement ne soit terminé, vérifiez l'état du chargement dans le journal d'événements système. La demande de chargement peut être rejetée si le service est déjà en train d'effectuer un chargement.

**Collecter des données et charger le package sur CIS :**

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath
    string] [-Description string] [-IncidentTime string] [-SRNumber
    string] [-Name string] [-UploadHeader string] [-AppendHeaders string
    ] [-Collect string] [<CommonParameters>]
<!--NeedCopy-->
```

**Collecter des données et les enregistrer localement :**

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
    Description string] [-IncidentTime string] [-SRNumber string] [-Name
     string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
    strings] [<CommonParameters>]
<!--NeedCopy-->
```

Les paramètres suivants sont valides :

- **Credential :** dirige le chargement sur CIS.
- **InputPath :** emplacement du fichier zip à inclure dans le package. Il peut s'agir d'un fichier supplémentaire qui vous a été demandé par l'assistance de Citrix. Veillez à inclure l'extension .zip.
- **OutputPath :** emplacement où les informations de diagnostic sont enregistrées. Ce paramètre est requis lors de l'enregistrement des données Call Home localement.
- **Description and Incident Time :** informations sur le chargement en format libre.
- **SRNumber :** numéro d'incident de l'assistance technique de Citrix.
- **Name :** nom qui identifie le package.

- **UploadHeader :** chaîne au format JSON qui spécifie les en-têtes de chargement chargés sur CIS.
- **AppendHeaders :** chaîne au format JSON qui spécifie les en-têtes ajoutés chargés sur CIS.
- **Collect :** chaîne au format JSON qui spécifie les données à collecter ou à ignorer, au format { 'collector':{'enabled':Boolean}}, où Boolean est true ou false.
  Valeurs de collecteur valides :
  - 'wmi'
  - 'process'
  - 'registry'
  - 'crashreport'
  - 'trace'
  - 'file'
  - 'msi'
  - 'localdata'
  - 'sitedata'
  - 'sfb'

  Par défaut, tous les collecteurs mis à part « sfb » sont activés.

  Le collecteur « sfb » est conçu pour être utilisé sur demande pour diagnostiquer les problèmes de Skype Entreprise. Outre le paramètre « enabled », le collecteur « sfb » prend en charge les paramètres « account » et « accounts » pour spécifier des utilisateurs cibles. Utilisez une des formules suivantes :
  - "-Collect "{'sfb':{'account':'domain\\user1'}}"
  - "-Collect "{'sfb':{'accounts':['domain\\\user1', 'domain\\\user2']}}"
- **Paramètres courants :** voir l'aide de PowerShell.

**Charger des données qui étaient préalablement enregistrées localement :**

```
Send-CitrixCallHomeBundle -Credential <PSCredentia\> -Path string [<
CommonParameters>]
```

Le paramètre `Path` spécifie l'emplacement dans lequel le package était préalablement enregistré.

**Exemples :**

L'applet de commande suivante demande le chargement des données Call Home (à l'exception des données du collecteur WMI) sur CIS. Ces données sont liées aux échecs d'enregistrement des VDA Citrix Provisioning, ce qui est indiqué à 14:30 pour le ticket de support technique de Citrix 123456. En plus des données Call Home, le fichier « c:\Diagnostics\ExtraData.zip » est incorporé au package chargé.

```
C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.
    zip" -Description "Registration failures with Citrix Provisioning
    VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "
    RegistrationFailure-021812016" -Collect "{
 'wmi':{
 'enabled':false }
  }
 " -UploadHeader "{
 'key1':'value1' }
 " -AppendHeaders "{
 'key2':'value2' }
 "
<!--NeedCopy-->
```

L'applet de commande suivante enregistre les données Call Home liées au ticket de support technique de Citrix 223344, ce qui est indiqué à 8:15. Les données enregistrées dans le fichier mydata.zip sur un partage réseau. En plus des données Call Home, le fichier« c:\Diagnostics\ExtraData.zip » sera incorporé au package enregistré.

```
C:\PS>Start-CitrixCallHomeUpload -OutputPath \mynetwork\myshare\mydata.
    zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "
    Diagnostics for incident number 223344" -IncidentTime "8:15" -
    SRNumber 223344
<!--NeedCopy-->
```

L'applet de commande suivante charge le package de données que vous avez enregistré précédemment.

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle  – Credential $cred -Path \mynetwork\
    myshare\mydata.zip
<!--NeedCopy-->
```

## Citrix Scout

June 27, 2024

### Introduction

Citrix Scout collecte des diagnostics et effectue des contrôles d'intégrité. Vous pouvez utiliser les résultats pour gérer votre déploiement Citrix Virtual Apps and Desktops. Citrix offre une analyse complète et automatique des collectes de diagnostics via Citrix Insight Services. Vous pouvez également utiliser Scout pour résoudre les problèmes, vous-même ou avec des instructions de l'assistance Citrix.

Vous pouvez charger des fichiers de collecte vers Citrix à des fins d'analyse et pour obtenir des instructions de l'assistance Citrix. Ou, vous pouvez enregistrer une collecte localement pour votre propre vérification et plus tard charger le fichier de la collecte vers Citrix pour analyse.

Scout propose les procédures suivantes :

- **Collecter :** exécute une collecte ponctuelle de diagnostics sur les machines que vous sélectionnez dans un site. Vous pouvez ensuite charger le fichier sur Citrix ou l'enregistrer localement.
- **Tracer et reproduire :** démarre une trace manuelle sur les machines que vous sélectionnez. Vous recréez ensuite les problèmes sur ces machines. Après la reproduction du problème, la trace est arrêtée. Scout collecte ensuite d'autres diagnostics et charge le fichier sur Citrix, ou enregistre le fichier localement.
- **Planifier :** planifie des collectes de diagnostics quotidiennes ou hebdomadaires à une heure spécifique, sur les machines que vous sélectionnez. Le fichier est automatiquement chargé sur Citrix.
- **Contrôle d'intégrité :** exécute des vérifications qui évaluent l'intégrité et la disponibilité du site et de ses composants. Vous pouvez exécuter des contrôles d'intégrité pour les Delivery Controller, les VDA, les serveurs StoreFront et les serveurs de licences Citrix. Si des problèmes sont détectés lors des vérifications, Scout fournit un rapport détaillé. Chaque fois que Scout démarre, il vérifie si les scripts de contrôle d'intégrité ont été mis à jour. Si de nouvelles versions sont disponibles, Scout les télécharge automatiquement, pour les utiliser lors de la prochaine exécution des contrôles d'intégrité.

> **Remarque :**
>
> Les procédures **Tracer et reproduire**, **Planifier** et **Contrôle d'intégrité** ne sont actuellement pas disponibles pour le VDA Linux.

L'interface graphique décrite dans cet article est le principal moyen d'utiliser Scout. Vous pouvez aussi utiliser PowerShell pour configurer des collectes de diagnostics ponctuelles ou planifiées et leurs chargements. Voir Call Home.

Où exécuter Scout :

- Dans un déploiement sur site, exécutez Scout à partir d'un Delivery Controller pour capturer des diagnostics ou exécuter des contrôles sur un ou plusieurs Virtual Delivery Agent (VDA), Delivery Controller, serveurs StoreFront et serveurs de licences. Vous pouvez également exécuter Scout à partir d'un VDA pour collecter les diagnostics locaux.
- Dans un environnement Citrix Cloud qui utilise Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), exécutez Scout à partir d'un VDA pour collecter les diagnostics locaux.

Le journal de l'application Scout est stocké dans `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`. Ce fichier peut être utilisé pour le dépannage.

### Quelles informations sont collectées

Les diagnostics collectés par Scout incluent des fichiers journaux de trace Citrix Diagnostic Facility (CDF). Un sous-ensemble des traces CDF appelé Suivi permanent (AOT, Always-On Tracing) est également inclus. Les informations AOT peuvent s'avérer utiles lors de la résolution de problèmes courants tels que des enregistrements de VDA et des lancements d'application ou de bureau. Aucune autre information de Suivi d'événements pour Windows (ETW) n'est collectée.

La collecte comprend :

- Entrées de registre créées par Citrix Virtual Apps and Desktops sous `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Informations Infrastructure de gestion Windows (WMI) sous l'**espace de noms de Citrix**.
- Processus qui sont en cours d'exécution.
- Vidages sur incident des processus Citrix qui sont stockés dans %PROGRAMDATA%\Citrix\CDF.
- Informations de stratégie Citrix au format CSV.
- Informations sur l'installation et la mise à niveau. La collecte peut inclure le journal du metainstaller complet du produit, les journaux de MSI défaillants, la sortie de l'analyseur des journaux MSI, les journaux StoreFront, les journaux de vérification de compatibilité des licences et les résultats des tests de mise à niveau préliminaires du site.

À propos des informations de trace :

- Les informations de trace sont compressées lorsqu'elles sont collectées, ce qui permet d'éviter l'encombrement de la machine.
- Sur chaque machine, le Citrix Telemetry Service conserve des informations de traçage récentes comprimées, pendant une période maximale de huit jours.
- À compter de Citrix Virtual Apps and Desktops 7 1808, les traces AOT sont enregistrées sur le disque local par défaut. (Dans les versions antérieures, les traces étaient conservées en mémoire.) Chemin par défaut = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`.
- À compter de Citrix Virtual Apps and Desktops 7 1811, les traces AOT enregistrées sur des partages réseau sont collectées avec d'autres diagnostics.
- Vous pouvez modifier la taille maximale (par défaut = 10 Mo) et la durée de la coupe à l'aide de l'applet de commande `Enable-CitrixTrace` ou de la chaîne de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`.
- Les traces s'ajoutent au fichier jusqu'à ce qu'il atteigne 10 % de `MaxSize`.

Pour obtenir une liste des points de données que Scout collecte, consultez la section Points de données clés Call Home.

### Configuration Scout

Scout peut être configuré pour fonctionner sur des VDA Linux. Pour plus d'informations sur le Linux VDA et la télémétrie, voir Intégrer avec Citrix Telemetry Service.

Le VDA Linux peut modifier automatiquement le port de socket `ctxtelemetry` ou le port du service de télémétrie. Si c'est le cas, vous devez configurer le port manuellement.

1. Accédez à C:\Program Files\Citrix\Telemetry Service
2. Ouvrez le fichier ScoutUI.exe.config.
3. Modifiez la valeur de LinuxVDATelemetryServicePort ou LinuxVDATelemetryWakeupPort vers ce qui a été configuré sur le VDA Linux :

- `<add key="LinuxVDATelemetryServicePort"value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort"value="7503"/>`

1. Enregistrez les modifications et fermez le fichier.
2. Ouvrez à nouveau Scout pour vous assurer qu'il charge la dernière configuration.

### A propos des vérifications de l'état de santé

Les données de vérification de l'état de santé sont stockées dans des dossiers sous `C:\ProgramData\Citrix\TelemetryService\`.

#### Contrôles d'intégrité du site

Les contrôles d'intégrité du site sont inclus dans le Environment Test Service, qui fournit une évaluation complète des services FlexCast Management Architecture (FMA). En plus de vérifier la disponibilité des services, ces contrôles recherchent d'autres indicateurs d'intégrité tels que les connexions de bases de données.

Les contrôles d'intégrité du site s'exécutent sur les Delivery Controller. Selon la taille de votre site, ces vérifications peuvent prendre jusqu'à une heure.

**Vérifications de configuration du Delivery Controller** Dans le cadre des contrôles d'intégrité du site. Les vérifications de configuration de Delivery Controller vérifient si les problèmes suivants existent, en fonction des recommandations Citrix pour les sites Virtual Apps and Desktops :

- Un ou plusieurs Delivery Controller sont en état d'échec.
- Il n'y a qu'un seul Delivery Controller sur le site.
- Les Delivery Controller sont de différentes versions

En plus de respecter les autorisations et conditions requises pour les contrôles d'intégrité, les vérifications de configuration de Delivery Controller nécessitent :

- Au moins un Controller sous tension.
- Service Broker s'exécutant sur un Controller.
- Une connexion fonctionnant entre le Controller et la base de données du site.

#### Vérifications d'état de santé du VDA

Les vérifications de l'état de santé du VDA identifient les causes possibles des problèmes courants d'enregistrement de VDA, de lancement de session et de redirection de fuseau horaire.

Pour l'enregistrement sur le VDA, Scout vérifie :

- Installation du logiciel VDA
- Appartenance au domaine de la machine VDA
- Disponibilité du port de communication VDA
- État du service VDA
- Configuration du pare-feu Windows
- Communication avec le Controller
- Synchronisation de l'heure avec le Controller
- État d'enregistrement de VDA

Pour le lancement de session sur les VDA, Scout vérifie :

- Disponibilité du port de communication de lancement de session
- État des services de lancement de sessions
- Configuration du pare-feu Windows de lancement de session
- Licences d'accès au client Remote Desktop Services du VDA
- Chemin de lancement de l'application VDA
- Paramètres du registre de lancement de session

Pour la redirection de fuseau horaire sur les VDA, Scout vérifie :

- Installation de correctifs Windows
- Installation de correctifs Citrix
- Paramètres de stratégie de groupe Microsoft
- Paramètres de stratégie de groupe Citrix

Pour Profile Management sur les VDA, Scout vérifie :

- Détection de l'hyperviseur
- Détection du provisionnement
- Citrix Virtual Apps and Desktops

- Configuration Personal vDisk
- Magasin de l'utilisateur
- Détection d'état du service Profile Management
- Test de hooking Winlogon.exe

Pour exécuter des contrôles sur Profile Management, vous devez installer et activer Profile Management sur le VDA. Pour plus d'informations sur les contrôles de configuration de Profile Management, consultez l'article du Centre de connaissances CTX132805.

#### Vérifications de l'état de santé StoreFront

Les contrôles StoreFront sont les suivants :

- Le service de domaine par défaut Citrix est en cours d'exécution
- Le service Citrix Credential Wallet est en cours d'exécution
- Connexion du serveur StoreFront au port 88 Active Directory
- Connexion du serveur StoreFront au port 389 Active Directory
- L'URL de base possède un nom de domaine complet valide
- L'adresse IP correcte de l'URL de base peut être récupérée
- Le pool d'applications IIS utilise .NET 4.0
- Le certificat est lié au port SSL pour l'URL de l'hôte
- La chaîne de certificat est complète
- Les certificats ont expiré
- Un certificat expire bientôt (dans les 30 jours)

#### Vérifications du serveur de licences

Les vérifications du serveur de licences sont les suivantes :

- Connexion au serveur de licences à partir du Delivery Controller
- État de l'accès distant du pare-feu du serveur de licences
- État du service Système de licences Citrix
- État de la période de grâce du serveur de licences
- Connexion aux ports du serveur de licences
- Le démon vendeur Citrix (CITRIX) est en cours d'exécution
- Les horloges système sont synchronisées
- Le service de licences Citrix est en cours d'exécution sous le compte de service local
- Présence du fichier `CITRIX.opt`
- Date d'éligibilité de Customer Success Services
- Mise à jour du serveur de licences Citrix

- Le certificat du serveur de licences se trouve dans le magasin racine approuvé du Delivery Controller

En plus de respecter les autorisations et conditions requises pour les contrôles d'intégrité, le serveur de licences doit être joint à un domaine. Sinon, le serveur de licences n'est pas découvert.

### Exécuter des contrôles d'intégrité

La procédure de contrôle d'intégrité comprend la sélection des machines, le démarrage de la vérification, puis l'affichage du rapport de résultats.

1. Lancer Scout. Depuis le menu **Démarrer** de la machine, sélectionnez **Citrix > Citrix Scout**. Sur la page d'ouverture, cliquez sur **Contrôle d'intégrité**.
2. Sélectionner des machines. Cliquez sur **Rechercher machine** pour découvrir des machines. La page **Sélectionner des machines** répertorie tous les VDA, Delivery Controller et serveurs de licences découverts sur le site. Vous pouvez filtrer l'affichage par nom de machine. Sélectionnez la case à cocher en regard de chaque machine à partir de laquelle vous voulez collecter des diagnostics, puis cliquez sur **Continuer**.

   Pour ajouter d'autres types de composants (tels que des serveurs StoreFront et des machines VDA), consultez Ajouter des machines manuellement et Importer des machines VDA. Vous ne pouvez pas ajouter manuellement des Citrix Provisioning Server ou des serveurs de licences.

   Scout démarre automatiquement des tests de vérification sur chaque machine sélectionnée, s'assurant ainsi que celle-ci remplit les critères répertoriés dans Tests de vérification. En cas d'échec de la vérification, un message est affiché dans la colonne **État** et la case à cocher de cette machine n'est plus sélectionnée. Vous pouvez :

   - Corriger le problème, puis sélectionner de nouveau la case à cocher de la machine. Cela déclenche une nouvelle tentative de tests de vérification.
   - Ignorer cette machine (laisser la case à cocher non sélectionnée). Les vérifications ne seront pas exécutées pour cette machine.

   Une fois les tests de vérification terminés, cliquez sur **Continuer**.
3. Exécuter les vérifications de l'état de santé sur les machines sélectionnées. Le résumé répertorie les machines sur lesquelles les tests sont exécutés (les machines que vous avez sélectionnées et qui ont réussi les tests de vérification). Cliquez sur **Démarrer la vérification**.

   Pendant et après la vérification :

   - La colonne **État** indique l'état actuel de vérification pour une machine.
   - Pour arrêter toutes les vérifications en cours, cliquez sur **Arrêter la vérification** dans le coin inférieur droit de la page. (Vous ne pouvez pas annuler le contrôle d'intégrité d'

une seule machine, uniquement toutes les machines sélectionnées. Les informations provenant des machines qui ont effectué les contrôles sont conservées.
- Lorsque les vérifications sont terminées pour toutes les machines sélectionnées, le bouton **Arrêter la vérification** dans le coin inférieur droit devient **Terminé**.
- Si une vérification échoue, vous pouvez cliquer sur **Réessayer** dans la colonne **Action**.
- Si une vérification se termine sans détection de problème, la colonne **Action** est vide.
- Si une vérification détecte des problèmes, cliquez sur **Afficher les détails** pour afficher les résultats.
- Une fois que la vérification est terminée pour toutes les machines sélectionnées, ne cliquez pas sur **Précédent**. (Si vous le faites, les résultats du contrôle sont perdus.)

4. Lorsque les vérifications sont terminées, cliquez sur **Terminé** pour revenir à la page d'ouverture de Scout.

#### Résultats de la vérification

Pour les vérifications Citrix générant des rapports, les rapports contiennent :

- Heure et date à laquelle le rapport de résultats a été généré
- Machines qui ont été vérifiées
- Conditions recherchées par le contrôle sur les machines ciblées

### Autorisations et conditions requises

Autorisations :

- Pour collecter les informations de diagnostic :
  - Vous devez être un administrateur local et un utilisateur de domaine pour chaque machine depuis laquelle vous collectez des diagnostics.
  - Vous devez disposer des permissions d'écriture dans le répertoire LocalAppData sur chaque machine.
- Pour exécuter des vérifications de l'état de santé :
  - Vous devez être membre du groupe d'utilisateurs du domaine.
  - Vous devez être administrateur complet ou avoir un rôle personnalisé avec les autorisations Lecture seule et **Exécuter les tests d'environnement** pour le site.
  - Définissez la stratégie d'exécution de script sur `RemoteSigned` au minimum pour permettre l'exécution des scripts. Par exemple : `Set-ExecutionPolicy RemoteSigned`. **Remarque :** d'autres privilèges d'exécution de script peuvent également fonctionner.

- Utilisez **Exécuter en tant qu'administrateur** lors du lancement de Scout.

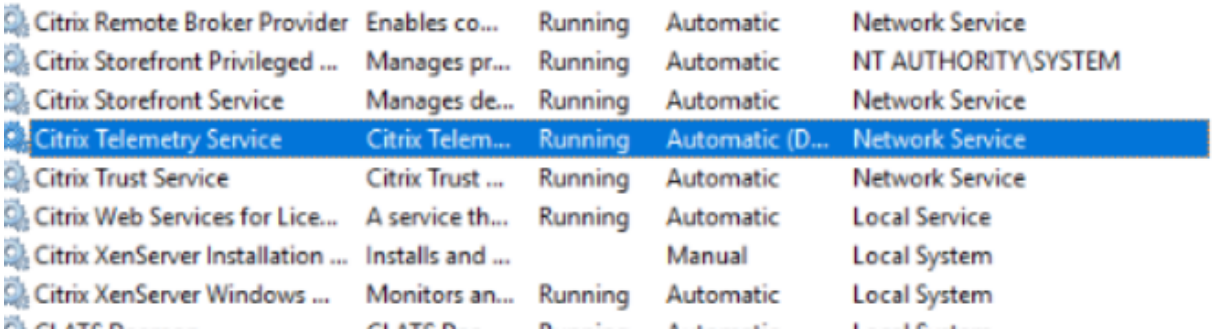
Pour chaque machine à partir de laquelle vous collectez des diagnostics ou exécutez des contrôles d'intégrité :

- Scout doit être en mesure de communiquer avec la machine.
- Le partage de fichiers et d'imprimantes doit être activé.
- PSRemoting et WinRM doivent être activés. La machine doit également exécuter PowerShell 3.0 ou version ultérieure.
- Le Service de télémétrie Citrix doit être en cours d'exécution sur la machine.
- L'accès WMI (Windows Management Infrastructure) doit être activé sur la machine.
- Pour définir une planification pour la collecte de diagnostics, la machine doit exécuter une version Scout compatible.

N'utilisez pas le signe dollar ($) dans les noms d'utilisateur spécifiés dans les noms de chemin. Il empêche la collecte d'informations de diagnostic.

Scout exécute des tests de vérification sur les machines que vous sélectionnez pour s'assurer que ces conditions sont remplies.

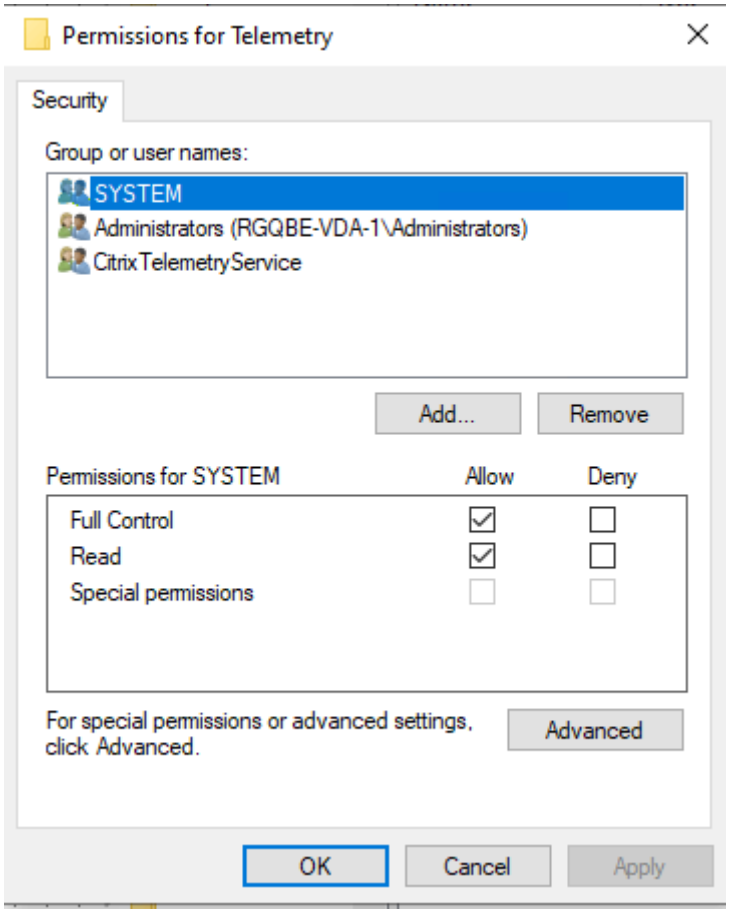
Le service de télémétrie pour Windows s'exécute sur le service réseau.




Le dossier de traces AOT est enregistré dans `C:\ProgramData\Citrix\TelemetryService\CitrixAOT`.

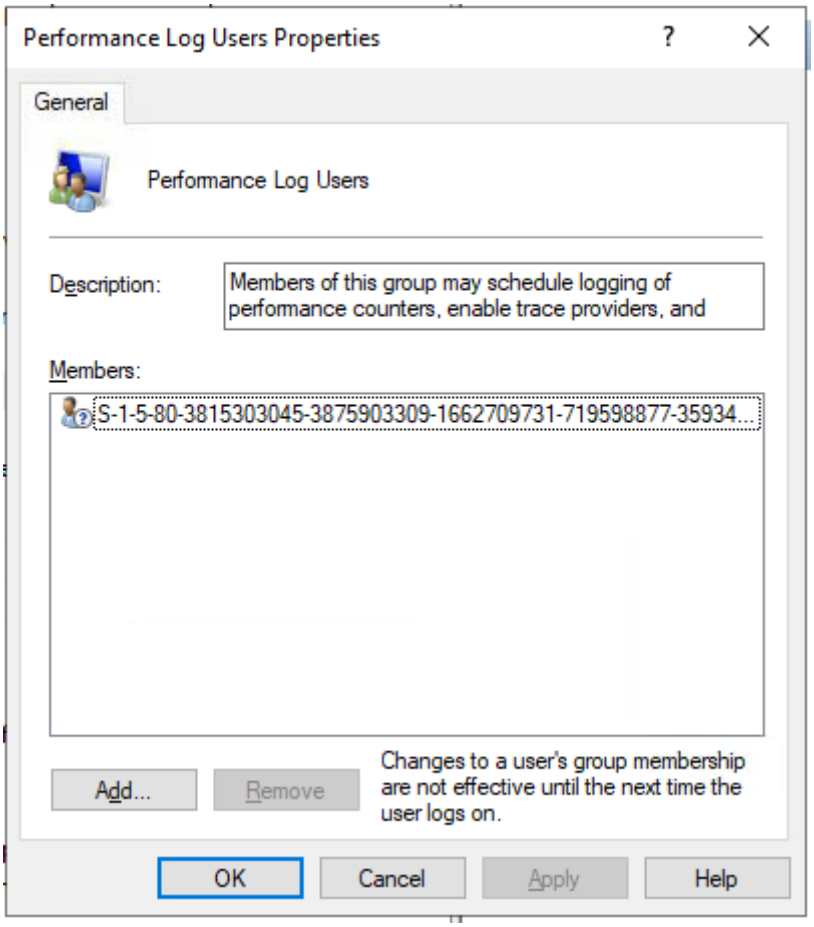
Seuls les utilisateurs du groupe Administrateur, Système et SID du service de télémétrie ont l'autorisation d'accéder au registre `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`.




Le SID du service de télémétrie reste dans le groupe Utilisateurs du journal de performances après la désinstallation du service de télémétrie, mais vous pouvez le supprimer manuellement.




### Tests de vérification

Avant le démarrage d'une collecte de diagnostics ou d'un contrôle d'intégrité, des tests de vérification sont exécutés automatiquement pour chaque machine sélectionnée. Ces tests garantissent que les conditions requises sont remplies. Si un test échoue pour une machine, Scout affiche un message avec actions correctives proposées.

- **Scout ne peut accéder à cette machine :** assurez-vous que :
  - La machine est démarrée.
  - La connexion réseau fonctionne correctement. (il peut vérifier que votre pare-feu est correctement configuré.)
  - Le partage de fichiers et d'imprimantes est activé. Consultez la documentation Microsoft pour obtenir des instructions.
- **Activer PSRemoting et WinRM :** vous pouvez activer la communication à distance PowerShell et WinRM en même temps. À l'aide de l'option **Exécuter en tant qu'administrateur**, exécutez l'applet de commande `Enable-PSRemoting`. Pour de plus amples informations, consultez l'aide de Microsoft pour l'applet de commande.

- **Scout requiert PowerShell 3.0 (minimum) :** installez PowerShell 3.0 (ou version ultérieure) sur la machine et activez la communication à distance PowerShell.
- **Impossible d'accéder au répertoire LocalAppData sur cette machine :** assurez-vous que votre compte est autorisé à écrire sur le répertoire LocalAppData de cette machine.
- **Impossible de trouver Citrix Telemetry Service :** assurez-vous que le service de télémétrie Citrix Telemetry Service est installé et démarré sur la machine.
- **Impossible d'obtenir la planification :** mettez la machine à niveau vers XenApp et XenDesktop 7.14 (minimum).
- **WMI n'est pas exécuté sur la machine :** vérifiez que l'accès WMI (Windows Management Instrumentation) est activé.
- **Connexions WMI bloquées :** activez WMI dans le service Pare-feu Windows.
- **Version plus récente de Citrix Telemetry Service requise :** (la version est vérifiée uniquement pour Collecter et Tracer et reproduire) mettez à niveau la version du Service de télémétrie sur la machine (voir Installation et mise à niveau). Si vous ne mettez pas à niveau le service, cette machine n'est pas incluse dans les actions **Collecter** ou **Tracer et reproduire**.
- **Scout ne peut pas se connecter à la socket systemd de cette machine** - Assurez-vous que :
  - Le port 7503 est ouvert. Vérifiez que systemd ctxtelemetry.socket écoute sur le port 7503 de la machine. Le port peut être différent si le port ctxtelemetry.socket a été modifié. Consultez la section Configuration Scout pour régler les ports.
  - La connexion réseau fonctionne correctement. (il peut vérifier que votre pare-feu est correctement configuré.)
- **Linux VDA Telemetry Service n'est pas démarré sur cette machine.** - Assurez-vous que :
  - Le port 7502 est ouvert. Vérifiez que Linux VDA Telemetry Service est installé et démarré sur la machine. Le port peut être différent si le port du service de télémétrie a été modifié. Consultez la section Configuration Scout pour régler les ports.
  - La connexion réseau fonctionne correctement. (il peut vérifier que votre pare-feu est correctement configuré.)

### Compatibilité de version

Cette version de Scout (3.x) est conçue pour être exécutée sur des Controller et des VDA Citrix Virtual Apps and Desktops (ou XenApp et XenDesktop 7.14 au minimum).

Une version antérieure de Scout est fournie avec les déploiements XenApp et XenDesktop de version antérieure à 7.14. Pour de plus amples informations sur cette version antérieure, consultez l'article CTX130147.

Si vous mettez à niveau un Controller ou un VDA antérieur à 7.14 vers la version 7.14 (ou une version supérieure prise en charge), la version antérieure de Scout est remplacée par la version actuelle.

| Fonctionnalité | Scout 2.23 | Scout 3.0 |
|---|---|---|
| Prise en charge de Citrix Virtual Apps and Desktops (plus XenApp et XenDesktop 7.14 à 7.18) | Oui | Oui |
| Prise en charge de XenDesktop 5.x, 7.1 à 7.13 | Oui | Non |
| Prise en charge de XenApp 6.x, 7.5 à 7.13 | Oui | Non |
| Mis à disposition avec le produit | 7.1–7.13 | À compter de 7.14 |
| Peut être téléchargé à partir de l'article CTX | Oui | Non |
| Capturer des traces CDF | Oui | Oui |
| Capturer des traces de suivi permanent (AOT) | Non | Oui |
| Autoriser la collecte de données de diagnostics | Jusqu'à 10 machines en même temps (par défaut) | Un nombre illimité (sous réserve de disponibilité des ressources) |
| Autoriser l'envoi des données de diagnostics à Citrix | Oui | Oui |
| Autoriser l'enregistrement local des données de diagnostics | Oui | Oui |
| Prise en charge des informations d'identification Citrix Cloud | Non | Oui |
| Prise en charge des informations d'identification Citrix | Oui | Oui |
| Prise en charge du serveur proxy pour les chargements | Oui | Oui |
| Régler les planifications | S/O | Oui |

| Fonctionnalité | Scout 2.23 | Scout 3.0 |
| --- | --- | --- |
| Prise en charge de script | Ligne de commande (Controller local uniquement) | PowerShell à l'aide des applets de commande Call Home (toute machine avec Telemetry Service installé) |
| Contrôles d'intégrité | Non | Oui |
| Masquage des données | Non | À compter de 3.17 |

### Installation et mise à niveau

Par défaut, Scout est installé ou mis à niveau automatiquement dans le cadre du Service de télémétrie Citrix lorsque vous installez ou mettez à niveau un VDA ou un Controller.

Si vous omettez le Service de télémétrie Citrix lorsque vous installez un VDA, ou que vous supprimez le service ultérieurement, exécutez `TelemetryServiceInstaller_xx.msi` à partir du dossier `x64\Virtual Desktop Components` ou `x86\Virtual Desktop Components` sur le support d'installation Citrix Virtual Apps and Desktops.

Lorsque vous utilisez l'action **Collecter** ou **Tracer et reproduire**, vous êtes averti si une machine exécute une version antérieure du Service de télémétrie Citrix. Citrix recommande d'utiliser la dernière version prise en charge. Si vous ne mettez pas à niveau le service de télémétrie, cette machine n'est pas incluse dans les actions **Collecter** ou **Tracer et reproduire**. Pour effectuer la mise à niveau du Service de télémétrie, utilisez la même procédure que l'installation.

### Autorisation de chargement

Si vous voulez charger les collectes de diagnostic vers Citrix, vous devez disposer d'un compte Citrix ou Citrix Cloud. (Il s'agit des informations d'identification que vous utilisez pour accéder aux téléchargements de Citrix ou pour accéder au Centre de contrôle Citrix Cloud.) Une fois vos informations d'identification de compte validées, un jeton est émis.

Si vous vous authentifiez avec un compte Citrix ou Citrix Cloud, cliquez sur un lien pour accéder à Citrix Cloud à l'aide de HTTPS avec votre navigateur par défaut. Une fois que vous avez entré vos informations d'identification Citrix Cloud, le jeton s'affiche. Copiez le jeton et collez-le dans Scout. Vous pouvez ensuite continuer dans l'Assistant Scout.

Le jeton est stocké localement sur la machine sur laquelle vous exécutez Scout. Pour utiliser ce jeton la prochaine fois que vous exécutez **Collecter** ou **Tracer et reproduire**, sélectionnez la case **Stocker le jeton et ignorer cette étape à l'avenir**.

Chaque fois que vous sélectionnez **Planifier** sur la page d'ouverture de Scout, vous devez renouveler l'autorisation. Vous ne pouvez pas utiliser un jeton stocké lors de la création ou modification d'une planification.

#### Utiliser un proxy pour les chargements

Si vous souhaitez utiliser un serveur proxy pour le chargement des collectes vers Citrix, vous pouvez demander à Scout d'utiliser les paramètres de proxy configurés pour les propriétés d'Internet de votre navigateur. Vous pouvez également spécifier l'adresse IP et le numéro de port du serveur proxy.

### Rechercher machine

Pour les procédures **Collecter**, **Tracer et reproduire**e t **Planifier**, Scout répertorie les Controller et VDA qu'il découvre automatiquement.

Lorsque vous exécutez Contrôle d'intégrité Scout à partir d'un Delivery Controller, cliquez sur **Rechercher machine** pour découvrir des machines, notamment des contrôleurs de mise à disposition, des VDA, des serveurs de licences et des serveurs StoreFront.

Lorsque vous exécutez le contrôle d'intégrité Scout à partir d'une machine jointe à un domaine qui n'est pas un Delivery Controller, Scout ne peut pas détecter automatiquement les machines. Vous devez ajouter des machines manuellement ou importer des machines VDA.

### Ajouter des machines manuellement

Une fois que Scout a répertorié les Controller et les VDA détectés, vous pouvez ajouter manuellement d'autres machines dans le déploiement, telles que des serveurs StoreFront, des serveurs de licences et des serveurs Citrix Provisioning.

Lors de l'exécution des contrôles d'intégrité :

- Les serveurs de licences Citrix du domaine sont découverts automatiquement. Vous ne pouvez pas ajouter des serveurs de licences manuellement.
- Actuellement, les contrôles d'intégrité ne prennent pas en charge les serveurs Citrix Provisioning.

Sur toute page Scout répertoriant les machines détectées, cliquez sur **+ Ajouter une machine**. Entrez le nom de domaine complet de la machine que vous souhaitez ajouter, puis cliquez sur **Continuer**. Répétez cette opération pour ajouter d'autres machines, si nécessaire. (Bien que la saisie d'un alias DNS au lieu d'un nom de domaine complet puisse paraître valide, les contrôles d'intégrité peuvent échouer.)

Les machines ajoutées manuellement apparaissent toujours en haut de la liste des machines, au-dessus des machines découvertes.

Un moyen simple d'identifier une machine ajoutée manuellement est le bouton rouge de suppression à l'extrémité droite de la ligne. Seules les machines ajoutées manuellement ont ce bouton. Les machines découvertes ne l'ont pas.

Pour supprimer une machine ajoutée manuellement, cliquez sur le bouton rouge à droite de la ligne. Confirmez la suppression. Répétez cette opération pour supprimer d'autres machines ajoutées manuellement.

Scout mémorise les machines ajoutées manuellement jusqu'à ce que vous les supprimiez. Lorsque vous fermez puis rouvrez Scout, les machines ajoutées manuellement sont toujours répertoriées en haut de la liste.

Les traces CDF ne sont pas collectées lors de l'utilisation de **Tracer et reproduire** sur les serveurs StoreFront. Cependant, toutes les autres informations de trace sont collectées.

### Importer des machines VDA

Vous pouvez importer des machines VDA dans le déploiement lors de l'exécution des vérifications.

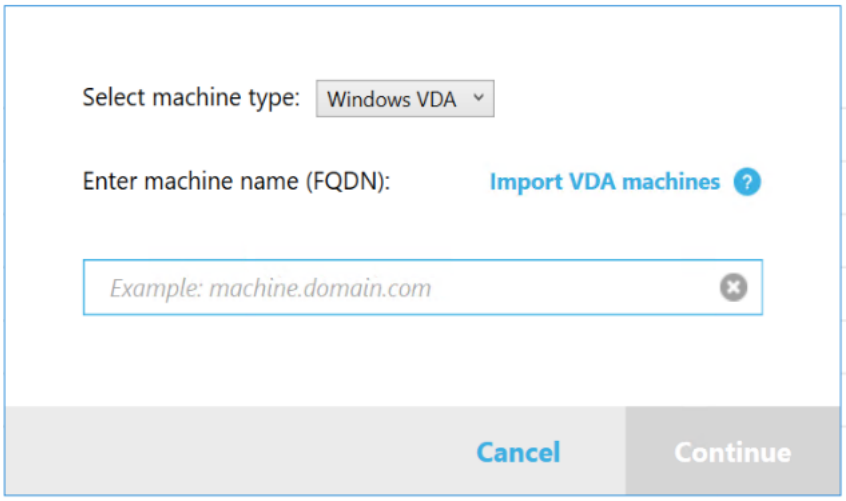
1. Sur le Delivery Controller ou le Connector, générez le fichier de liste de machines à l'aide de la commande PowerShell. Sur le Connector, vous devez entrer des informations d'identification Citrix et sélectionner le client dans la boîte de dialogue contextuelle.

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList
   .txt
   ```

2. Copiez le fichier machineList.txt sur la machine jointe au domaine que vous souhaitez lancer le contrôle d'intégrité Scout.
3. Sur la page du contrôle d'intégrité Scout, cliquez sur **Ajouter une machine**.
4. Sélectionnez le type de machine **VDA Windows**.
5. Cliquez sur **Importer des machines VDA**.
6. Sélectionnez le fichier machineList.txt.
7. Cliquez sur **Ouvrir**.

Les machines VDA importées sont répertoriées sur la page de contrôle d'intégrité Scout.




### Collecter informations de diagnostic

La procédure **Collecter** consiste à sélectionner des machines, à démarrer la collecte de diagnostics et à charger ensuite le fichier contenant la collecte vers Citrix ou à l'enregistrer localement.

1. Lancer Scout. Depuis le menu **Démarrer** de la machine, sélectionnez **Citrix > Citrix Scout**. Sur la page d'ouverture, cliquez sur **Collecter**.
2. Sélectionner des machines.

   - Sur un Controller, la page **Sélectionner des machines** répertorie tous les VDA et Controller du site. Vous pouvez filtrer l'affichage par nom de machine. Pour ajouter d'autres machines manuellement (telles que des serveurs StoreFront ou Citrix Provisioning), consultez la section Ajouter des machines manuellement.
   - Sur d'autres composants (tels que les serveurs VDA), la page **Sélectionner des machines** répertorie uniquement la machine locale. L'ajout manuel de machines n'est pas pris en charge.

   Sélectionnez la case à cocher en regard de chaque machine à partir de laquelle vous voulez collecter des diagnostics, puis cliquez sur **Continuer**.

   Scout démarre automatiquement des tests de vérification sur chaque machine sélectionnée, s'assurant ainsi que celle-ci remplit les critères répertoriés dans Tests de vérification. En cas d'échec de la vérification, un message est affiché dans la colonne **État** et la case à cocher de cette machine n'est plus sélectionnée. Vous pouvez :

   - Corriger le problème, puis sélectionner de nouveau la case à cocher de la machine. Cela déclenche une nouvelle tentative de tests de vérification.
   - Ignorer cette machine (laisser la case à cocher non sélectionnée). Les diagnostics ne seront pas collectés à partir de cette machine.

Une fois les tests de vérification terminés, cliquez sur **Continuer**.

3. Collectez les informations de diagnostic. Le résumé répertorie toutes les machines à partir desquelles les diagnostics sont collectés (les machines que vous avez sélectionnées et qui ont réussi les tests de vérification). Cliquez sur **Collecte**.

   Lors de la collecte :

   - La colonne **État** indique l'état actuel de collecte pour une machine.
   - Pour arrêter une collecte en cours sur une seule machine, cliquez sur **Annuler** dans la colonne **Action** pour cette machine.
   - Pour arrêter toutes les collectes en cours, cliquez sur **Arrêter la collecte** dans le coin inférieur droit de la page. Les diagnostics à partir de machines qui ont terminé la collecte sont conservés. Pour reprendre la collecte, cliquez sur **Réessayer** dans la colonne **Action** pour chaque machine.
   - Lorsque la collecte est terminée pour toutes les machines sélectionnées, le bouton **Arrêter la collecte** dans le coin inférieur droit devient **Continuer**.
   - Pour collecter à nouveau les diagnostics, cliquez sur **Collecter à nouveau** dans la colonne **Action** de cet ordinateur. La collecte plus récente remplace la version antérieure.
   - Si une collecte échoue, vous pouvez cliquer sur **Réessayer** dans la colonne **Action**. Seules les collectes réussies sont chargées ou enregistrées.
   - Une fois que la collecte est terminée pour toutes les machines sélectionnées, ne cliquez pas sur **Précédent**. (Si vous cliquez dessus, la collection est perdue.)

   Lorsque la collecte est terminée, cliquez sur **Continuer**.

4. Enregistrer ou charger la collecte. Choisissez si vous souhaitez charger le fichier vers Citrix, ou l'enregistrer sur la machine locale.

   Si vous choisissez de charger le fichier maintenant, passez à l'étape 5.

   Si vous choisissez d'enregistrer le fichier localement :

   - La boîte de dialogue **Enregistrer** de Windows s'affiche. Naviguez jusqu'à l'emplacement souhaité.
   - Lorsque l'enregistrement local est terminé, le nom de chemin du fichier est affiché et lié. Vous pouvez afficher le fichier. Vous pouvez charger le fichier ultérieurement sur Citrix. Voir CTX136396.

   Cliquez sur **Terminé** pour revenir sur la page d'ouverture de Scout. Vous n'avez pas besoin de suivre les autres étapes de cette procédure.

5. Authentifiez-vous pour les chargements et spécifiez le proxy (facultatif). Pour plus d'informations, consultez la section Autorisation de chargement.

   - Si vous ne vous êtes pas authentifié via Scout, passez à cette étape.

- Si vous vous êtes authentifié via Scout, le jeton d'autorisation stocké est utilisé par défaut. Si c'est ce que vous souhaitez faire, sélectionnez cette option et cliquez sur **Continuer**. Vous n'êtes pas invité à entrer d'informations d'identification pour cette collecte. Passez à l'étape 6.
- Si vous vous êtes précédemment authentifié, mais souhaitez renouveler l'autorisation et obtenir un nouveau jeton, cliquez sur **Changer/réautoriser** et poursuivez avec cette étape.

Choisissez si vous souhaitez utiliser les informations d'identification Citrix ou les informations d'identification Citrix Cloud pour authentifier le chargement. Cliquez sur **Continuer**. La page d'informations d'identification s'affiche uniquement si vous n'utilisez pas de jeton stocké.

Sur la page d'informations d'identification :

- Si vous souhaitez utiliser un serveur proxy pour le chargement du fichier, cliquez sur **Configurer le proxy**. Vous pouvez demander à Scout d'utiliser les paramètres de proxy configurés pour les propriétés d'Internet de votre navigateur. Vous pouvez également spécifier l'adresse IP du serveur proxy et son numéro de port. Fermez la boîte de dialogue de proxy.
- Pour un compte Citrix Cloud, cliquez sur **Générer jeton**. Votre navigateur par défaut s'ouvre sur une page de Citrix Cloud où un jeton s'affiche. Copiez le jeton et collez-le sur la page Scout.
- Pour un compte Citrix, entrez vos informations d'identification.

Lorsque vous avez terminé, cliquez sur **Continuer**.

6. Entrez des informations sur le chargement.

   - Le champ de nom contient le nom par défaut du fichier pour les diagnostics collectés. Il convient à la plupart des collectes, mais vous pouvez le modifier. (Si vous supprimez le nom par défaut et laissez le champ de nom vide, le nom par défaut est utilisé.)
   - Si vous le souhaitez, vous pouvez spécifier un numéro de ticket d'assistance Citrix à 8 chiffres.
   - Dans le champ **Description** (facultatif), décrivez le problème et indiquez à quel moment il s'est produit, le cas échéant.

   Lorsque vous avez terminé, cliquez sur **Démarrer le chargement**.

   Durant le chargement, la partie inférieure gauche de la page indique le pourcentage du chargement qui a été effectué. Pour annuler le chargement en cours, cliquez sur **Arrêter le chargement**.

   Lorsque le chargement est terminé, l'adresse URL de son emplacement est affichée et liée. Vous pouvez suivre le lien vers l'emplacement Citrix pour afficher l'analyse du chargement, ou vous pouvez copier le lien.

   Cliquez sur **Terminé** pour revenir sur la page d'ouverture de Scout.

### Tracer et reproduire

La procédure **Tracer et reproduire** consiste à sélectionner des machines, à démarrer une trace, à reproduire les problèmes, à effectuer la collecte de diagnostics et à charger ensuite le fichier vers Citrix ou à l'enregistrer localement.

Cette procédure est similaire à la procédure de **collecte** standard. Toutefois, elle vous permet de démarrer une trace sur les machines, puis de recréer les problèmes sur ces machines. Toutes les informations de diagnostics incluent des données de suivi AOT. Cette procédure ajoute des traces CDF pour faciliter le dépannage.

1. Lancer Scout. Depuis le menu **Démarrer** de la machine, sélectionnez **Citrix > Citrix Scout**. Sur la page d'ouverture, cliquez sur **Tracer et reproduire**.
2. Sélectionner des machines. La page **Sélectionner des machines** répertorie tous les VDA et Controller du site. Vous pouvez filtrer l'affichage par nom de machine. Sélectionnez la case à cocher en regard de chaque machine à partir de laquelle vous voulez collecter des diagnostics. Puis cliquez sur **Continuer**.

   Pour ajouter d'autres machines manuellement (telles que des serveurs StoreFront ou Citrix Provisioning), consultez la section Ajouter des machines manuellement.

   Scout démarre automatiquement des tests de vérification sur chaque machine sélectionnée, s'assurant ainsi que celle-ci remplit les critères répertoriés dans Tests de vérification. En cas d'échec de la vérification pour une machine, un message est affiché dans la colonne **État** et la case à cocher de cette machine n'est plus sélectionnée. Vous pouvez :

   - Corriger le problème, puis sélectionner de nouveau la case à cocher de la machine. Cela déclenche une nouvelle tentative de tests de vérification.
   - Ignorer cette machine (laisser la case à cocher non sélectionnée). Les diagnostics et les traces ne sont pas collectés à partir de cette machine.

   Une fois les tests de vérification terminés, cliquez sur **Continuer**.
3. Démarrez la trace. Le résumé répertorie toutes les machines à partir desquelles les traces sont collectées. Cliquez sur **Démarrer le traçage**.

   Sur une ou plusieurs des machines sélectionnées, reproduisez les problèmes que vous avez rencontrés. La collecte de traces continue pendant que vous procédez. Lorsque vous avez terminé de reproduire le problème, cliquez sur **Continuer** dans Scout. Le traçage s'arrête.

   Une fois que vous avez arrêté la trace, indiquez si vous avez reproduit le problème lors du traçage.
4. Collecter des informations de diagnostics depuis les machines. Cliquez sur **Collecte**. Lors de la collecte :

- La colonne **État** indique l'état actuel de collecte pour une machine.
- Pour arrêter une collecte en cours sur une seule machine, cliquez sur **Annuler** dans la colonne **Action** pour cette machine.
- Pour arrêter toutes les collectes en cours, cliquez sur **Arrêter la collecte** dans le coin inférieur droit de la page. Les diagnostics à partir de machines qui ont terminé la collecte sont conservés. Pour reprendre la collecte, cliquez sur **Réessayer** dans la colonne **Action** pour chaque machine.
- Lorsque la collecte est terminée pour toutes les machines sélectionnées, le bouton **Arrêter la collecte** dans le coin inférieur droit devient **Continuer**.
- Pour collecter à nouveau des diagnostics à partir d'un ordinateur, cliquez sur **Collecter à nouveau** dans la colonne **Action** de cet ordinateur. La collecte plus récente remplace la version antérieure.
- Si une collecte échoue, vous pouvez cliquer sur **Réessayer** dans la colonne **Action**. Seules les collectes réussies sont chargées ou enregistrées.
- Une fois que la collecte est terminée pour toutes les machines sélectionnées, ne cliquez pas sur **Précédent**. (Si vous le faites, la collecte est perdue.)

Lorsque la collecte est terminée, cliquez sur **Continuer**.

5. Enregistrer ou charger la collecte. Choisissez si vous souhaitez charger le fichier sur Citrix ou l'enregistrer localement.

   Si vous choisissez de charger le fichier maintenant, passez à l'étape 6.

   Si vous choisissez d'enregistrer le fichier localement :

   - La boîte de dialogue Enregistrer de Windows s'affiche. Sélectionnez l'emplacement souhaité.
   - Lorsque l'enregistrement local est terminé, le nom de chemin du fichier est affiché et lié. Vous pouvez afficher le fichier. Rappel : vous pouvez charger le fichier plus tard à partir de Citrix ; consultez l'article CTX136396 pour Citrix Insight Services.

   Cliquez sur **Terminé** pour revenir sur la page d'ouverture de Scout. Vous n'avez pas besoin de suivre les autres étapes de cette procédure.

6. S'authentifier pour les chargements et spécifier le proxy (facultatif). Consultez la section Autorisation de chargement pour plus de détails sur ce processus.

   - Si vous ne vous êtes pas authentifié via Scout, passez à cette étape.
   - Si vous vous êtes authentifié via Scout, le jeton d'autorisation stocké est utilisé par défaut. Si c'est ce que vous voulez faire, choisissez cette option et cliquez sur **Continuer**. Vous n'êtes pas invité à entrer d'informations d'identification pour cette collecte. Passez à l'étape 7.

- Si vous vous êtes précédemment authentifié, mais souhaitez renouveler l'autorisation et obtenir un nouveau jeton, cliquez sur **Changer/réautoriser** et poursuivez avec cette étape.

Choisissez si vous souhaitez utiliser les informations d'identification Citrix ou les informations d'identification Citrix Cloud pour authentifier le chargement. Cliquez sur **Continuer**. La page d'informations d'identification s'affiche uniquement si vous n'utilisez pas de jeton stocké.

Sur la page d'informations d'identification :

- Si vous souhaitez utiliser un serveur proxy pour le chargement du fichier, cliquez sur **Configurer le proxy**. Vous pouvez demander à Scout d'utiliser les paramètres proxy configurés pour les propriétés Internet de votre navigateur. Vous pouvez également spécifier l'adresse IP du serveur proxy et son numéro de port. Fermez la boîte de dialogue de proxy.
- Pour un compte Citrix Cloud, cliquez sur **Générer jeton**. Votre navigateur par défaut s'ouvre sur une page de Citrix Cloud où un jeton s'affiche. Copiez le jeton et collez-le sur la page Scout.
- Pour un compte Citrix, entrez vos informations d'identification.

Lorsque vous avez terminé, cliquez sur **Continuer**.

7. Fournir des informations sur le chargement.

   Entrez les détails de chargement :

   - Le champ de nom contient le nom par défaut du fichier pour les diagnostics collectés. Il convient à la plupart des collectes, mais vous pouvez le modifier. (Si vous supprimez le nom par défaut et laissez le champ de nom vide, le nom par défaut est utilisé.)
   - Si vous le souhaitez, vous pouvez spécifier un numéro de ticket d'assistance Citrix à 8 chiffres.
   - Dans le champ Description (facultatif), décrivez le problème et indiquez lorsque le problème s'est produit, le cas échéant.

   Lorsque vous avez terminé, cliquez sur **Démarrer le chargement**.

   Durant le chargement, la partie inférieure gauche de la page indique le pourcentage du chargement qui a été effectué. Pour annuler le chargement en cours, cliquez sur **Arrêter le chargement**.

   Lorsque le chargement est terminé, l'adresse URL de son emplacement est affichée et liée. Vous pouvez suivre le lien vers l'emplacement Citrix pour afficher l'analyse du chargement, ou vous pouvez copier le lien.

   Cliquez sur **Terminé** pour revenir sur la page d'ouverture de Scout.

### Activer la collecte de journaux supplémentaires

La fonction **Activer la collecte de journaux supplémentaires** vous permet d'utiliser la fonction de suivi et de reproduction avec d'autres outils, tels que perfmon, Netsh, DebugView et Wireshark.

> **Remarque :**
>
> Cela s'applique uniquement aux machines locales.

Pour configurer une collecte de journaux supplémentaire :

1. Lancez Citrix Scout.
2. Cliquez sur l'icône d'engrenage **Paramètres**.
3. Cliquez sur **Activer la collecte de journaux supplémentaires avec d'autres outils**.
4. Cliquez sur **Enregistrer**.

Pour collecter des journaux supplémentaires :

1. Sur la page d'accueil de Scout, cliquez sur **Tracer et reproduire**.
2. Sur la page **Sélectionner des machines**, cliquez sur l'icône d'engrenage située sur le côté droit de la machine locale.
3. Sur la page **Sélectionnez les outils requis pour la journalisation :**, cliquez sur **Télécharger les outils**.
4. Sur la page **Télécharger les outils**, sélectionnez les outils que vous souhaitez utiliser et cliquez sur **Télécharger**. Les outils sont ensuite téléchargés, à l'exception de Wireshark. Wireshark ne peut être téléchargé et installé que manuellement.
   Remarque : Si vous choisissez de télécharger d'autres outils manuellement, vous devez extraire le contenu du fichier .zip téléchargé sur `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\<toolname>`. Par exemple, si vous téléchargez le fichier DebugView.zip, vous décompressez le contenu du fichier dans `C:\ProgramData\Citrix\TelemetryService\CDC\Lib\Resources\Tools\DebugView\`.
5. Sur la page **Sélectionnez les outils requis pour la journalisation :**, cliquez sur **Actualiser l'état**. Tous les outils sélectionnés apparaissent comme **Présent** dans la colonne État.
6. Sélectionnez les outils de journalisation, puis cliquez sur **Suivant**.
7. Suivez les instructions de Tracer et reproduire.
8. Une fois terminé, vérifiez les journaux dans le fichier zip. Les journaux sont zippés dans le dossier *CDCLogs*.

> **Remarque :**
>
> Si l'outil Procmon est sélectionné pour le traçage, la taille des journaux Process Monitor peut augmenter rapidement. Assurez-vous de sélectionner uniquement les outils nécessaires. Vous pouvez également surveiller la taille des journaux sous *%temp%\Scout-CDC-Log*.

### Planifier des collectes

> **Remarque :**
>
> Vous pouvez actuellement planifier des collectes, mais pas des contrôles d'intégrité.

La procédure de planification consiste à sélectionner des machines et à définir ou à annuler la planification. Les collectes planifiées sont automatiquement chargées vers Citrix. (Vous pouvez enregistrer les collectes planifiées localement à l'aide de l'interface PowerShell. Voir Citrix Call Home.)

1. Lancer Scout. Depuis le menu Démarrer de la machine, sélectionnez **Citrix > Citrix Scout**. Sur la page d'ouverture, cliquez sur **Planifier**.
2. Sélectionner des machines. Tous les VDA et Controller du site sont répertoriés. Vous pouvez filtrer l'affichage par nom de machine.

   Lorsque vous avez installé des VDA et des Controller à l'aide de l'interface graphique, si vous avez défini un programme Call Home (voir Citrix Call Home), Scout affiche ces paramètres, par défaut. Vous pouvez utiliser cette version de Scout pour démarrer les collectes planifiées pour la première fois, ou modifier une planification configurée précédemment.

   Bien que vous ayez activé/désactivé Call Home machine par machine lors de l'installation des composants, un programme configuré dans Scout affecte toutes les machines que vous sélectionnez.

   Sélectionnez la case à cocher en regard de chaque machine à partir de laquelle vous voulez collecter des diagnostics, puis cliquez sur **Continuer**.

   Pour ajouter d'autres machines manuellement (telles que des serveurs StoreFront ou Citrix Provisioning), consultez la section Ajouter des machines manuellement.

   Scout démarre automatiquement des tests de vérification sur chacune des machines sélectionnées, s'assurant ainsi que celle-ci remplit les critères répertoriés dans Tests de vérification. En cas d'échec de la vérification pour une machine, un message est affiché dans la colonne **État** et la case à cocher de cette machine n'est plus sélectionnée. Vous pouvez :

   - Corriger le problème, puis sélectionner de nouveau la case à cocher de la machine. Cela déclenche une nouvelle tentative de tests de vérification.
   - Ignorer cette machine (laisser la case à cocher non sélectionnée). Les diagnostics (ou traces) ne sont pas collectés à partir de cette machine.

   Une fois les tests de vérification terminés, cliquez sur **Continuer**.

   La page Résumé répertorie les machines auxquelles sont appliquées les planifications. Cliquez sur **Continuer**.
3. Définissez la planification. Indiquez quand vous souhaitez que les diagnostics soient collectés. Rappel : la planification affecte toutes les machines sélectionnées.

- Pour configurer une planification hebdomadaire pour les machines sélectionnées, cliquez sur **Hebdomadaire**. Choisissez le jour de la semaine. Entrez l'heure de la journée (horloge de 24 heures) pour le début de la collecte.
- Pour configurer une planification quotidienne pour les machines sélectionnées, cliquez sur **Quotidien**. Entrez l'heure de la journée (horloge de 24 heures) pour le début de la collecte.
- Pour annuler une planification existante pour les machines sélectionnées (et ne pas la remplacer par une autre), cliquez sur **Désactiver**. Cela annule toute planification qui a été configurée précédemment pour ces machines.

Cliquez sur **Continuer**.

4. Authentifiez-vous pour les chargements et spécifiez le proxy (facultatif). Consultez la section Autorisation de chargement pour plus de détails sur ce processus. Rappel : vous ne pouvez pas utiliser de jeton stocké pour vous authentifier lorsque vous travaillez avec une planification Scout.

   Choisissez si vous souhaitez utiliser les informations d'identification Citrix ou les informations d'identification Citrix Cloud pour authentifier le chargement. Cliquez sur **Continuer**.

   Sur la page d'informations d'identification :

   - Si vous souhaitez utiliser un serveur proxy pour le chargement du fichier, cliquez sur **Configurer le proxy**. Vous pouvez demander à Scout d'utiliser les paramètres proxy configurés pour les propriétés Internet de votre navigateur. Vous pouvez également spécifier l'adresse IP du serveur proxy et son numéro de port. Fermez la boîte de dialogue de proxy.
   - Pour un compte Citrix Cloud, cliquez sur **Générer jeton**. Votre navigateur par défaut s'ouvre sur une page de Citrix Cloud où un jeton s'affiche. Copiez le jeton et collez-le sur la page Scout.
   - Pour un compte Citrix, entrez vos informations d'identification.

   Lorsque vous avez terminé, cliquez sur **Continuer**.

   Passez en revue la planification configurée. Cliquez sur **Terminé** pour revenir sur la page d'ouverture de Scout.

   Au cours d'une collecte, le journal des applications Windows de chaque machine sélectionnée contient des entrées relatives à la collecte et au chargement.

### Masquage des données

Les informations de diagnostic collectées à l'aide de Citrix Scout peuvent contenir des informations sensibles à la sécurité. La fonction de masquage des données Citrix Scout vous permet de masquer les données sensibles dans les fichiers de diagnostic avant de les charger sur Citrix.

Le masquage des données Scout est configuré pour masquer l'adresse IP, les noms de machine, les noms de domaine, les noms d'utilisateur, les noms d'hyperviseur, les noms de groupe de mise à disposition, les noms de catalogue, les noms d'applications et les SID.

> **Remarque :**
>
> Les traces CDF sont cryptées et ne peuvent pas être masquées.
>
> Les journaux des VDA Linux sont compressés au format `.tar.gz2` et ne peuvent pas être masqués.

#### Recueillir de nouveaux diagnostics et effectuer le masquage des données

Pour exécuter la fonction de masquage des données Citrix Scout, vous devez lancer Scout à partir de la ligne de commande.

1. Dans Windows, exécutez l'invite de commandes en tant qu'administrateur.
2. Accédez au répertoire où Scout est installé : `cd C:\Program Files\Citrix\Telemetry Service`.
3. Lancez Scout : `ScoutUI.exe datamasking`.
4. Cliquez sur **Collecter** ou **Tracer et reproduire** pour collecter les diagnostics.
5. Une fois la collection terminée, sélectionnez **Activer le masquage des données** pour continuer. Cette option est activée par défaut.
6. Configurez le masque de données. Vous pouvez utiliser les règles par défaut ou personnaliser les règles.
7. Indiquez si vous souhaitez télécharger ou enregistrer les informations de diagnostics.
    - Si l'option **Charger les informations de diagnostic recueillies auprès de Citrix** est sélectionnée, les fichiers de diagnostic masqués sont chargés sur Citrix.
    - Si vous sélectionnez **Enregistrer les informations de diagnostic recueillies sur votre machine locale**, les diagnostics d'origine et masqués sont enregistrés à l'emplacement spécifié.

#### Effectuer le masquage des données sur les diagnostics existants

1. Dans Windows, exécutez l'invite de commandes en tant qu'administrateur.
2. Accédez au répertoire où Scout est installé : `cd C:\Program Files\Citrix\Telemetry Service`.
3. Lancez Scout directement en mode de masquage des données : `ScoutUI.exe datamasking filePath`.
4. Sélectionnez « Activer le masquage des données » pour continuer. Cette option est activée par défaut.

5. Configurez le masque de données. Vous pouvez exécuter le masquage des données avec les règles par défaut ou personnaliser les règles.
6. Indiquez si vous souhaitez télécharger ou enregistrer les informations de diagnostics.
    - Si l'option **Charger les informations de diagnostic recueillies auprès de Citrix** est sélectionnée, les fichiers de diagnostic masqués sont chargés sur Citrix.
    - Si vous sélectionnez **Enregistrer les informations de diagnostic recueillies sur votre machine locale**, les diagnostics d'origine et masqués sont enregistrés à l'emplacement spécifié.

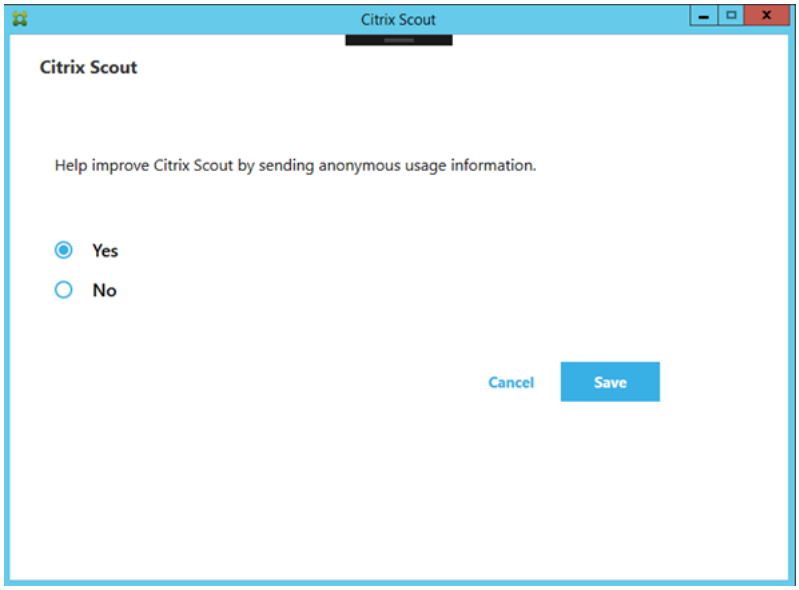
#### Emplacements des fichiers de données masqués et des fichiers de mappage

Après avoir téléchargé ou enregistré les informations de diagnostics, cliquez sur le lien pour ouvrir les diagnostics d'origine et masqués, puis ouvrez le fichier d'informations de mappage.

### Collecte de données d'utilisation

Lorsque vous utilisez Scout, Citrix utilise Google Analytics pour collecter des données d'utilisation anonymes qui seront utilisées pour les futures fonctionnalités et améliorations du produit. La collecte de données est activée par défaut.

Pour modifier la collecte et le chargement des données d'utilisation, cliquez sur l'icône d'engrenages **Paramètres** de l'interface utilisateur Scout. Vous pouvez ensuite choisir d'envoyer les informations en sélectionnant **Oui** ou **Non**, puis en cliquant sur **Enregistrer**.



# Collecte d'une trace CDF (Citrix Diagnostic Facility) au démarrage du système

June 27, 2024

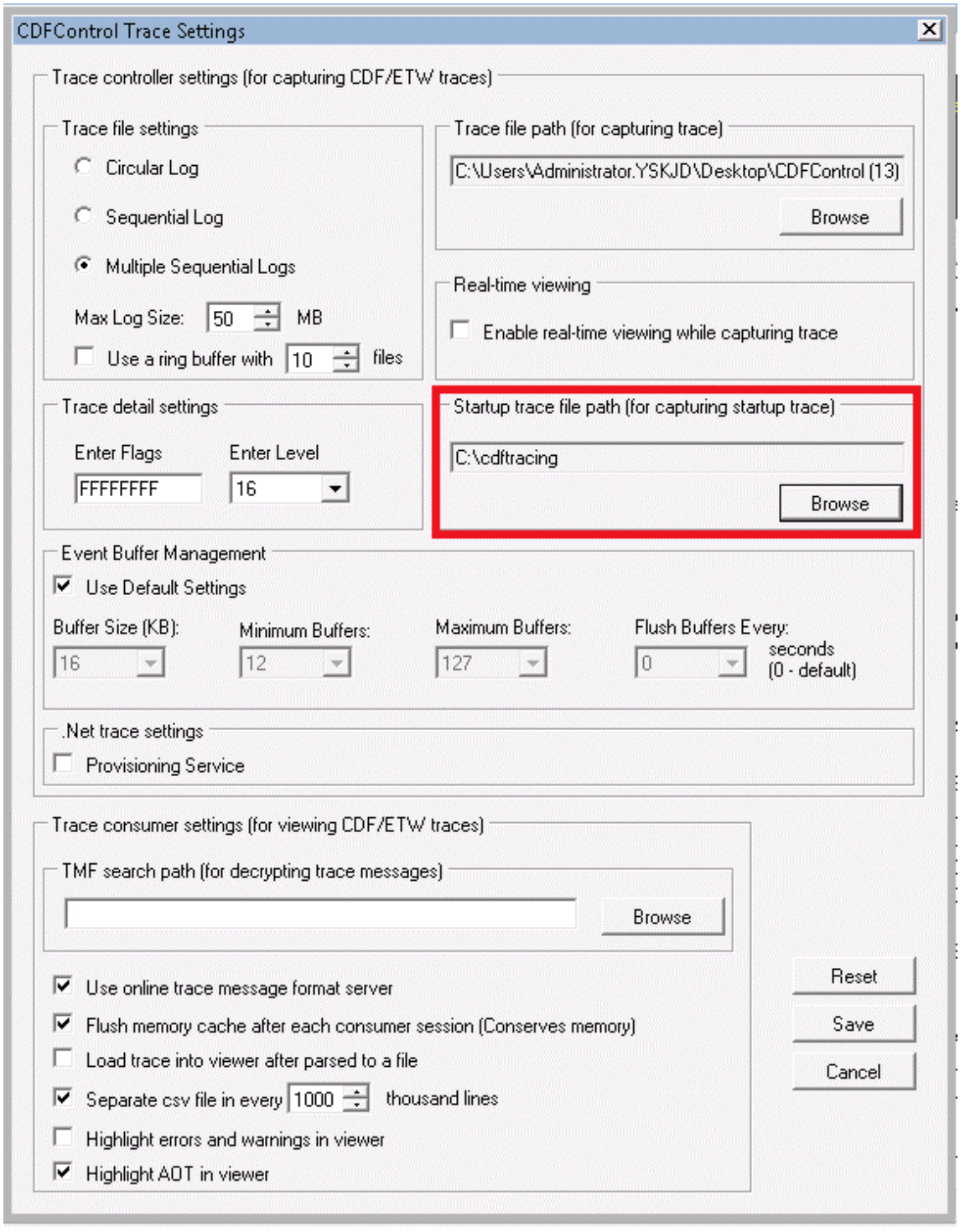
L'utilitaire CDFControl est un contrôleur ou un consommateur de traçage d'événements permettant de capturer les messages de trace CDF (Citrix Diagnostic Facility) affichés à partir de divers fournisseurs de trace Citrix. Il est conçu pour résoudre les problèmes complexes liés à Citrix, analyser la prise en charge des filtres et collecter des données de performances. Pour télécharger l'utilitaire CDFControl, voir CTX111961.

## Recueillir une trace au démarrage du système

Utilisez la procédure suivante pour collecter une trace CDF au démarrage du système. Vous avez besoin de privilèges d'administrateur.

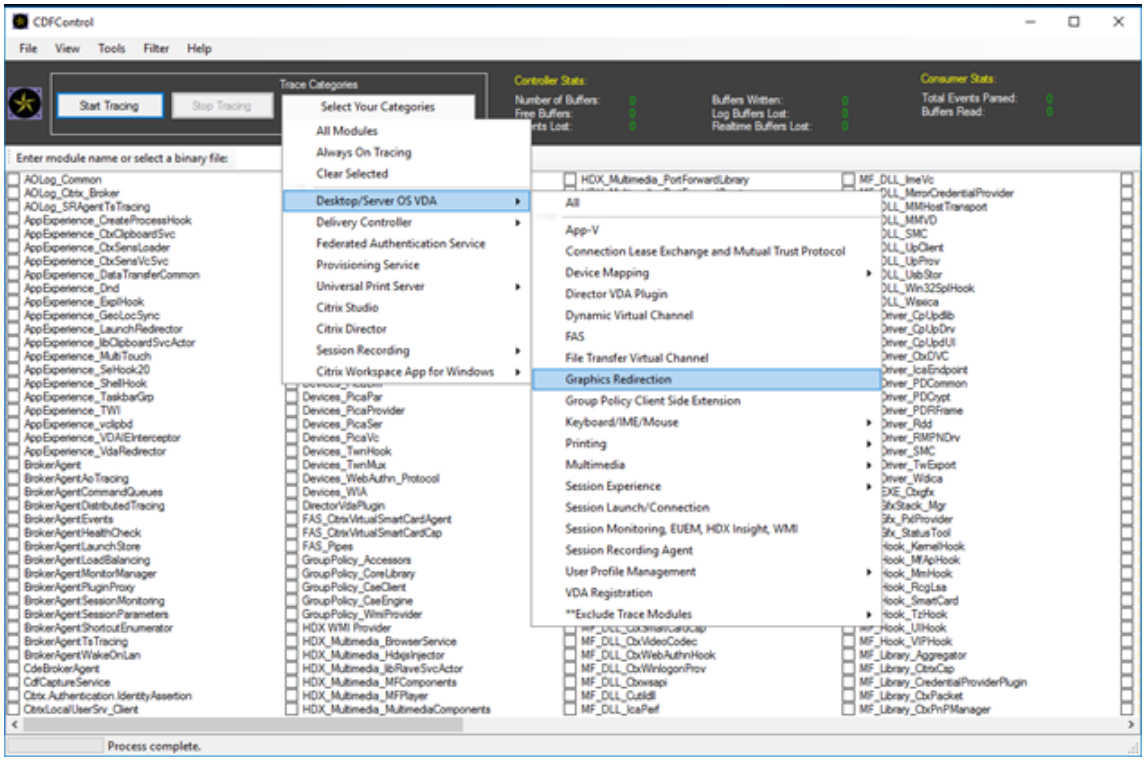
1. Démarrez **CDFControl** et sélectionnez **Options** dans le menu **Tools**.
2. Spécifiez le chemin du fichier de trace dans la section **Startup trace file path for capturing startup trace**. Cliquez ensuite sur **Enregistrer**.




3. Dans **Trace Categories**, effectuez la sélection recommandée par le support Citrix. (Dans l'exemple suivant, la **redirection des graphiques** est sélectionnée. Cette sélection n'est qu'un exemple. Nous vous recommandons d'activer les fournisseurs correspondant au problème que vous corrigez.)




4. Sélectionnez **Startup Tracing** et sélectionnez **Enable** dans le menu **Tools**.

   Après avoir sélectionné **Enable**, la barre animée commence à défiler. Cette activité n'affecte pas la procédure. Passez à l'étape suivante.

5. Une fois que **Startup Tracing** est activé, fermez **CDFControl utility** et redémarrez le système.
6. Démarrez l'utilitaire **CDFControl**. Une fois que le système redémarre et que l'erreur s'affiche, désactivez le suivi du démarrage en sélectionnant **Startup Tracing** dans le menu **Tools**, puis en cliquant sur **Disable**.
7. Accédez au chemin d'accès au fichier de trace spécifié à l'étape 2 et collectez le fichier journal de trace (.etl) à des fins d'analyse.

## Administration déléguée

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, con-

> sultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Grâce à l'utilisation d'un contrôle basé sur des objets et des rôles, le modèle d'administration déléguée vous offre une souplesse permettant d'adapter les activités d'administration déléguée aux besoins de votre entreprise. L'administration déléguée prend en charge les déploiements de toutes les tailles et vous permet d'affiner la granularité des autorisations à mesure que votre déploiement gagne en complexité. L'administration déléguée utilise trois concepts : les administrateurs, les rôles et les étendues.

- **Administrateurs** : un administrateur représente une personne ou un groupe de personnes identifié par leur compte Active Directory. Chaque administrateur est associé à une ou plusieurs paires rôle/étendue.
- **Rôles** : un rôle représente une fonction de tâche à laquelle des permissions sont associées. Par exemple, le rôle Administrateur du groupe de mise à disposition possède des autorisations telles que « Créer un groupe de mise à disposition » et « Supprimer le bureau d'un groupe de mise à disposition ». Un administrateur peut avoir plusieurs rôles pour un même site, donc une personne peut être administrateur du groupe de mise à disposition et administrateur du catalogue de machines. Les rôles peuvent être intégrés ou personnalisés.

  Les rôles intégrés sont :

| Rôle | Autorisations |
|---|---|
| Administrateur complet | Peut effectuer toutes les tâches et toutes les opérations. Un administrateur complet est toujours associé à l'étendue Tout. |
| Administrateur en lecture seule | Peut afficher tous les objets dans les étendues spécifiées ainsi que les informations générales, mais ne peut rien modifier. Par exemple, un administrateur en lecture seule avec l'étendue = Londres peut voir tous les objets globaux (tels que la journalisation de la configuration) et les objets associés à Londres (par exemple, les groupes de mise à disposition Londres). Toutefois, cet administrateur ne peut pas afficher d'objets dans l'étendue New York (en supposant que les étendues Londres et New York ne se chevauchent pas). |

| Rôle | Autorisations |
| --- | --- |
| Administrateur du service d'assistance | Peut voir les groupes de mise à disposition et gérer les sessions et machines associées à ces groupes. Peut afficher le catalogue de machines et les informations d'hôte des groupes de mise à disposition en cours de surveillance. Peut également effectuer des opérations de gestion de session et de gestion de l'alimentation de la machine pour les machines figurant dans ces groupes de mise à disposition. |
| Administrateur du catalogue de machines | Peut créer et de gérer des catalogues de machines et y provisionner des machines. Peut créer des catalogues de machines à partir de l'infrastructure de virtualisation, Provisioning Services et des machines physiques. Ce rôle peut gérer les images de base et installer le logiciel, mais ne peut pas assigner les applications ou bureaux aux utilisateurs. |
| Administrateur du groupe de mise à disposition | Peut mettre à disposition des applications, bureaux et machines ; peut également gérer les sessions associées. Il peut également gérer les configurations d'applications et de bureaux, telles que les stratégies et les paramètres de gestion de l'alimentation. |
| Administrateur hôte | Peut gérer des connexions hôtes et leurs paramètres de ressource associés. Impossible de mettre à disposition des machines, applications ou bureaux aux utilisateurs. |

Dans certaines éditions du produit, vous pouvez créer des rôles personnalisés correspondants aux besoins de votre organisation, et déléguer des autorisations avec plus de détails. Vous pouvez utiliser les rôles personnalisés pour allouer des autorisations à la précision d'une action ou d'une tâche dans la console.

- **Étendues :** une étendue représente une collection d'objets. Les étendues sont utilisées pour grouper les objets de manière pertinente pour votre organisation (par exemple, l'ensemble de groupes de mise à disposition utilisé par l'équipe des ventes). Les objets peuvent appartenir à plus d'une étendue ; par exemple, un objet peut être marqué comme appartenant à une ou plusieurs étendues. Il existe une étendue intégrée appelée « Tout » qui contient tous les objets.

Le rôle d'administrateur complet est toujours associé à l'étendue Tout.

### Exemple

La société XYZ a décidé de gérer les applications et bureaux en fonction de leur département (Comptabilité, Ventes et Production) et de leur système d'exploitation de bureau (Windows 7 ou Windows 8). L'administrateur a créé cinq étendues, puis a attribué deux étendues à chaque groupe de mise à disposition : une pour le département où ils sont utilisés et une pour le système d'exploitation qu'ils utilisent.

Les administrateurs suivants ont été créés :

| Administrateur | Rôles | Étendues |
|---|---|---|
| domaine/fred | Administrateur complet | Tous (le rôle Administrateur complet a toujours la portée Tout) |
| domaine/rob | Administrateur en lecture seule | Tous |
| domaine/heidi | Administrateur en lecture seule, Administrateur du service d'assistance | Toutes les ventes |
| domaine/warehouseadmin | Administrateur du service d'assistance | Distribution |
| domaine/peter | Administrateur du groupe de mise à disposition, Administrateur du catalogue de machines | Win7 |

- Fred est un administrateur complet qui peut afficher, modifier et supprimer tous les objets dans le système.
- Rob peut afficher tous les objets dans le site mais ne peut pas les modifier ou les supprimer.
- Heidi peut afficher tous les objets et peut effectuer des tâches de support technique sur les groupes de mise à disposition dans l'étendue Ventes. Cela lui permet de gérer les sessions et les machines associées à ces groupes ; elle ne peut pas effectuer de modifications dans le groupe de mise à disposition, telles que l'ajout ou la suppression de machines.
- Toute personne qui est membre du groupe de sécurité Active Directory warehouseadmin peut afficher et effectuer des tâches d'assistance sur des machines dans l'étendue Distribution.
- Peter est un spécialiste Windows 7 et peut gérer tous les catalogues de machines Windows 7 et mettre à disposition des applications, bureaux et machines Windows 7, quelle que soit l'étendue du département auquel elles appartiennent. L'administrateur a envisagé de donner à Peter

le rôle d'administrateur complet pour l'étendue Win7. Elle en a décidé autrement, car un administrateur complet a également des droits complets sur tous les objets qui ne sont pas inclus dans l'étendue, tels que « Site » et « Administrateur ».

### Comment utiliser l'administration déléguée

En général, le nombre d'administrateurs et la granularité de leurs autorisations dépendent de la taille et de la complexité du déploiement.

- Dans les déploiements de petite taille ou de preuve de concept, toutes les tâches sont effectuées par un ou plusieurs administrateurs. Il n'y a pas de délégation. Dans ce cas, créez chaque administrateur avec le rôle Administrateur complet intégré, qui a la portée Tout.
- Dans les déploiements plus importants avec plus d'ordinateurs, d'applications et de bureaux, une plus grande délégation est nécessaire. Plusieurs administrateurs ont peut-être des responsabilités fonctionnelles plus spécifiques (rôles). Par exemple, deux sont des administrateurs complets et les autres sont des administrateurs du service d'assistance. En outre, un administrateur peut ne gérer que certains groupes d'objets (étendues), tels que des catalogues de machines. Dans ce cas, créez de nouvelles étendues, ainsi que des administrateurs avec l'un des rôles intégrés et les étendues appropriées.
- Même les déploiements plus importants peuvent nécessiter plus (ou plus spécifiques) d'étendues, ainsi que des administrateurs différents dotés de rôles non conventionnels. Dans ce cas, modifiez ou créez des étendues supplémentaires, créez des rôles personnalisés et créez chaque administrateur avec un rôle personnalisé ou intégré, ainsi que des étendues existantes et nouvelles.

Pour garantir une souplesse et facilité de configuration, vous pouvez créer des étendues lorsque vous créez un administrateur. Vous pouvez également spécifier des étendues lors de la création ou de la modification de catalogues de machines ou de connexions.

### Créer et gérer des administrateurs

Lorsque vous créez un site en tant qu'administrateur local, votre compte d'utilisateur devient automatiquement un administrateur complet avec autorisations complètes sur tous les objets. Après la création d'un site, les administrateurs locaux n'ont pas de privilèges spéciaux.

Le rôle administrateur complet a toujours l'étendue Tout ; vous ne pouvez pas le modifier.

Par défaut, un administrateur est activé. La désactivation d'un administrateur peut être nécessaire si vous créez l'administrateur maintenant, mais cette personne ne possèdera des droits d'administration que bien plus tard. Pour les administrateurs activés existants, il se peut que vous souhaitiez désactiver plusieurs d'entre eux pendant que vous réorganisez vos objets/étendues, puis les réactiver

lorsque vous êtes prêt à utiliser la configuration mise à jour dans votre environnement de production. Vous ne pouvez pas désactiver un administrateur complet si cela a pour conséquence qu'il n'existe plus d'administrateur complet activé. La case à cocher activer/désactiver est disponible lors de la création, de la copie ou de la modification d'un administrateur.

Lorsque vous supprimez une paire rôle/étendue lors de la copie, la modification ou la suppression d'un administrateur, il supprime uniquement la relation entre le rôle et l'étendue de cet administrateur. Il ne peut pas supprimer le rôle ou l'étendue. Il n'affecte aucun autre administrateur qui est configuré avec cette paire rôle/étendue.

Pour créer et gérer des administrateurs, procédez comme suit :

1. Connectez-vous à Web Studio, cliquez sur **Administrateurs** dans le volet de gauche, puis sur l'onglet **Administrateurs**.
2. Suivez les instructions relatives à la tâche que vous souhaitez effectuer :

    - **Créer un administrateur :** cliquez sur **Créer l'administrateur** dans la barre d'actions. Entrez le nom ou recherchez le nom du compte d'utilisateur, sélectionnez ou créez une étendue, puis sélectionnez un rôle. Le nouvel administrateur est activé par défaut, vous pouvez le modifier.
    - **Copier un administrateur :** sélectionnez l'administrateur, puis cliquez sur **Copier l'administrateur** dans la barre d'actions. Entrez le nom ou recherchez le nom de compte de l'utilisateur. Vous pouvez sélectionner puis modifier les paires rôle/étendue et vous pouvez en ajouter de nouvelles. Le nouvel administrateur est activé par défaut, vous pouvez le modifier.
    - **Modifier un administrateur :** sélectionnez l'administrateur, puis cliquez sur **Modifier l'administrateur** dans la barre d'actions. Vous pouvez modifier ou supprimer les paires rôle/étendue et en ajouter de nouvelles.
    - **Supprimer un administrateur :** sélectionnez l'administrateur, puis cliquez sur **Supprimer l'administrateur** dans la barre d'actions. Vous ne pouvez pas supprimer un administrateur complet si cela a pour conséquence qu'il n'existe plus d'administrateur complet.

Le volet supérieur affiche les administrateurs que vous avez créés. Sélectionnez un administrateur pour afficher ses détails dans le volet inférieur. La colonne **Avertissements** indique si les paires rôle/étendue associées à l'administrateur contiennent des rôles ou des étendues inutilisables. Le message d'avertissement suivant s'affiche si une paire rôle/étendue associée contient des rôles ou des étendues inutilisables :

- Rôle ou étendue associée inutilisable

> **Important :**
>
> Un message d'avertissement s'affiche uniquement si une paire rôle/étendue associée contient des rôles ou des étendues inutilisables.

Pour supprimer la paire rôle/étendue de l'administrateur, effectuez l'une des étapes suivantes :

- Supprimez la paire rôle/étendue.
  1. Dans la barre d'actions, cliquez sur **Modifier l'administrateur**.
  2. Dans la fenêtre **Nom et détails de l'administrateur**, sélectionnez la paire rôle/étendue, puis cliquez sur **Supprimer**.
  3. Cliquez sur **Enregistrer** pour quitter la fenêtre.
- Supprimez l'administrateur.
  1. Dans la barre d'actions, cliquez sur **Supprimer l'administrateur**.
  2. Dans la fenêtre de confirmation, cliquez sur **Supprimer**.

## Créer et gérer les rôles

Lorsque les administrateurs créent ou modifient un rôle, ils ne peuvent activer que les autorisations dont ils disposent eux-mêmes. Cela empêche les administrateurs de créer un rôle avec plus d'autorisations qu'ils ne disposent actuellement, puis de l'attribuer à eux-mêmes (ou de modifier un rôle qui leur est déjà attribué).

Les noms de rôles peuvent contenir jusqu'à 64 caractères Unicode ; ils ne peuvent pas contenir les caractères suivants : barre oblique inverse, barre oblique, point-virgule, deux-points, symbole de la livre, virgule, astérisque, point d'interrogation, signe égal, flèche gauche, flèche droite, barre verticale, crochet gauche ou droit, parenthèse gauche ou droite, guillemets et apostrophe. Les descriptions peuvent contenir jusqu'à 256 caractères unicode.

Vous ne pouvez pas modifier ou supprimer un rôle intégré. Vous ne pouvez pas supprimer un rôle personnalisé si un administrateur l'utilise.

> **Remarque :**
>
> Seules certaines éditions de produit prennent en charge les rôles personnalisés. Seules les éditions qui prennent en charge les rôles personnalisés n'ont aucune entrée dans la barre d'actions.

Pour créer et gérer des rôles, procédez comme suit :

1. Connectez-vous à Web Studio, cliquez sur **Administrateurs** dans le volet de gauche, puis sur l'onglet **Rôles**.
2. Suivez les instructions relatives à la tâche que vous souhaitez effectuer :

- **Afficher les détails d'un rôle :** sélectionnez le rôle. Le volet inférieur répertorie les types d'objets et les autorisations associées pour le rôle. Cliquez sur l'onglet **Administrateurs** dans le volet inférieur pour afficher une liste des administrateurs qui détiennent actuellement ce rôle.
- **Créer un rôle personnalisé :** cliquez sur **Créer un rôle** dans la barre d'actions. Entrez un nom et une description. Sélectionnez les types d'objets et les autorisations.
- **Copier un rôle :** sélectionnez le rôle, puis cliquez sur **Copier rôle** dans la barre d'actions. Modifiez le nom, la description, les types d'objet et les autorisations nécessaires.
- **Modifier un rôle personnalisé :** sélectionnez le rôle, puis cliquez sur **Modifier un rôle** dans la barre d'actions. Modifiez le nom, la description, les types d'objet et les autorisations nécessaires.
- **Supprimer un rôle personnalisé :** sélectionnez le rôle, puis cliquez sur **Supprimer un rôle** dans la barre d'actions. Lorsque vous y êtes invité, confirmez la suppression.

### Créer et gérer des étendues

Lorsque vous créez un site, la seule étendue disponible est l'étendue 'Tout', qui ne peut pas être supprimée.

Vous pouvez créer des étendues à l'aide de la procédure suivante. Vous pouvez également créer des étendues lorsque vous créez un administrateur ; chaque administrateur doit être associé à au moins une paire de un rôle/étendue. Lorsque vous créez ou modifiez des bureaux, des catalogues de machines, des applications ou des hôtes, vous pouvez les ajouter à une étendue existante. Si vous ne les ajoutez pas à une étendue, ils restent dans l'étendue 'Toute'.

La création d'un site ne peut faire être incluse à une étendue, ni les objets d'administration déléguée (étendues et rôles). Cependant, les objets ne pouvant pas être inclus à une étendue sont inclus dans l'étendue « Tout ». (Les administrateurs complets ont toujours l'étendue Tous.) Les machines, les actions d'alimentation, les bureaux et les sessions ne sont pas ajoutés directement à une étendue. Les administrateurs peuvent se voir attribuer des autorisations sur ces objets via les catalogues de machines ou les groupes de mise à disposition associés.

Règles de création et de gestion des étendues :

- Les noms d'étendue peuvent contenir jusqu'à 64 caractères Unicode. Les étendues ne peuvent pas contenir les caractères suivants : barre oblique inverse, barre oblique, point-virgule, deux-points, symbole de la livre, virgule, astérisque, point d'interrogation, signe égal, flèche gauche ou droite, barre verticale, crochet gauche ou droit, parenthèse gauche ou droite, guillemets et apostrophe.
- Les descriptions d'étendues peuvent contenir jusqu'à 256 caractères unicode.

- Lorsque vous copiez ou modifier une étendue, n'oubliez pas que la suppression des objets dans l'étendue peut rendre ces objets inaccessibles à l'administrateur. Si l'étendue modifiée est associée à un ou plusieurs rôles, assurez-vous que les mises à jour que vous apportez à l'étendue ne rendent pas une paire rôle/étendue inutilisable.

Pour créer et gérer des étendues, procédez comme suit :

1. Connectez-vous à Web Studio, cliquez sur **Administrateurs** dans le volet de gauche, puis sur l'onglet **Étendues**.
2. Suivez les instructions relatives à la tâche que vous souhaitez effectuer :

    - **Créer une étendue :** cliquez sur **Créer une étendue** dans la barre d'actions. Entrez un nom et une description. Pour inclure tous les objets d'un type particulier (par exemple, les groupes de mise à disposition), sélectionnez le type d'objet. Pour inclure des objets spécifiques, développez le type, puis sélectionnez les objets individuels (par exemple, les groupes de mise à disposition individuels utilisés par l'équipe des Ventes).
    - **Copier une étendue :** sélectionnez l'étendue, puis cliquez sur **Copier étendue** dans la barre d'actions. Entrez un nom et une description. Modifiez les types d'objets et les objets, si nécessaire.
    - **Modifier une étendue :** sélectionnez l'étendue, puis cliquez sur **Modifier l'étendue** dans la barre d'actions. Modifiez le nom, la description, les types d'objet et les objets, si nécessaire.
    - **Supprimer une étendue :** sélectionnez l'étendue, puis cliquez sur **Supprimer l'étendue** dans la barre d'actions. Lorsque vous y êtes invité, confirmez la suppression.

### Créer des rapports

Vous pouvez créer deux types de rapports d'administration déléguée :

- Ce rapport HTML indique les paires rôle/étendue associées à un administrateur et dresse la liste des autorisations individuelles pour chaque type d'objet (par exemple, les groupes de mise à disposition et les catalogues de machines). Vous pouvez générer ce rapport à partir de Web Studio.

  Pour créer ce rapport, procédez comme suit :

  1. Connectez-vous à Web Studio, cliquez sur **Administrateurs** dans le volet de gauche
  2. Sélectionnez un administrateur, puis cliquez sur **Créer un rapport** dans la barre d'actions.

  Vous pouvez également demander ce rapport lors de la création, de la copie ou de la modification d'un administrateur.

- Un rapport HTML ou CSV qui mappe tous les rôles personnalisés et intégrés à des autorisations. Vous pouvez générer ce rapport en exécutant le script PowerShell nommé OutputPermissionMapping.ps1.

  Pour exécuter ce script, vous devez être un administrateur complet, un administrateur en lecture seule ou un administrateur personnalisé avec autorisation de lecture des rôles. Le script se trouve dans : Program Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts.

  Syntaxe :

  ```
  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]
  ```

| Paramètre | Description |
|---|---|
| -Help | Affiche l'aide du script. |
| -Csv | Spécifie le fichier CSV de sortie. Valeur par défaut = HTML |
| -Path string | Où écrire la sortie. Valeur par défaut = stdout |
| -AdminAddress string | Adresse IP ou nom d'hôte du Delivery Controller auquel se connecter. Valeur par défaut = XA |
| -Show | (Valide uniquement lorsque le paramètre -Path est également spécifié). Lorsque vous écrivez la sortie vers un fichier, -Show entraîne l'ouverture de la sortie dans un programme approprié, tel qu'un navigateur Web. |
| CommonParameters | Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer et OutVariable. Pour plus d'informations, veuillez consulter la documentation Microsoft. |

L'exemple suivant écrit une table HTML sur un fichier appelé Roles.html et ouvre la table dans un navigateur Web.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html  – Show
<!--NeedCopy-->
```

L'exemple suivant écrit une table CSV sur un fichier appelé Roles.csv. La table n'est pas affichée.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
```

```
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
 – CSV -Path Roles.csv
<!--NeedCopy-->
```

À partir d'une invite de commande Windows, l'exemple de commande précédente est :

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
<!--NeedCopy-->
```

## Delivery Controller

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Le Delivery Controller est le composant côté serveur qui est responsable de la gestion de l'accès utilisateur, ainsi que de la négociation et de l'optimisation des connexions. Les Controller fournissent également les services Machine Creation qui créent des images de bureau et de serveur.

Un site doit avoir au moins un Controller. Après avoir installé le Controller initial, vous pouvez ajouter des Controller supplémentaires lorsque vous créez un site, ou plus tard. Avoir plus d'un Controller dans un site présente deux avantages.

- **Redondance :** il est recommandé qu'un site de production dispose toujours d'au moins deux Controller sur des serveurs physiques différents. Si un Controller échoue, les autres peuvent gérer les connexions et administrer le site.
- **Évolutivité :** au fur et à mesure que l'activité du site augmente, il en va de même pour l'utilisation de l'UC sur le Controller et l'activité de la base de données. Les Controller supplémentaires permettent de gérer plus d'utilisateurs et plus de demandes d'applications et de bureaux, et peuvent améliorer la réactivité générale.

Chaque Controller communique directement avec la base de données du site. Dans un site avec plusieurs zones, les Controller de chaque zone communiquent avec la base de données du site dans la zone principale.

> **Important :**
>
> Ne modifiez pas le nom de l'ordinateur ou l'appartenance à un domaine d'un Controller une fois que le site est configuré.

### Comment les VDA s'enregistrent auprès d'un Controller

Avant qu'un VDA puisse être utilisé, il doit s'enregistrer (établir la communication) auprès d'un Delivery Controller sur le site. Pour plus d'informations sur l'enregistrement de VDA, voir Enregistrement d'un VDA auprès d'un Delivery Controller.

### Ajouter, supprimer ou déplacer des Delivery Controller

Pour ajouter, supprimer ou déplacer un Controller, vous devez disposer des autorisations de rôle de serveur et de rôle de base de données répertoriées dans l'article Bases de données.

L'installation d'un Controller sur un nœud dans une installation de mise en cluster SQL ou mise en miroir SQL n'est pas prise en charge.

Lorsque vous ajoutez un Delivery Controller à un site, veillez à ajouter des informations d'identification d'ouverture de session pour cette machine à n'importe quel réplica SQL Server que vous utilisez pour la haute disponibilité.

Si votre déploiement utilise la mise en miroir de base de données :

- Avant l'ajout, la suppression ou le déplacement d'un Controller, assurez-vous que les bases de données principale et en miroir sont en cours d'exécution. En outre, si vous utilisez les scripts avec SQL Server Management Studio, activez le mode SQLCMD avant d'exécuter les scripts.
- Pour vérifier la mise en miroir après l'ajout, la suppression ou le déplacement d'un Controller, exécutez l'applet de commande PowerShell `Get-configdbconnection`. Cette applet de commande garantit que le partenaire de basculement a été défini dans la chaîne de connexion au miroir.

Après avoir ajouté, supprimé ou déplacé un Delivery Controller :

- Si la mise à jour automatique est activée, les VDA reçoivent une liste actualisée des Delivery Controller dans les 90 minutes qui suivent.
- Si la mise à jour automatique n'est pas activée, vérifiez que le paramètre de stratégie du Delivery Controller ou la clé de registre ListOfDDCs sont mis à jour pour tous les VDA. Après déplacement d'un Delivery Controller vers un autre site, mettez à jour le paramètre de stratégie ou la clé de registre sur les deux sites.

### Ajouter un Controller

Vous pouvez ajouter des Controller lorsque vous créez un site et ultérieurement. Vous ne pouvez pas ajouter des Controller installés avec une version antérieure de ce logiciel à un site qui a été créé avec cette version.

1. Exécutez le programme d'installation sur un serveur contenant un système d'exploitation pris en charge. Installez le composant Delivery Controller et les autres composants principaux requis. Suivez les instructions de l'assistant d'installation.
2. Si vous n'avez pas encore créé de site, exécutez Citrix Site Manager sur ce Controller pour créer un site. L'adresse IP de ce Controller est automatiquement ajoutée au nouveau site.

   Si vous souhaitez générer des scripts qui initialisent les bases de données, ajoutez les Controller avant de générer les scripts.
3. Si vous avez déjà créé un site, procédez comme suit :

   a) Exécutez Citrix Site Manager sur ce Controller, cliquez sur **Rejoindre un site existant** et saisissez l'adresse d'un Controller pour le site que vous souhaitez rejoindre.
   b) Exécutez l'outil de configuration Studio pour ajouter le Controller à Web Studio.

### Supprimer un Controller

La suppression d'un Controller d'un site ne désinstalle pas le logiciel Citrix ou tout autre composant. Cette action supprime le Controller de la base de données afin qu'il ne puisse plus être utilisé pour négocier des connexions et effectuer d'autres tâches. Si vous supprimez un Delivery Controller, vous pouvez le rajouter par la suite au même site ou à un autre site. Un site a besoin d'au moins un Delivery Controller ; vous ne pouvez donc pas supprimer le dernier Delivery Controller répertorié dans Web Studio.

Lorsque vous supprimez un Controller d'un site, l'ouverture de session Controller sur le serveur de base de données n'est pas supprimée. Cela évite potentiellement la suppression d'une ouverture de session utilisée par des services d'autres produits sur la même machine. L'ouverture de session doit être supprimée manuellement si elle n'est plus requise. L'autorisation de rôle serveur `securityadmin` est nécessaire pour supprimer l'ouverture de session.

Après avoir supprimé un Controller :

- Les VDA utilisant la mise à jour automatique se réinscrivent auprès d'autres Controller disponibles. Ce réenregistrement se produit uniquement si le mécanisme de mise à jour automatique est activé et si les VDA peuvent contacter d'autres Controller (dans la même zone secondaire que le Controller supprimé ou dans la zone principale pour les déploiements locaux).

- Mettez à jour les informations du Controller dans Citrix StoreFront. Pour plus d'informations, consultez Gérer les Controller.
- Dans Citrix StoreFront, mettez à jour les URL de Secure Ticket Authority (STA) pour l'accès à distance via Citrix Gateway. Pour plus d'informations, consultez Gérer les Secure Ticket Authorities.
- Dans Citrix Gateway, mettez à jour toutes les URL de STA de serveur virtuel. Pour de plus amples informations, consultez Citrix Gateway.

> **Important :**
>
> Ne supprimez pas le Controller depuis Active Directory tant que vous ne l'avez pas supprimé du site.

1. Assurez-vous que le Controller est sous tension afin que Web Studio puisse se charger en moins d'une heure. Une fois que Web Studio a chargé le Controller que vous souhaitez supprimer, assurez-vous que tous les services du Controller sont en cours d'exécution et que le Controller est hors tension.
2. Connectez-vous à Web Studio et sélectionnez **Paramètres** dans le volet de gauche.
3. Localisez la vignette **Delivery Controller** et cliquez sur **Modifier**.
4. Sur la page **Gérer les Delivery Controller**, sélectionnez le Controller que vous souhaitez supprimer.
5. Sélectionnez **Supprimer Controller**. Si vous ne possédez pas les droits et les rôles de base de données appropriés, vous pouvez générer un script qui permet à votre administrateur de base de données de supprimer le Delivery Controller à votre place.

   Web Studio effectue une pré-vérification avant de supprimer un Controller. Un Controller peut être supprimé en toute sécurité s'il est hors tension et ne se trouve pas dans l'un des états de service suivants :

   - Inconnu
   - Défaillance en attente
   - Ancienne version
   - Version plus récente
   - Changement de version en cours
   - Fonctionnalités obligatoires manquantes

   Si le Controller n'est pas hors tension et se trouve dans l'un des états de service mentionnés, Web Studio vous invite à mettre le Controller hors tension.
6. Vous devez supprimer le compte de machine du Delivery Controller du serveur de base de données. Avant la suppression, vérifiez qu'aucun autre service n'utilise le compte.

Après utilisation de Web Studio pour supprimer un Controller, le trafic vers ce Controller peut rester affiché pour un laps de temps pour assurer le bon d'achèvement des tâches courantes. Si vous souhaitez forcer la suppression d'un Controller dans un bref délai, Citrix vous recommande de fermer le serveur sur lequel il a été installé, ou de supprimer ce serveur à partir d'Active Directory. Ensuite, redémarrez les autres Controller du site pour vous assurer qu'aucune autre communication avec le Controller supprimé n'est réalisée.

#### Déplacer un Controller vers une autre zone

Si votre site contient plusieurs zones, vous pouvez déplacer un Controller vers une autre zone. Consultez Zones pour savoir comment ce déplacement peut affecter l'enregistrement de VDA et d'autres opérations.

1. Sélectionnez **Zone** dans le volet de gauche.
2. Sélectionnez une zone dans le volet central, puis sélectionnez un Controller.
3. Sélectionnez **Déplacer des éléments** dans la barre d'actions.
4. Sur la page **Déplacer des éléments** qui s'affiche, sélectionnez la zone dans laquelle vous souhaitez déplacer le Controller.
5. Cliquez sur **Enregistrer**.

#### Déplacer un VDA vers un autre site

Si un VDA a été provisionné à l'aide de Citrix Provisioning ou qu'il est une image existante, vous pouvez déplacer un VDA vers un autre site (d'un site 1 au site 2) lors de la mise à niveau, ou lors du déplacement d'une image de VDA qui a été créée dans un site test vers un site de production. Les VDA provisionnés à l'aide de Machine Creation Services (MCS) ne peuvent pas être déplacés d'un site à un autre. MCS ne prend pas en charge la modification de la liste ListOfDDC qu'un VDA vérifie pour s'enregistrer auprès d'un Controller. Les VDA provisionnés à l'aide de MCS vérifient toujours la liste ListOfDDC associée au site dans lequel ils ont été créés.

Il existe deux façons de déplacer un VDA vers un autre site : à l'aide du programme d'installation ou de stratégies Citrix.

**Programme d'installation** Exécutez le programme d'installation et ajoutez un Controller, en spécifiant le nom complet (entrée DNS) d'un Controller du site 2.

Ne spécifiez les Controller dans le programme d'installation que lorsque le paramètre de stratégie des Controller n'est pas utilisé.

**Éditeur de stratégie de groupe** L'exemple suivant déplace plusieurs VDA entre sites.

1. Créez une stratégie dans le site 1 qui contient les paramètres suivants, puis filtrez la stratégie au niveau du groupe de mise à disposition pour initier une migration VDA échelonnée entre les sites.

    - Controller : contenant les noms complets (entrées DNS) d'un ou de plusieurs Controller dans le site 2.
    - Activer la mise à jour automatique des Controller : défini sur désactivé.

2. Chaque VDA dans le groupe de mise à disposition reçoit une alerte dans les 90 minutes qui suivent la création de la nouvelle stratégie. Le VDA ignore la liste de Controller qu'il reçoit (car la mise à jour automatique est désactivée) : il sélectionne l'un des Controller spécifiés dans la stratégie, qui répertorie les Controller du site 2.

3. Lorsque le VDA s'enregistre avec succès auprès d'un Controller du site 2, il reçoit la liste ListOfDDC du site 2 et les informations de stratégie, dans laquelle la mise à jour automatique est activée par défaut. Le Controller avec lequel le VDA a été enregistré sur le site 1 ne figure pas sur la liste envoyée par le Controller sur le site 2. Par conséquent, le VDA se réenregistre, en choisissant parmi les Controller dans la liste du site 2. Dès lors, le VDA est automatiquement mis à jour avec les informations du site 2.

Pour plus d'informations sur l'utilisation de l'éditeur de stratégie de groupe, consultez la documentation sur les stratégies Citrix.

## Prise en charge de IPv4/IPv6

June 27, 2024

Cette version prend en charge les déploiements IPv4 purs, IPv6 purs et double pile qui utilisent des réseaux IPv4 et IPv6 qui se chevauchent.

Les composants suivants prennent uniquement en charge IPv4. Tous les autres prennent en charge IPv4 et IPv6.

- XenServer
- VDA non contrôlés par le paramètre de stratégie **Uniquement utiliser l'enregistrement du contrôleur IPv6**

Les communications IPv6 sont contrôlées par deux paramètres de stratégie Citrix liés à la connexion au VDA :

- **Paramètre principal qui applique l'utilisation de IPv6 :** Uniquement utiliser l'enregistrement du contrôleur IPv6.

  Ce paramètre de stratégie détermine le format d'adresse utilisé par le VDA pour s'enregistrer avec le Delivery Controller :

  Lorsqu'il est activé, le VDA s'enregistre auprès du Controller et communique avec ce dernier à l'aide d'une seule adresse IPv6 choisie dans l'ordre suivant : adresse IP globale, adresse locale unique (ULA), adresse locale du lien (uniquement si aucune autre adresse IPv6 n'est disponible).

  Lorsque cette stratégie est désactivée, le VDA s'enregistre et communique avec le Controller à l'aide de l'adresse IPv4 de la machine. Il s'agit de la valeur par défaut.

  Si une équipe utilise fréquemment un réseau IPv6, publiez les bureaux et les applications pour ces utilisateurs en fonction d'une image ou d'une unité d'organisation (UO) sur laquelle le paramètre de stratégie **Uniquement utiliser l'enregistrement du contrôleur IPv6** est activé.

  Si une équipe utilise fréquemment un réseau IPv4, publiez les bureaux et les applications pour ces utilisateurs en fonction d'une image ou d'une unité d'organisation (UO) sur laquelle le paramètre de stratégie **Uniquement utiliser l'enregistrement du contrôleur IPv6** est désactivé.

- **Paramètre dépendant qui définit un masque de réseau IPv6 :** Masque réseau IPv6 d'enregistrement du contrôleur.

  Une machine peut avoir plusieurs adresses IPv6. Ce paramètre de stratégie permet aux administrateurs de restreindre le VDA uniquement à un sous-réseau favori, plutôt qu'une adresse IP globale, si elle est enregistrée. Ce paramètre spécifie le réseau auprès duquel le VDA s'enregistre. Le VDA s'enregistre uniquement sur la première adresse qui correspond au masque de sous-réseau spécifié.

  Ce paramètre est uniquement valide si le paramètre de stratégie **Uniquement utiliser l'enregistrement du contrôleur IPv6** est activé. Valeur par défaut = chaîne vide

### Considérations de déploiement

Si votre environnement contient à la fois les réseaux IPv4 et IPv6, créez des configurations de groupe de mise à disposition distinctes pour les clients IPv4 et pour les clients qui peuvent accéder au réseau IPv6. Pensez à différencier les utilisateurs à l'aide de noms différents, attributions manuelles de groupes Active Directory ou filtres SmartAccess.
La reconnexion à une session peut échouer si la connexion démarre sur un réseau IPv6, puis que vous essayez de vous connecter à nouveau à partir d'un client ne disposant que d'un accès IPv4.

REMARQUE - Ces considérations ne s'appliquent pas si la résolution DNS est activée

# Système de licences pour Citrix Virtual Apps and Desktops avec Web Studio

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Vous pouvez utiliser Web Studio pour gérer et suivre les licences, à condition que le serveur de licences se trouve dans le même domaine que Web Studio, ou dans un domaine approuvé. Pour de plus amples informations sur les tâches liées aux licences, consultez la documentation relative au système de licences et Licences multitypes.

Le tableau suivant dresse la liste des versions prises en charge et les modèles de licences :

| Produits | Éditions | Modèles de licence |
|---|---|---|
| Citrix Virtual Apps | Premium, Advanced, Standard | Licences simultanées |
| Citrix Virtual Desktops | Premium, Advanced, Standard | Utilisateur/machine et Utilisateurs simultanés |

Pour plus d'informations, consultez Licences simultanées et Licence utilisateur/machine.

## Version actuelle (CR) et version Long Term Service Release (LTSR) prises en charge

Le tableau suivant répertorie la **version LS minimale compatible** pour Citrix Virtual Apps and Desktops, XenApp et XenDesktop. Pour plus d'informations sur les dates de cycle de vie des produits Citrix, consultez le Tableau des produits.

> **Important :**
>
> Les informations du tableau suivant sont fournies uniquement pour la compatibilité des produits. Citrix vous recommande vivement de toujours utiliser la dernière version disponible du serveur de licences Citrix pour bénéficier des améliorations fonctionnelles ou de sécurité qu'elle peut contenir.
>
> **Remarque :**

> Le serveur de licences VPX est obsolète et ne bénéficiera pas d'autres correctifs de maintenance ou de sécurité. Les clients utilisant la version 11.16.6 ou des versions antérieures de License Server VPX sont invités à migrer vers la dernière version du serveur de licences pour Windows dès que possible.

| Version actuelle | Version LS minimale compatible |
|---|---|
| 2305 | 11.17.2.0 Build 35000 |
| 2303 | 11.17.2.0 Build 35000 |
| 2212 | 11.17.2.0 Build 35000 |
| 2209 | 11.17.2.0 Build 35000 |
| 2206 | 11.17.2.0 Build 35000 |
| 2203 | 11.17.2.0 Build 35000 |
| 2112 | 11.17.2.0 Build 35000 |
| 2109 | 11.17.2.0 Build 35000 |
| 2106 | 11.17.2.0 Build 35000 |
| 2103 | 11.16.3.0 Build 28000 |

| Long Term Service Release | Version LS minimale compatible |
|---|---|
| 2203 LTSR | 11.17.2.0 Build 35000 |
| 1912 LTSR | 11.16.3.0 Build 28000 |
| 7.15 LTSR | 11.15.0.0 Build 24100 |
| 7.6 LTSR | 11.14.0.1 Build 21103 |

Pour de plus amples informations sur les anciens produits et les versions de produits, reportez-vous au Tableau des produits d'ancienne génération.

Vous devez être un administrateur de licence complet pour effectuer les tâches suivantes. Pour afficher les informations de licence dans Web Studio, un administrateur doit avoir au moins l'autorisation d'administration déléguée de licence en lecture. Les rôles d'administrateur complet et d'administrateur en lecture seule intégrés disposent de cette autorisation.

### Télécharger et installer une licence à partir de Citrix à l'aide de Web Studio

1. Connectez-vous à Web Studio et sélectionnez **Gestion des licences** dans le volet de gauche.

2. Sélectionnez **Allouer des licences** dans la barre d'actions.
3. Entrez le code d'accès à la licence que vous avez reçu dans un e-mail de Citrix après l'achat ou le renouvellement des licences.
4. Sélectionnez un produit et choisissez **Allouer des licences**. Les licences disponibles pour ce produit sont allouées et téléchargées. Veuillez noter qu'après avoir alloué et téléchargé toutes les licences pour un code d'accès aux licences spécifique, vous ne pouvez plus utiliser ce code. Pour effectuer d'autres transactions avec le même code, connectez-vous à Mon Compte.

### Ajouter des licences qui sont stockées sur votre ordinateur local ou sur le réseau

1. Connectez-vous à Web Studio et sélectionnez **Gestion des licences** dans le volet de gauche.
2. Sélectionnez **Ajouter des licences** dans la barre d'actions.
3. Accédez à un fichier de licences et ajoutez-le au serveur de licences.

### Changer de serveur de licences

1. Connectez-vous à Web Studio et sélectionnez **Gestion des licences** dans le volet de gauche.
2. Sélectionnez **Changer le serveur de licences** dans la barre d'actions.
3. Tapez l'adresse du serveur de licences sous la forme *nom:port*, où nom est une adresse DNS, NetBIOS ou IP. Si vous n'indiquez pas de numéro de port, le port par défaut (27000) est utilisé.

### Sélectionner le type de licence à utiliser

- Lors de la configuration du site, après avoir spécifié le serveur de licences, vous êtes invité à sélectionner le type de licence à utiliser. S'il n'y a aucune licence sur le serveur, l'option d'utilisation du produit pour une période d'évaluation de 30 jours est automatiquement sélectionnée.
- Si le serveur comporte des licences, leurs détails sont affichés et vous pouvez sélectionner l'une d'elles. Vous pouvez également ajouter un fichier de licences au serveur et le sélectionner.

### Changer l'édition du produit et le modèle de licence

1. Connectez-vous à Web Studio et sélectionnez **Gestion des licences** dans le volet de gauche.
2. Sélectionnez **Modifier l'édition du produit** dans la barre d'actions.
3. Mettez à jour les options appropriées.

Pour accéder à la console License Administration Console, sélectionnez **License Administration Console** dans la barre d'actions. La console soit apparaît immédiatement soit, si le tableau de bord est

configuré comme protégé par un mot de passe, vous êtes invité à entrer les informations d'identification de la console License Administration Console. Pour plus de détails sur l'utilisation de la console, veuillez consulter la documentation concernant les licences.

> **Remarque :**
>
> Lorsque vous changez de licence dans Web Studio, la modification prend jusqu'à 5 minutes pour apparaître dans Citrix Director. Par exemple, si vous basculez entre Advanced et Premium ou vice versa.

### Ajouter un administrateur de licences

1. Connectez-vous à Web Studio et sélectionnez **Gestion des licences** dans le volet de gauche.
2. Sélectionnez l'onglet **Administrateurs de licences**.
3. Sélectionnez **Ajouter un administrateur de licences** dans la barre d'actions.
4. Recherchez le nom de l'utilisateur que vous souhaitez ajouter en tant qu'administrateur et choisissez les autorisations.

### Modifier les autorisations d'un administrateur de licences ou supprimer un administrateur de licences

1. Connectez-vous à Web Studio et sélectionnez **Gestion des licences** dans le volet de gauche.
2. Sélectionnez l'onglet **Administrateurs de licences**, puis sélectionnez l'administrateur.
3. Sélectionnez **Modifier l'administrateur de licences** ou **Supprimer l'administrateur de licences** dans la barre d'actions.

### Ajouter un groupe d'administrateurs de licences

1. Connectez-vous à Web Studio et sélectionnez **Gestion des licences** dans le volet de gauche.
2. Sélectionnez l'onglet **Administrateurs de licences**.
3. Sélectionnez **Ajouter un groupe d'administrateurs de licences** dans la barre d'actions.
4. Recherchez le groupe que vous souhaitez voir opérer en tant qu'administrateur de licences et choisissez les autorisations. L'ajout d'un groupe Active Directory donne à l'administrateur de licences des autorisations d'accès aux utilisateurs dans ce groupe.

### Modifier les autorisations d'un groupe d'administrateurs de licences ou supprimer un groupe d'administrateurs de licences

1. Connectez-vous à Web Studio et sélectionnez **Gestion des licences** dans le volet de gauche.

2. Sélectionnez l'onglet **Administrateurs de licences**, puis sélectionnez le groupe d'administrateurs.
3. Sélectionnez **Modifier le groupe d'administrateurs de licences** ou **Supprimer le groupe d'administrateurs de licences** dans la barre d'actions.

### Afficher les informations de licence

Connectez-vous à Web Studio et sélectionnez **Gestion des licences** dans le volet de gauche. Un récapitulatif de l'utilisation des licences et des paramètres du site est affiché, ainsi qu'une liste de toutes les licences actuellement installées sur le serveur de licences spécifié.

Assurez-vous que les paramètres de licence du site, qui incluent le type de produit, l'édition de licence et le modèle de licence, correspondent aux licences que votre serveur de licences configuré utilise. Si ce n'est pas le cas, vous devrez peut-être télécharger ou allouer vos licences existantes pour qu'elles correspondent aux paramètres de licence du site.

### Afficher les alertes d'expiration de licence

Web Studio interroge les dates d'expiration du fichier de licence à partir du serveur de licences Citrix. Web Studio avertit les administrateurs dans l'onglet Aperçu si les fichiers de licence approchent de la date d'expiration ou ont déjà expiré.

### Liens associés

- Consultez Abonnement local Citrix pour les licences de détail annuelles et temporaires.
- Consultez Transition et échange avec droits hybrides.

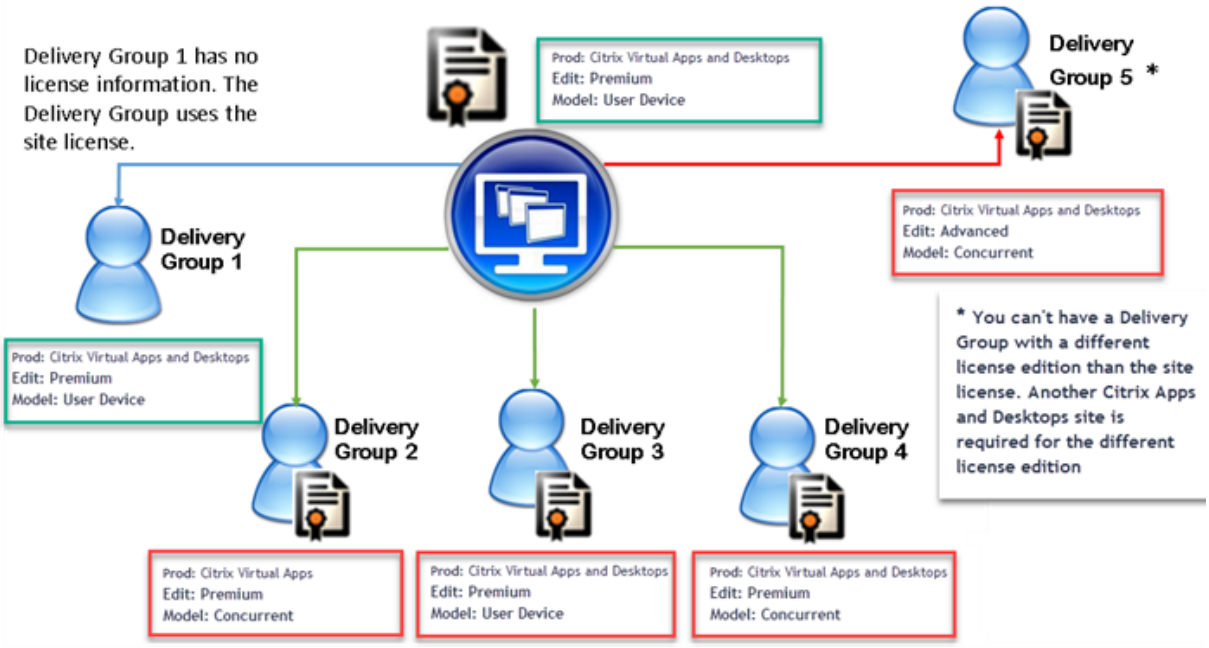
## Licences multitypes

June 27, 2024

La fonction Licences multitypes prend en charge la consommation de différents types de licence pour les groupes de mise à disposition sur un seul site Citrix Virtual Apps and Desktops. Le **Type** est une combinaison unique de l'ID du produit (XDT ou MPS) et du modèle (UserDevice ou Concurrent). Les groupes de mise à disposition doivent utiliser la même édition de produit (PLT/Premium ou ENT/Advanced) que celle configurée au niveau du site. Tenez compte des considérations spéciales figurant à la fin de cet article lorsque vous configurez des licences multitypes pour vos déploiements Citrix Virtual Apps and Desktops.

Si la fonction Licences multitypes n'est pas configurée, il est possible d'utiliser différents types de licences uniquement si elles sont configurées sur des sites distincts. Les groupes de mise à disposition utilisent la licence de site. Pour connaître les limitations de notification importantes lorsque des licences multitypes sont configurées, consultez les considérations spéciales.




Pour déterminer les groupes de mise à disposition qui consomment différents types de licence, utilisez ces applets de commande PowerShell de Broker :

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

Pour installer des licences, utilisez :

- Citrix Studio
- Citrix Licensing Manager
- citrix.com

Les dates de Customer Success Services sont spécifiques à chaque fichier de licence et à chaque produit et modèle. Les groupes de mise à disposition définis différemment peuvent avoir différentes dates de Customer Success Services.

### Considérations spéciales

Les licences multitypes proposent des fonctionnalités différentes des licences Citrix Virtual Apps and Desktops standard.

Director et Studio n'envoient pas d'alertes ni de notifications pour les groupes de mise à disposition configurés pour utiliser un type différent de celui de la configuration du site :

- Aucune notification lors de l'approche des limites de la licence ou du déclencheur ou de l'expiration de la période de grâce supplémentaire.
- Aucune notification lorsqu'un groupe spécifique a un problème.

Les groupes de mise à disposition configurés pour des licences multitypes consomment SEULEMENT ce type de licence et ne reviennent pas à la configuration du site lorsqu'elles sont entièrement consommées.

Bien que les noms d'édition de licence Citrix Virtual Apps Standard et Citrix Virtual Desktops Standard indiquent qu'elles sont toutes les deux de type standard, elles ne correspondent pas à la même édition. Les licences multitypes ne sont pas disponibles avec les licences Citrix Virtual Apps Standard et Citrix Virtual Desktop Standard.

### Matrice de compatibilité des licences

Ce tableau détaille les anciens noms de produits, les nouveaux noms de produits et les noms de fonctions associés. Les quatre colonnes de compatibilité spécifient les combinaisons de produits et de modèles de licence compatibles pour les licences multi-types. CCU et CCS désigne des licences simultanées et UD des licences utilisateurs/périphériques.

| Old Name | New Name | Feature | Multi-type licensing compatibility | | | |
|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 |
| Citrix XenApp Standard | Citrix XenApp Standard | MPS_STD_CCU | X | | | |
| Citrix XenApp Advanced | Citrix Virtual Apps Standard | MPS_ADV_CCU | | X | | |
| Citrix XenApp Enterprise | Citrix Virtual Apps Advanced | MPS_ENT_CCU | | | X | |
| Citrix XenApp Platinum | Citrix Virtual Apps Premium | MPS_PLT_CCU | | | | X |
| CSP - Citrix XenApp Base | Citrix Virtual Apps Base | XDT_ADV_UD | | X | | |
| CSP Premium | Citrix Virtual Apps and Desktops Premium | XDT_PLT_UD | | | | X |
| Citrix XenDesktop VDI Edition (XDT-U) | Citrix Virtual Desktops - Per User/Device | XDT_STD_UD | X | | | |
| Citrix XenDesktop VDI Edition (XDT-C) | Citrix Virtual Desktops - Concurrent | XDT_STD_CCS | X | | | |
| Citrix XenDesktop Enterprise Edition (XDT-C) | Citrix Virtual Apps and Desktops Advanced - Concurrent | XDT_ENT_CCS | | | X | |
| Citrix XenDesktop Enterprise Edition (XDT-U) | Citrix Virtual Apps and Desktops Advanced - Per User/Device | XDT_ENT_UD | | | X | |
| Citrix XenDesktop Platinum Edition (XDT-C) | Citrix Virtual Apps and Desktops Premium - Concurrent | XDT_PLT_CCS | | | | X |
| Citrix XenDesktop Platinum Edition (XDT-U) | Citrix Virtual Apps and Desktops Premium - Per User/Device | XDT_PLT_UD | | | | X |

### SDK PowerShell de Broker

L'objet **DesktopGroup** a ces deux propriétés que vous pouvez manipuler à l'aide des applets de commande New-BrokerDesktopGroup et Set-BrokerDesktopGroup.

| Nom | Valeur | Restriction |
|---|---|---|
| LicenseModel | Un paramètre (Concurrent ou UserDevice) spécifiant le modèle de licence pour le groupe. Si aucun n'est spécifié, le modèle de licence à l'échelle du site est utilisé. | Si la fonctionnalité est désactivée, la définition des propriétés échoue. |
| ProductCode | Chaîne de texte XDT (pour Citrix Virtual Desktops) ou MPS (pour Citrix Virtual Apps) spécifiant l'ID de produit de licence pour le groupe. Si aucun n'est spécifié, le code produit à l'échelle du site est utilisé. | Si la fonctionnalité est désactivée, la définition des propriétés échoue. |

Pour plus d'informations sur LicenseModel et ProductCode, consultez about_Broker_Licensing.

#### New-BrokerDesktopGroup

Crée un groupe de bureaux pour gérer la négociation des groupes de bureaux. Pour plus d'informations sur cette applet de commande, voir https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/.

#### Set-BrokerDesktopGroup

Désactive ou active un groupe de bureaux broker existant ou modifie ses paramètres. Pour plus d'informations sur cette applet de commande, voir https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/

#### Get-BrokerDesktopGroup

Récupère les groupes de bureaux correspondant aux critères spécifiés. Le résultat de l'applet de commande Get-BrokerDesktopGroup inclut les propriétés **ProductCode** et **LicenseModel** du groupe. Si

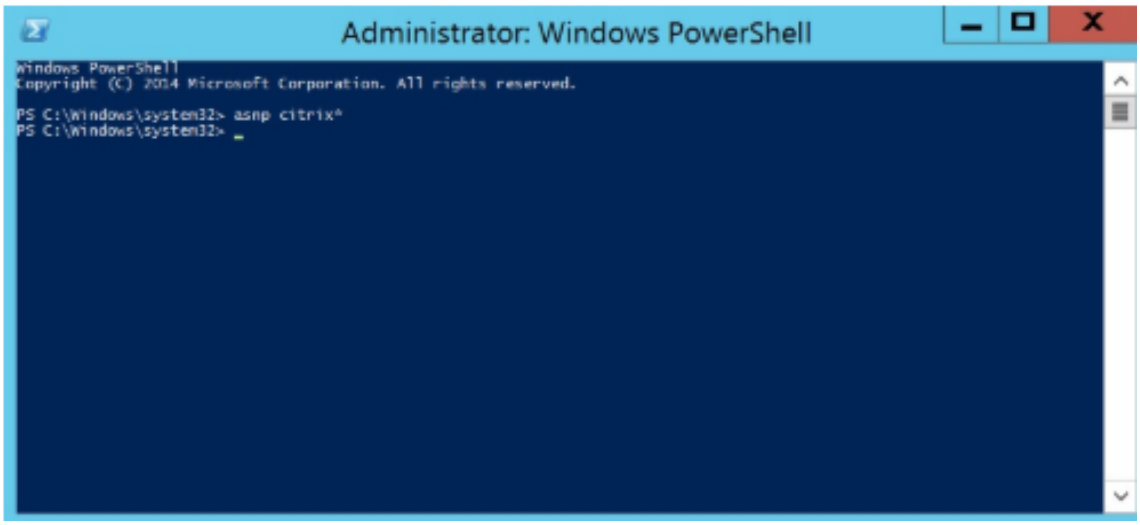
 

les propriétés n'ont pas été définies à l'aide de New-BrokerDesktopGroup ou Set- BrokerDesktop-Group, des valeurs null sont renvoyées. Si la valeur est null, le code de produit et le modèle de licence de l'ensemble du site sont utilisés. Pour plus d'informations sur cette applet de commande, voir https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/.

### Configurer différents produits et modèles de licence par groupe de mise à disposition

> **Remarque** vous ne pouvez pas configurer plus de deux types de produits, d'éditions ou de modèles de licence différents configurés sur un même groupe de mise à disposition. Si vous avez différents types de produits, d'éditions ou de modèles de licence, configurez-les dans des groupes de mise à disposition distincts.

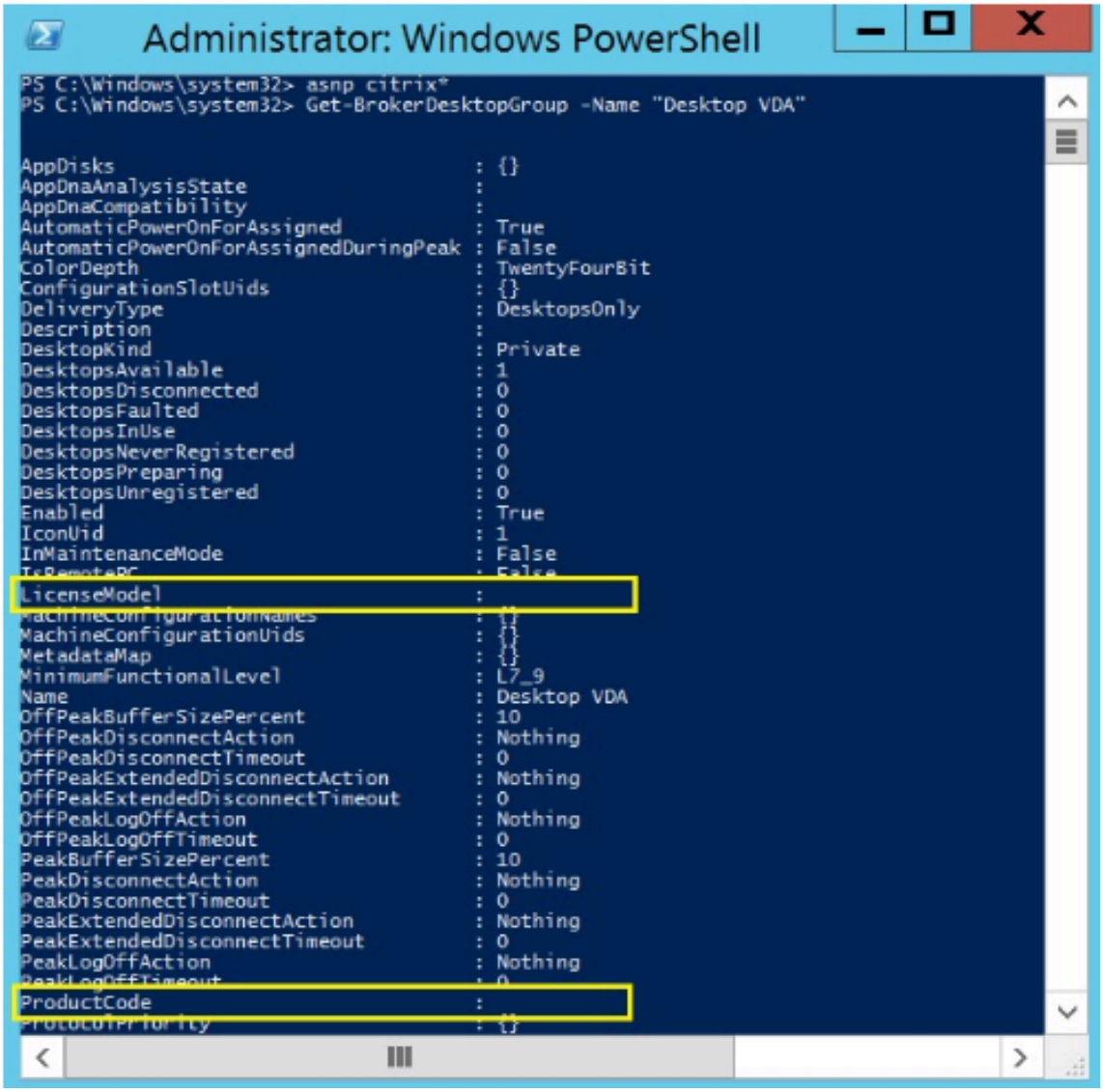
1. Ouvrez PowerShell avec des droits d'administration et ajoutez le composant logiciel enfichable Citrix.




2. Exécutez la commande **Get-BrokerDesktopGroup –Name "DeliveryGroupName"** pour afficher la configuration de licence actuelle. Recherchez les paramètres **LicenseModel** et **ProductCode**. Si vous n'avez pas configuré ces paramètres auparavant, ils peuvent être vides.

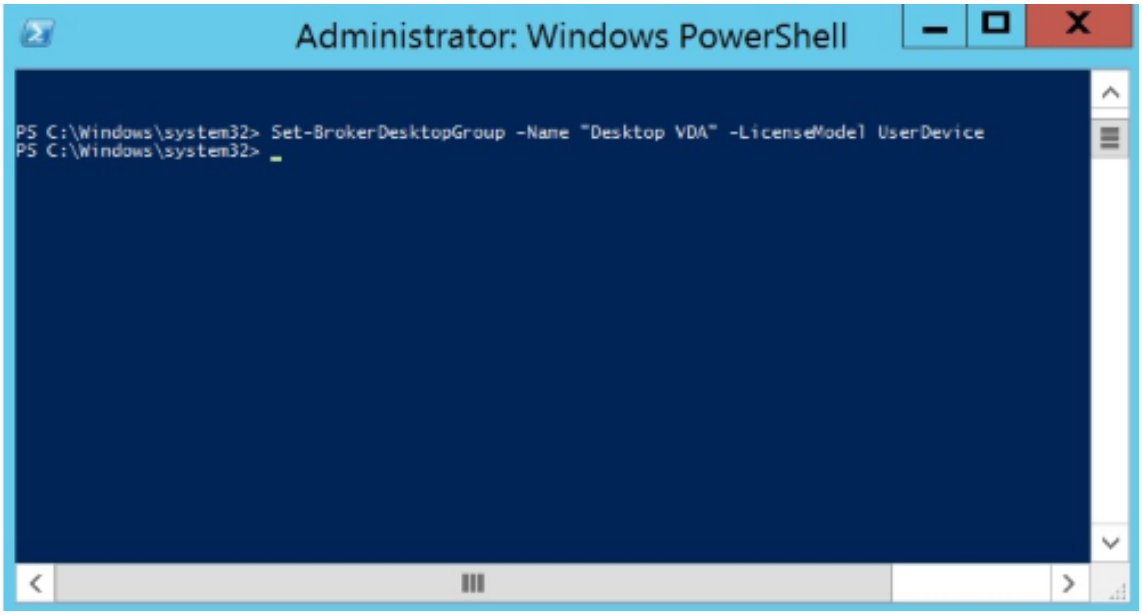
> **Remarque :**
>
> Si un groupe de mise à disposition ne dispose pas d'informations sur les licences, la **licence du site au niveau du site** est utilisée par défaut.

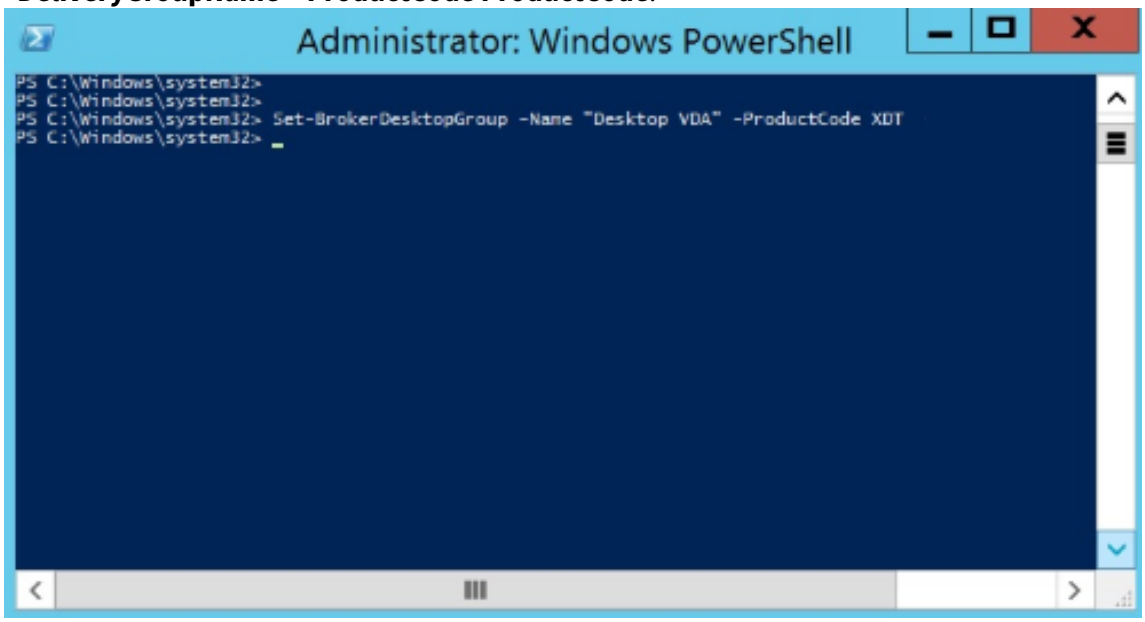



3. Modifiez le modèle de licence en exécutant la commande **Set-BrokerDesktopGroup –Name “DeliveryGroupName”–LicenseModel LicenseModel**.



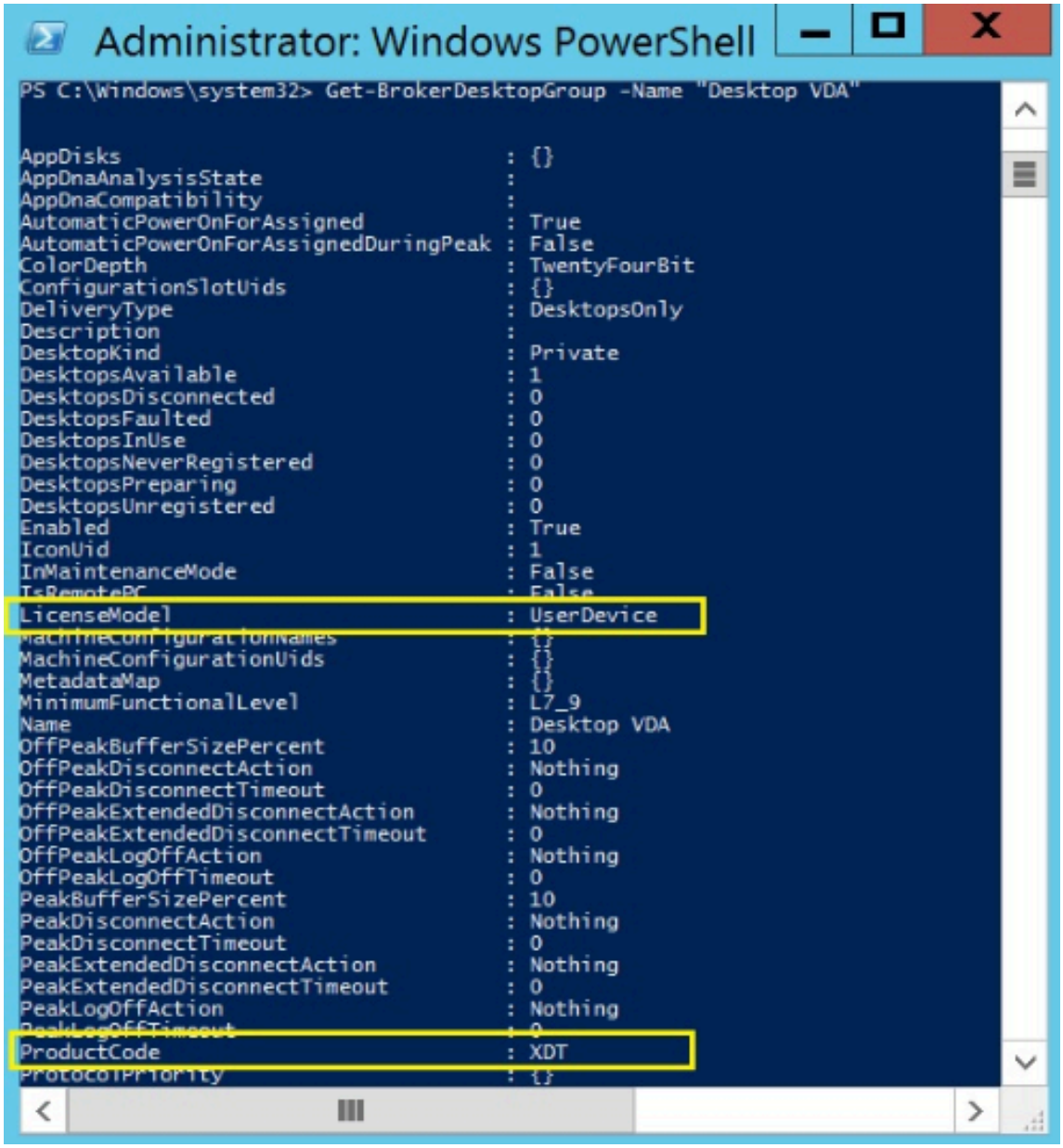

4. Modifiez le produit de licence en exécutant la commande **Set-BrokerDesktopGroup** –**Name “DeliveryGroupName”**–**ProductCode ProductCode**.




5. Entrez la commande **Get-BrokerDesktopGroup** –**Name “DeliveryGroupName”** pour valider les modifications.

> **Remarque :**
>
> Vous ne pouvez pas combiner différentes éditions au sein du même site. Par exemple, les licences Premium et Advanced. Plusieurs sites sont requis si vous disposez de licences avec différentes éditions.

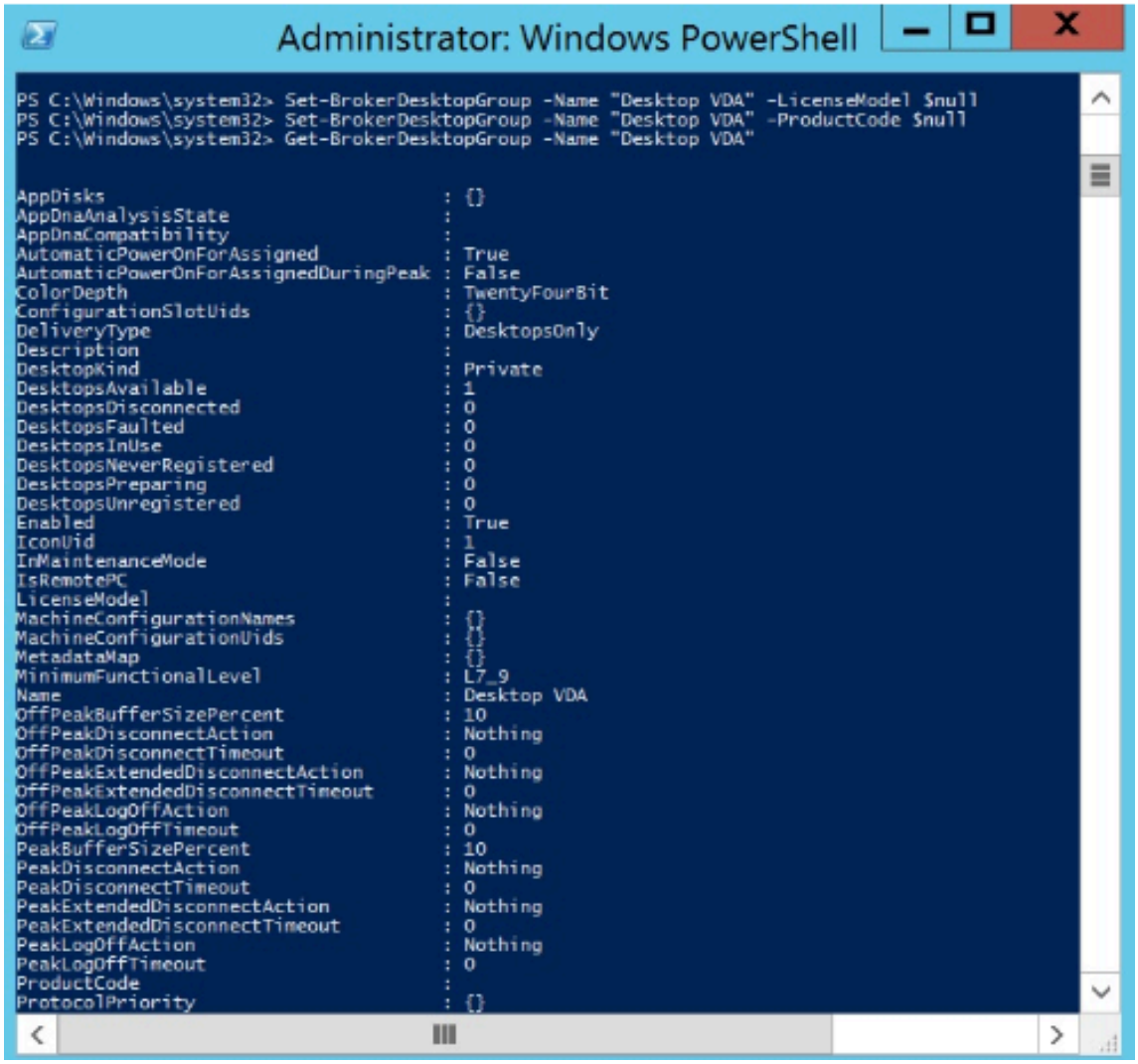
 




6. Supprimez la configuration de licence en exécutant les mêmes commandes **Set-BrokerDesktopGroup** décrites dans les étapes précédentes et définissez la valeur sur **$null**.

> **Remarque :**
>
> Studio n'affiche pas la configuration de licence pour chaque groupe de mise à disposition. Utilisez PowerShell pour afficher la configuration actuelle.




### Exemple

Cet exemple d'applet de commande PowerShell illustre la définition d'une licence multitypes pour deux groupes de mise à disposition existants et crée et définit un troisième groupe de mise à disposition.

Pour voir le produit sous licence et le modèle de licence associés à un groupe de mise à disposition, utilisez l'applet de commande PowerShell **Get-BrokerDesktopGroup**.

1. Nous définissons le premier groupe de mise à disposition pour XenApp et Concurrent.

   **Set-BrokerDesktopGroup -Name "Delivery group for Citrix Virtual Apps Premium Concurrent"-ProductCode MPS -LicenseModel Concurrent**

2. Nous définissons le deuxième groupe de mise à disposition pour XenDesktop et Concurrent.

**Set-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium Concurrent”-ProductCode XDT -LicenseModel Concurrent**

3. Nous créons et définissons le troisième groupe de mise à disposition pour XenDesktop et UserDevice.

   **New-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium UserDevice”-PublishedName “MyDesktop”-DesktopKind Private -ProductCode XDT -LicenseModel UserDevice**

## Questions fréquentes sur le système de licences

June 27, 2024

> **Remarque :**
>
> - Pour plus d’informations sur les ressources relatives à la continuité des activités liées à la pandémie COVID-19, consultez l’article CTX27055.
> - Pour plus d’informations sur le maintien de la continuité des activités, consultez la section Continuité des activités —à la demande.
> - Pour de plus amples informations sur la dernière version du serveur de licences Citrix, consultez la section Gestion des licences.

### Système de licences Citrix

#### Comment puis-je obtenir mon fichier de licence ?

Nous envoyons le code d’accès à la licence par e-mail. Il existe trois façons de générer des fichiers de licence à l’aide du code d’accès de licence :

- La page **Gérer les licences** depuis votre page Mon Compte sur `citrix.com`. Pour plus d’informations, consultez Gérer les licences sur citrix.com.
- Web Studio pour attribuer votre achat, le fichier de licence s’installe automatiquement sur votre serveur de licences Citrix.
- Citrix Licensing Manager au sein du serveur de licences Citrix pour attribuer votre achat et installer votre fichier de licence. Pour plus d’informations, consultez Installer des licences.

#### Comment attribuer une licence sur Mon compte ?

Consultez Allouer des licences.

### Comment ajouter des licences allouées au serveur de licences ?

Consultez Modifier les licences.

### Quels ports TCP utilise le système de licences Citrix ?

- Numéro de port du serveur de licences : 27000
- Numéro de port du démon vendeur : 7279
- Le port Web de la console Web de gestion est 8082.
- Le port Web Service for Licensing est 8083.

### Qu'est-ce que le serveur de licences Citrix ?

Un serveur de licences Citrix est un système permettant de partager les licences en réseau. Pour plus d'informations, voir Présentation des opérations du système de licences.

### Puis-je virtualiser ou regrouper le serveur de licences Citrix ?

Oui. Vous pouvez virtualiser ou regrouper le serveur de licences Citrix. Pour plus d'informations, consultez la section Serveurs de licences en cluster.

### Quels sont les avantages de la virtualisation du serveur de licences Citrix ?

La virtualisation du serveur de licences Citrix fournit une solution redondante. Cette solution permet la mobilité entre plusieurs serveurs physiques sans nécessiter de temps d'arrêt.

### Existe-t-il des limites à prendre en compte si je virtualise le serveur de licences Citrix ?

Non.

### Le serveur de licences Citrix gère-t-il toutes les licences pour mon déploiement Citrix Virtual Apps and Desktops ?

Le serveur de licences Citrix gère toutes les licences que vous recevez pour Citrix Virtual Apps and Desktop, à l'exception des licences Premium Edition utilisées avec Citrix Gateway. Les serveurs de licences intégrés aux appliances réseau en fonction des besoins de ces périphériques réseau orientés sécurité gèrent ces licences.

### Qu'est-ce que Citrix Licensing Manager ?

Citrix Licensing Manager permet de télécharger et d'allouer des fichiers de licences depuis le serveur de licences sur lequel vous avez installé Citrix Licensing Manager. Citrix Licensing Manager est la méthode de gestion de serveur de licences recommandée qui permet d'effectuer les actions suivantes :

- Enregistrement à l'aide d'un code court du serveur de licences sur Citrix Cloud et suppression facile de l'enregistrement.
- Configurer les comptes d'utilisateurs et de groupes
- Utilisez le tableau de bord pour afficher les licences installées, en cours d'utilisation, expirées et disponibles, ainsi que les dates Customer Success Services.
- Exporter les données d'utilisation de licence à utiliser dans les rapports
- Configurer la période de rétention des données historiques. La période de rétention par défaut des données est de 180 jours.
- Simplifier l'installation des fichiers de licences sur le serveur de licences en utilisant un code d'accès de licence ou un fichier téléchargé
- Activer et désactiver la période de grâce supplémentaire
- Configurer le Programme d'amélioration de l'expérience utilisateur (CEIP) et Call Home
- Vérifier manuellement ou automatiquement la disponibilité de licences de renouvellement Customer Success Services à des fins de notification ou d'installation
- Informer de l'état du serveur de licences : licence de démarrage absente, délais, échecs de chargement
- Modifier les ports suivants :
  - Serveur de licences (27000 par défaut)
  - Démon vendeur (7279 par défaut)
  - Web Services for Licensing (8083 par défaut)

Pour plus d'informations, consultez Citrix Licensing Manager.

### Où se trouve la console d'administration de licences Citrix ?

La console d'administration de licences n'est plus prise en charge et a été supprimée de la version 11.16.6 du serveur de licences. Nous vous recommandons d'utiliser Citrix Licensing Manager.

Vous pouvez utiliser Studio pour gérer et suivre les licences, à condition que le serveur de licences se trouve dans le même domaine que Studio, ou dans un domaine approuvé.

Pour plus d'informations, consultez Citrix Licensing Manager.

#### Quelle est la période d'attribution de licence ?

La période d'attribution de licence est le délai pendant lequel une licence Citrix Virtual Apps and Desktops est attribuée à un utilisateur ou à un appareil. La période d'attribution de licence par défaut est de 90 jours.

#### Comment puis-je savoir combien de licences mon organisation a achetées ?

Toutes les licences achetées peuvent être consultées et sont accessibles à tout moment (24 h/24 et 7 j/7) à partir de votre boîte à outils **Gérer les licences** sécurisée sur votre page **Mon compte** sur https://www.citrix.com.

#### Comment savoir combien de licences sont utilisées à tout moment ?

Citrix Licensing Manager et Studio fournissent des détails sur l'utilisation des licences en temps réel.

#### Récupération d'urgence et maintenance du serveur de licences

Pour plus d'informations sur la récupération d'urgence et la maintenance de votre serveur de licences, reportez-vous à Récupération d'urgence et maintenance dans la documentation relative aux licences Citrix.

### Licences Citrix Virtual Apps and Desktops

#### Système de licences de Citrix Virtual Apps and Desktops

Le système de licences de Citrix Virtual Apps and Desktops propose des modèles de licences utilisateur/appareil et de licences simultanées.

**Utilisateur/appareil :**

Le modèle utilisateur/appareil flexible s'aligne sur :

- l'utilisation des bureaux à l'échelle de l'entreprise,
- le système de licences de virtualisation des bureaux Microsoft sous-jacent,
- Licences simultanées pour les clients dont les utilisateurs n'ont besoin que d'un accès occasionnel à leurs bureaux et applications virtuels.

Le système de licences utilisateur/appareil permet aux utilisateurs d'accéder à leurs bureaux et applications virtuels à partir d'un nombre illimité d'appareils. Les licences d'appareils permettent à un

nombre illimité d'utilisateurs d'accéder à leurs bureaux et applications virtuels à partir d'un seul appareil. Cette approche vous offre une flexibilité maximale et se rapproche du système de licences de virtualisation des bureaux Microsoft.

> **Important :**
>
> Vous ne pouvez pas attribuer manuellement des licences à un utilisateur ou à un appareil. Le serveur de licences ou le service cloud attribue les licences. Avec le système de licences utilisateur/appareil, une fois qu'une licence est attribuée, elle ne peut être attribuée à un autre utilisateur qu'après 90 jours d'inactivité.

**Licences simultanées :**

Les licences simultanées permettent une connexion unique à un nombre illimité d'applications et de bureaux virtuels pour n'importe quel utilisateur et n'importe quel appareil. Une licence est consommée uniquement pendant une session active. Si la session se déconnecte ou est interrompue, la licence est réintégrée dans le pool.

Pour plus d'informations sur le système de licences utilisateur/appareil, voir Licences utilisateur ou associées à une machine et sur les licences simultanées, voir Licences simultanées.

### Est-il possible d'essayer Citrix Virtual Apps and Desktops avant d'acheter des licences ?

Oui. Vous pouvez télécharger le logiciel Citrix Virtual Apps and Desktops et l'exécuter en mode d'évaluation. Le mode d'évaluation vous permet d'utiliser Citrix Virtual Apps and Desktops sur site pendant 30 jours, avec 10 connexions, sans licence. Pour plus d'informations, consultez Licences d'évaluation.

Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) pour Citrix Cloud est disponible sous forme de service d'évaluation sur approbation. Consultez votre représentant Citrix pour plus de détails.

### Comment la simultanéité est-elle définie pour Citrix Virtual Apps and Desktops ?

Le modèle de licences simultanées de Citrix Virtual Apps and Desktops permet une connexion unique à un nombre illimité d'applications et de bureaux virtuels pour tout utilisateur et tout appareil. Une licence est consommée uniquement pendant une session active. Si la session se déconnecte ou est interrompue, la licence est réintégrée dans le pool. Pour plus d'informations, consultez Licence simultanée.

**Puis-je déployer plusieurs éditions de licences Citrix Virtual Apps and Desktops sur un serveur de licences commun ?**

Oui. Le serveur de licences gère simultanément les licences pour Citrix Virtual Apps and Desktops. Nous vous recommandons d'installer la dernière version du serveur de licences. Si vous souhaitez vérifier la version actuelle de votre serveur de licences, comparez-la au numéro que vous trouverez sur le site de téléchargements Citrix.

**Un site unique peut-il utiliser les licences Citrix Virtual Apps et Citrix Virtual Apps and Desktops ?**

Selon la version, un seul site Citrix Virtual Apps ou Citrix Virtual Apps and Desktops peut prendre en charge les deux modèles de licences - utilisateur/appareil ou simultanées. Un seul site Citrix Virtual Apps ou Citrix Virtual Apps and Desktops peut prendre en charge une seule édition. Pour plus d'informations, consultez la section Licences multitypes.

Les versions minimales qui prennent en charge les licences multi-types sont XenApp et XenDesktop 7.15 Long Term Service Release (LTSR) et Citrix Virtual Apps and Desktops 7 1808.

**Puis-je sélectionner le modèle simultané Citrix Virtual Apps en tant que modèle de produit si des licences utilisateur/appareil Citrix Virtual Apps and Desktops ou des licences simultanées Citrix Virtual Apps and Desktops sont installées sur le serveur de licences ?**

Si vous utilisez Citrix Virtual Apps en tant que fonctionnalité de Citrix Virtual Apps and Desktops Advanced ou Premium Edition, votre modèle de licences Citrix Virtual Apps est identique à celui de Citrix Virtual Apps and Desktops. Si vous avez acheté Citrix Virtual Apps and Desktops, configurez votre licence comme Citrix Virtual Apps and Desktops, même si vous prévoyez d'utiliser uniquement la fonctionnalité Citrix Virtual Apps. Sélectionnez Citrix Virtual Apps comme modèle de produit uniquement si vous disposez de licences autonomes simultanées Citrix Virtual Apps installées sur le serveur de licences.

**Quels composants de produit sont inclus avec chaque édition Citrix Virtual Apps et Citrix Virtual Apps and Desktops ?**

Pour obtenir une matrice complète des fonctionnalités par édition, consultez la section Fonctionnalités de Citrix Virtual Apps and Desktops.

**Comment puis-je appliquer des licences aux environnements Citrix Virtual Desktops en conformité avec le CLUF de Citrix Virtual Apps and Desktops ?**

Pour déployer Citrix Virtual Apps and Desktops dans un modèle de licences utilisateur/appareil ou simultanées conformément au CLUF de Citrix Virtual Apps and Desktops, appliquez les fichiers de licence à votre serveur de licences. Le serveur de licences contrôle et surveille ensuite la conformité des licences. Nous vous recommandons de configurer votre produit en fonction de ce que vous avez acheté. Par exemple, si vous achetez Citrix Virtual Apps and Desktops Premium mais que vous souhaitez uniquement utiliser la fonctionnalité Citrix Virtual Apps, configurez le produit sur Citrix Virtual Apps and Desktops afin de respecter la conformité. Pour plus d'informations, consultez le Centre de conformité des licences produit.

**Comment puis-je appliquer des licences aux environnements Citrix Virtual Apps en conformité avec le CLUF de Citrix Virtual Apps ?**

Pour déployer Citrix Virtual Apps dans un modèle de licences simultanées conformément au CLUF de Citrix Virtual Apps, appliquez les fichiers de licence à votre serveur de licences. Le serveur de licences contrôle et surveille ensuite la conformité des licences.

**Existe-t-il une condition de licence pour les options de maintenance Citrix Virtual Apps and Desktops : Long Term Service Release (LTSR) ou Current Release (CR) ?**

Les options de maintenance Citrix Virtual Apps and Desktops, telles que Long Term Service Release, sont un avantage du programme Customer Success Services. Vous devez disposer d'un compte Customer Success Services actif pour bénéficier des avantages de LTSR. Pour en savoir plus, voir Options de service Citrix Virtual Apps, Citrix Virtual Apps and Desktops et XenServer.

**Comment fonctionnent les heures groupées de Remote Browser Isolation (RBI) Service ?**

Lorsque vous achetez un minimum de 25 utilisateurs pour le service, vous recevez 5000 heures de droits d'utilisation du service, regroupées entre tous les utilisateurs. Les achats ultérieurs de droits d'utilisateur n'augmentent pas le nombre d'heures regroupées. Pour augmenter le nombre d'heures de service, achetez des packs complémentaires.

**Puis-je utiliser Remote PC Access avec des licences CCU ?**

Oui.

Pour de plus amples informations sur Remote PC Access, consultez la section Remote PC Access.

**Que se passe-t-il lorsque la maintenance logicielle de mon environnement Citrix expire ?**

Après une période de grâce de 30 jours, les utilisateurs reçoivent un message d'avertissement indiquant que Citrix Virtual Apps and Desktops n'est pas pris en charge après le lancement de la session.
Avertissement concernant Citrix Virtual Apps and Desktops :

```
Your corporate Citrix environment is currently unsupported. Please
contact your IT department to resolve any support related issues.
```

## Licences utilisateur ou appareil

**Comment les licences sont-elles attribuées aux utilisateurs dans le modèle de licences utilisateur/appareil ?**

Avec le modèle de licences utilisateur/périphérique, le serveur de licences attribue la licence à un ID utilisateur unique. Elle donne à cet utilisateur des connexions illimitées à partir d'appareils illimités. Si un utilisateur se connecte à un bureau ou à un appareil, il a besoin d'une licence pour accéder à un bureau virtuel ou à une application virtuelle. Le serveur de licences ou le service cloud attribue la licence. Vous ne pouvez pas attribuer ces licences manuellement. La licence est attribuée à l'utilisateur, et non à l'appareil partagé. Une fois qu'une licence est attribuée, elle ne peut être attribuée à un autre utilisateur qu'après 90 jours d'inactivité. Pour plus d'informations, consultez Licence utilisateur/appareil.

**Comment un appareil sous licence est-il défini dans le modèle de licences utilisateur/appareil ?**

Un appareil sous licence nécessite un ID d'appareil de point de terminaison unique. Dans le modèle utilisateur/appareil, un appareil est tout équipement dont vous avez autorisé l'utilisation par toute personne pour accéder aux instances de Citrix Virtual Apps and Desktops. Pour un appareil partagé, une seule licence utilisateur/appareil Citrix Virtual Apps and Desktops peut prendre en charge plusieurs utilisateurs qui partagent l'appareil. Par exemple, un appareil partagé peut être un poste de travail en salle de classe ou un poste de travail clinique dans un hôpital.

**Puis-je convertir mes licences simultanées Citrix Virtual Desktops Standard Edition en modèle utilisateur/appareil ?**

Vous ne pouvez pas convertir les licences simultanées Citrix Virtual Desktops Standard Edition en licences utilisateur/appareil Citrix Virtual Desktops Standard Edition. De même, vous ne pouvez pas convertir les licences utilisateur/appareil Citrix Virtual Desktops Standard Edition en licences simultanées Citrix Virtual Desktops Standard Edition.

Si vous disposez de licences simultanées Citrix Virtual Desktops Standard Edition et que vous souhaitez utiliser le modèle de licences utilisateur/appareil, effectuez une mise à niveau vers Citrix Virtual Apps and Desktops Advanced ou Premium Edition.

| À partir de | Vers des licences simultanées Standard | Vers des licences utilisateur/appareil Standard | Vers des licences utilisateur/appareil Advanced | Vers des licences utilisateur/appareil Premium |
|---|---|---|---|---|
| Licences simultanées Citrix Virtual Desktops Standard Edition | S/O | Conversion licences simultanées vers licences utilisateur/appareil NON autorisée | Vous ne pouvez pas convertir les modèles de licence, mais vous pouvez effectuer une mise à niveau vers Citrix Virtual Apps and Desktops Advanced ou Premium Edition. | Vous ne pouvez pas convertir les modèles de licence, mais vous pouvez effectuer une mise à niveau vers Citrix Virtual Apps and Desktops Advanced ou Premium Edition. |
| Licences utilisateur/appareil Citrix Virtual Desktops Standard Edition | Conversion licences utilisateur/appareil vers licences simultanées NON autorisée | S/O | S/O | S/O |

**En quoi les licences simultanées fonctionnent-elles différemment des licences utilisateur/appareil ?**

Nous basons les licences simultanées sur des connexions d'appareil simultanées. Une licence simultanée n'est utilisée que lorsqu'un appareil a établi une connexion active. Une fois la connexion terminée, la licence simultanée revient au pool de licences pour une utilisation immédiate. Nous recommandons ce modèle de licences pour une utilisation occasionnelle. Les licences utilisateur/appareil sont louées pour une période donnée et ne sont pas disponibles pour les autres utilisateurs avant l'expiration du bail.

**Dans le cadre du modèle utilisateur/appareil, pouvons-nous attribuer des licences à la fois aux utilisateurs et aux appareil de la même entreprise ?**

Oui. Les deux types peuvent être présents dans la même entreprise. Le serveur de licences attribue de manière optimale les licences aux utilisateurs ou aux appareil en fonction de leur utilisation. Vous ne pouvez pas attribuer ces licences manuellement.

**Comment déterminer le nombre d'utilisateurs ou d'appareils auxquels attribuer une licence ?**

Évaluez les exigences relatives au cas d'utilisation afin de déterminer le nombre approprié de licences. Le système de licences utilisateur/appareil donne un accès illimité à un nombre illimité de bureaux et d'applications virtuels à partir d'un nombre illimité d'appareils. Les licences simultanées permettent un accès illimité à des bureaux virtuels et à des applications virtuelles illimités à partir d'un seul appareil qu'un nombre illimité d'utilisateurs peut utiliser. Observez la formule suivante :

```
(Number of total users) – (number of users that only access
   exclusively
 with shared devices) + (number shared devices) = total number
 of licenses to buy.

For example, there are 1000 total users at the hospital. If 700 of them
    access only
Citrix Virtual Desktops from 300 shared devices in the hospital, the
   number of
licenses to purchase is 1000 – 700 + 300 = 600 licenses.
<!--NeedCopy-->
```

**Dans le modèle utilisateur/appareil, quel est le nombre maximal d'appareils qu'un utilisateur avec licence peut utiliser pour se connecter à mon environnement ?**

Chaque utilisateur avec licence a le droit d'utiliser un nombre illimité d'appareils connectés ou hors ligne.

**Dans le modèle utilisateur/appareil, quel est le nombre maximal d'utilisateurs qui peuvent accéder à un appareil avec licence ?**

Chaque appareil avec licence peut desservir un nombre illimité d'utilisateurs au sein d'une organisation.

**Sous le modèle utilisateur/appareil, quel est le nombre maximal de bureaux virtuels ou d'applications Web pooled hours qu'un utilisateur avec licence peut consommer à tout moment ?**

Chaque utilisateur avec licence peut se connecter à un nombre illimité de bureaux virtuels ou d'applications Web.

**Puis-je acheter des licences Citrix Virtual Apps and Desktops pour augmenter le nombre d'utilisateurs/appareils avec licence dans mon environnement Citrix Virtual Apps and Desktops existant ?**

Oui. Vous pouvez acheter des licences Citrix Virtual Apps and Desktops pour augmenter le nombre d'utilisateurs/appareils avec licence dans votre environnement Citrix Virtual Apps and Desktops existant.

**Comment puis-je libérer une licence utilisateur/appareil autorisé(e) ?**

Pour libérer l'attribution d'un utilisateur/appareil autorisé, utilisez l'utilitaire `udadmin` conformément aux termes du CLUF. Le serveur de licences attribue ensuite la licence à l'utilisateur ou à l'appareil approprié suivant. Pour plus d'informations, consultez Afficher ou libérer des licences pour des utilisateurs ou des machines.

**Que se passe-t-il si je dépasse le nombre de licences utilisateur/appareil achetées ?**

Les licences utilisateur/appareil comprennent un découvert de 10 %, qui est inclus lorsque les licences sont générées. Le découvert est également inclus dans le nombre de licences installées. Si le pic d'utilisation dépasse le nombre de licences installés, y compris le découvert, l'accès à un plus grand nombre d'utilisateurs est refusé. Achetez et déployez une nouvelle licence pour permettre l'accès à un plus grand nombre d'utilisateurs.

Si toutes les licences sont en cours d'utilisation, y compris le découvert de licences, la période de grâce supplémentaire permet des connexions illimitées à un produit. La période de grâce supplémentaire vous offre la possibilité de déterminer pourquoi vous avez dépassé le nombre maximal de licences et d'acheter plus de licences sans perturber vos utilisateurs. Cette période dure pendant 15 jours, ou jusqu'à ce que vous installiez des licences de détail supplémentaires, selon la première occurrence. Pour plus d'informations, consultez Période de grâce supplémentaire.

Director affiche les états de période de grâce. Pour plus d'informations, consultez Panneaux sur le tableau de bord Director.

**Quel est le nombre maximal d'applications virtuelles qu'un utilisateur avec licence peut consommer à tout moment ?**

Chaque utilisateur avec licence peut se connecter à un nombre illimité d'applications virtuelles.

**Que se passe-t-il si un utilisateur avec licence quitte mon organisation ?**

Lorsqu'un utilisateur avec licence quitte votre organisation, vous pouvez libérer la licence de l'utilisateur sortant sans en informer Citrix. Utilisez l'utilitaire `udadmin` pour libérer la licence. Si vous ne libérez pas la licence, le serveur de licences libère automatiquement toute licence après 90 jours d'inactivité. Ces informations sont soumises aux conditions spécifiées dans le CLUF.

**Que se passe-t-il si un utilisateur avec licence est absent pendant une période prolongée ?**

Si un utilisateur avec licence est absent pendant une période prolongée, vous pouvez libérer la licence sans en informer Citrix, afin qu'elle puisse être réaffectée. Utilisez l'utilitaire `udadmin` pour libérer la licence.

**Que se passe-t-il si nous remplaçons un appareil avec licence dans mon organisation ?**

Si vous remplacez un appareil avec licence, vous pouvez libérer la licence sans en informer Citrix, afin qu'elle puisse être réaffectée. Utilisez l'utilitaire `udadmin` pour libérer la licence.

**Que se passe-t-il si un appareil avec licence est hors service pendant une période prolongée ?**

Si un appareil avec licence est hors service pendant une période prolongée, vous pouvez libérer la licence sans en informer Citrix, afin qu'elle puisse être réaffectée. Utilisez l'utilitaire `udadmin` pour libérer les licences. Si vous ne libérez pas la licence, le serveur de licences libère automatiquement toute licence après 90 jours d'inactivité. Ces informations sont soumises aux conditions spécifiées dans le CLUF.

**Puis-je changer des licences utilisateur en licences appareil et inversement une fois que j'ai attribué les licences à un appareil ou un utilisateur ?**

Oui. Ce changement se produit automatiquement. Le serveur de licences attribue des licences aux utilisateurs ou aux appareils en fonction des modèles d'utilisation. Si les modèles d'utilisation changent, le serveur de licences peut changer l'attribution en fonction de la nouvelle utilisation. Le serveur de licences attribue toujours les licences de la manière la plus économique pour le client. En

outre, le serveur de licences surveille les licences pour identifier les licences **inutilisées** après leur période d'attribution de 90 jours. Vous pouvez réaffecter des licences identifiées comme inutilisées après la période d'attribution de 90 jours à d'autres utilisateurs ou appareils.

## Licences simultanées

### Sous le modèle de licences simultanées, quel est le nombre maximal de bureaux virtuels qu'un utilisateur avec licence Citrix Virtual Apps and Desktops peut consommer à tout moment ?

Un point de terminaison peut servir de nombreux utilisateurs et permet des connexions illimitées.

### Puis-je déployer des licences simultanées à partir d'une version précédente de Citrix Virtual Apps and Desktops et de nouvelles licences utilisateur/appareil ou simultanées sur un seul serveur de licences ?

Oui. Vous pouvez continuer à utiliser le même serveur de licences pour prendre en charge les déploiements sous licence utilisateur/appareil ou simultanés.

### Puis-je déployer des licences simultanées et des licences utilisateur/appareil ou simultanées sur un seul serveur de licences ?

Oui. Vous pouvez continuer à utiliser le même serveur de licences pour prendre en charge les déploiements sous licence simultanés et utilisateurs/appareil ou simultanés.

### Les éditions Citrix Virtual Apps and Desktops Advanced et Premium incluent-elles des licences simultanées Citrix Virtual Apps ?

Les licences utilisateur/appareil Citrix Virtual Apps and Desktops Advanced et Premium incluent des licences Citrix Virtual Apps simultanées à des fins de compatibilité uniquement. Ces licences simultanées ne sont utilisées qu'avec des versions antérieures de produits incompatibles avec les licences utilisateur/appareil. L'utilisation des licences de compatibilité simultanées incluses avec les licences utilisateur/appareil n'est autorisée qu'avec ces versions : les versions XenApp antérieures à 6.5 et les versions XenDesktop antérieures à 5.0 Service Pack 1.

### Que se passe-t-il si je dépasse le nombre de licences simultanées achetées ?

Si toutes les licences sont en cours d'utilisation, la période de grâce supplémentaire permet des connexions illimitées à un produit. La période de grâce supplémentaire vous offre la possibilité de déterminer pourquoi vous avez dépassé le nombre maximal de licences et d'acheter plus de licences sans

perturber vos utilisateurs. Cette période dure pendant 15 jours, ou jusqu'à ce que vous installiez des licences de détail supplémentaires, selon la première occurrence. Pour plus d'informations, consultez Période de grâce supplémentaire.

Director affiche les états de période de grâce. Pour plus d'informations, consultez Panneaux sur le tableau de bord Director.

## Découvert de licences

### Comment puis-je obtenir des découverts de licences ?

Les produits (à l'exception de Citrix Cloud) qui prennent en charge les modèles de licence utilisateur/appareil, utilisateur ou appareil incluent une fonctionnalité de découvert de licences qui vous permet d'utiliser un nombre limité de licences supplémentaires afin d'empêcher les refus d'accès. Nous offrons la fonction de découvert à titre de commodité, mais elle ne constitue pas un droit de licence. Les licences simultanées et les licences serveur ne contiennent pas de découvert. Toute licence de découvert utilisée doit être achetée dans les 30 jours suivant la première utilisation, mais l'utilisation n'est pas limitée à 30 jours. Citrix se réserve le droit de supprimer toute fonctionnalité de découvert dans les nouvelles versions de produits. Pour de plus amples informations, consultez la section Découvert de licences.

### Comment puis-je identifier un découvert de licences ?

Vous pouvez afficher les informations d'utilisation, notamment le nombre de licences dans le découvert, dans Citrix Licensing Manager. Studio contient également des informations sur l'utilisation du découvert.

### Que se passe-t-il lorsqu'un découvert est consommé ?

Une licence est attribuée à partir de vos licences installées pour activer l'accès à votre environnement Citrix Virtual Apps and Desktops. Ce découvert offre autant d'accès et de fonctionnalités que vos autres licences.

### Puis-je recevoir une alerte lorsque mes découverts de licences sont consommés ?

À l'heure actuelle, aucune alerte spécifique n'est fournie lorsque les découverts de licences sont consommés.

**Pendant combien de temps un découvert de licence peut-il être consommé ?**

Achetez tous les découverts de licences utilisés dans les 30 jours suivant la première utilisation.

### Autres informations sur les licences spécifiques aux produits

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- XenServer
- Système de licences Citrix

## Équilibrer la charge des machines

June 27, 2024

> **Remarque :**
>
> Cette fonctionnalité s'applique à tous vos catalogues, qu'il s'agisse de catalogues OS mono-session ou OS multi-sessions. L'équilibrage de charge vertical s'applique uniquement aux machines avec OS multi-sessions.

L'équilibrage de charge peut être configuré au niveau du site et au niveau du groupe de mise à disposition. Vous avez deux options : verticale et horizontale. Par défaut, l'équilibrage de charge horizontal est activé.

### Paramètres d'équilibrage de charge au niveau du site

- **Équilibrage de charge vertical**. Affecte la session utilisateur entrante à la machine la plus chargée qui n'a pas encore atteint la charge maximale. Ce processus sature les machines existantes avant de passer à de nouvelles machines. La déconnexion des utilisateurs des machines existantes libère de la capacité sur ces machines. Les charges entrantes sont alors affectées à ces machines. L'équilibrage de charge vertical affecte l'expérience utilisateur mais réduit les coûts (les sessions maximisent la capacité des machines sous tension).

  Exemple : Deux machines sont configurées pour 10 sessions chacune. La première machine gère les 10 premières sessions simultanées. La deuxième machine s'occupe de la onzième session.

> **Conseil :**
>
> Pour spécifier le nombre maximal de sessions qu'une machine peut héberger, utilisez le paramètre de stratégie Nombre maximum de sessions.

Vous pouvez également utiliser PowerShell pour activer ou désactiver l'équilibrage de charge vertical à l'échelle du site. Utilisez le paramètre `UseVerticalScalingForRdsLaunches` de l'applet de commande `Set-BrokerSite`. Utilisez `Get-BrokerSite` pour afficher la valeur du paramètre `UseVerticalScalingForRdsLaunches`. Consultez l'aide de l'applet de commande pour plus de détails.

- **Équilibrage de charge horizontal**. Attribue une session utilisateur entrante à la machine sous tension la moins chargée disponible. L'équilibrage de charge horizontal améliore l'expérience utilisateur mais augmente les coûts (car davantage de machines sont maintenues sous tension). Par défaut, l'équilibrage de charge horizontal est activé.

  Exemple : Deux machines sont configurées pour 10 sessions chacune. La première machine gère cinq sessions simultanées. La deuxième machine en gère également cinq.

Pour configurer cette fonctionnalité, dans **Gérer > Configuration complète**, sélectionnez **Paramètres** dans le volet gauche. Sélectionnez une option sous **Catalogues multi-sessions d'équilibrage de charge**.

### Paramètres d'équilibrage de charge au niveau du groupe de mise à disposition

La configuration de l'équilibrage de charge au niveau du groupe de mise à disposition vous permet de remplacer les paramètres d'équilibrage de charge hérités au niveau du site. Vous pouvez obtenir une utilisation maximale pour chaque machine lorsque vous sélectionnez l'équilibrage de charge vertical au niveau du groupe de mise à disposition. Cela permettra de réduire les coûts dans les clouds publics. Cette configuration peut être effectuée lors de la création d'un nouveau groupe de mise à disposition ou de la modification d'un groupe de mise à disposition existant.

**Équilibrage de charge horizontal**. Les sessions sont réparties entre les machines sous tension. Par exemple, si vous avez deux machines configurées pour 10 sessions chacune, la première gère cinq sessions simultanées et la seconde en gère également cinq.

**Équilibrage de charge vertical**. Les sessions optimisent la capacité des machines sous tension et réduisent les coûts des machines. Par exemple, si vous avez deux machines configurées pour 10 sessions chacune, la première machine gère les 10 premières sessions simultanées. La deuxième machine s'occupe de la onzième session.

# Cache d'hôte local

June 27, 2024

Pour vous assurer que la base de données du site Citrix Virtual Apps and Desktops est toujours disponible, Citrix recommande de commencer par un déploiement SQL Server ayant une tolérance aux pannes en suivant la haute disponibilité des meilleures pratiques de Microsoft. (La section Bases de données répertorie les fonctionnalités de haute disponibilité de SQL Server prises en charge). Toutefois, les utilisateurs peuvent ne pas être en mesure de se connecter à leurs applications ou bureaux à cause de problèmes et d'interruptions réseau.

La fonctionnalité Cache d'hôte local permet aux opérations de négociation de connexions sur un site de se poursuivre en cas de panne. Une panne se produit lorsque la connexion entre un Delivery Controller et la base de données du site échoue dans un environnement Citrix local. Le cache de l'hôte local est activé lorsque la base de données du site est inaccessible pendant 90 secondes.

À partir de XenApp et XenDesktop version 7.16, la fonction de location de connexion (fonctionnalité de haute disponibilité dans les versions antérieures) a été supprimée du produit et n'est plus disponible.

## Contenu des données

Le cache d'hôte local inclut les informations suivantes, qui constituent un sous-ensemble des informations de la base de données principale :

- Identités des utilisateurs et des groupes auxquels sont attribués des droits sur les ressources publiées à partir du site.
- Identités des utilisateurs qui utilisent actuellement ou ont récemment utilisé des ressources publiées à partir du site.
- Identités des machines VDA (y compris les machines Remote PC Access) configurées sur le site.
- Identités (noms et adresses IP) des machines Citrix Receiver utilisées activement pour se connecter aux ressources publiées.

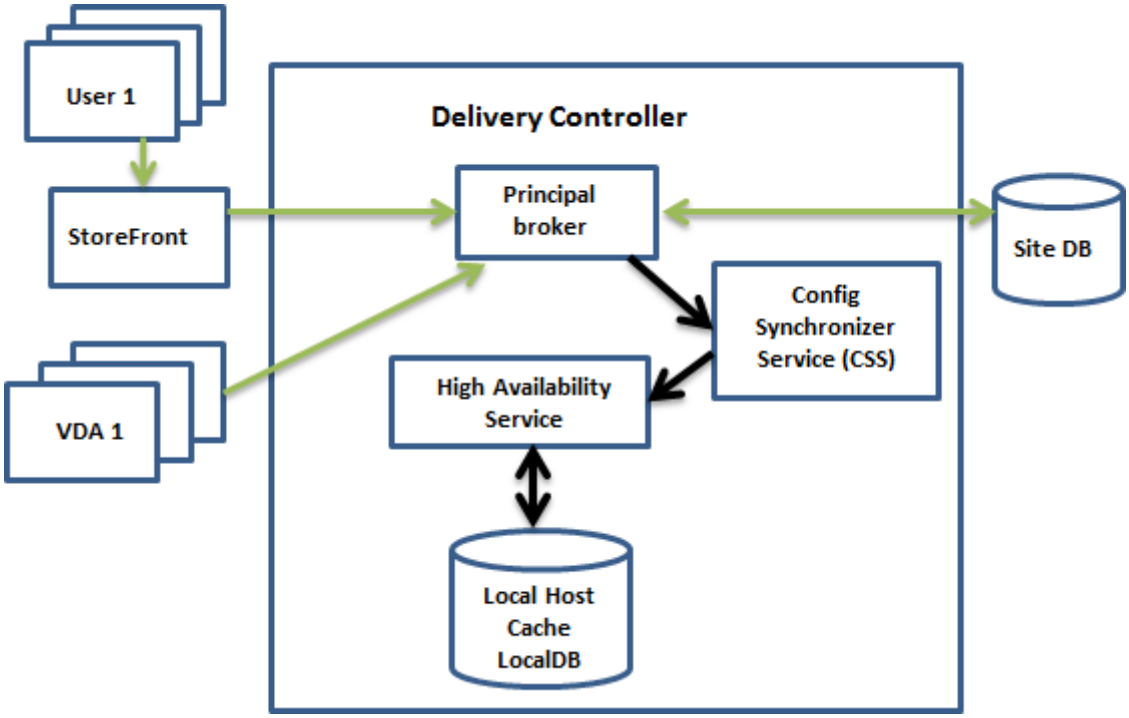
Il contient également des informations sur les connexions actuellement actives qui ont été établies alors que la base de données principale était indisponible :

- Résultats de toute analyse de point de terminaison de machine client réalisée par Citrix Receiver.
- Identités des machines d'infrastructure (telles que les serveurs NetScaler Gateway et StoreFront) impliquées dans le site.
- Dates/heures et types d'activités récentes des utilisateurs.

### Fonctionnement

Le graphique suivant illustre les composants et les chemins de communication du cache d'hôte local en fonctionnement normal.




#### En mode de fonctionnement normal

- Le *broker principal* (Citrix Broker Service) sur un Controller accepte les demandes de connexion provenant de StoreFront. Le broker communique avec la base de données du site pour connecter les utilisateurs aux VDA qui sont enregistrés auprès du Controller.
- Citrix Config Synchronizer Service (CSS) interroge le broker environ toutes les 5 minutes pour savoir si des modifications ont été apportées. Ces modifications peuvent avoir été initiées par un administrateur (telles que la modification d'une propriété de groupe de mise à disposition) ou être des actions du système (telles que les attributions de machine).
- Si la configuration a été modifiée depuis la dernière vérification, le service CSS synchronise (copie) les informations sur un broker secondaire sur le Controller. (le broker secondaire est également connu sous le nom de service de haute disponibilité.)

  Toutes les données de configuration sont copiées, et pas seulement les éléments qui ont été modifiés depuis la dernière vérification. Le CSS importe les données de configuration dans une base de données Microsoft SQL Server Express LocalDB sur le Controller. Cette base de données est appelée base de données du cache d'hôte local. Le service CSS s'assure que les informations de la base de données du cache d'hôte local du broker secondaire correspondent

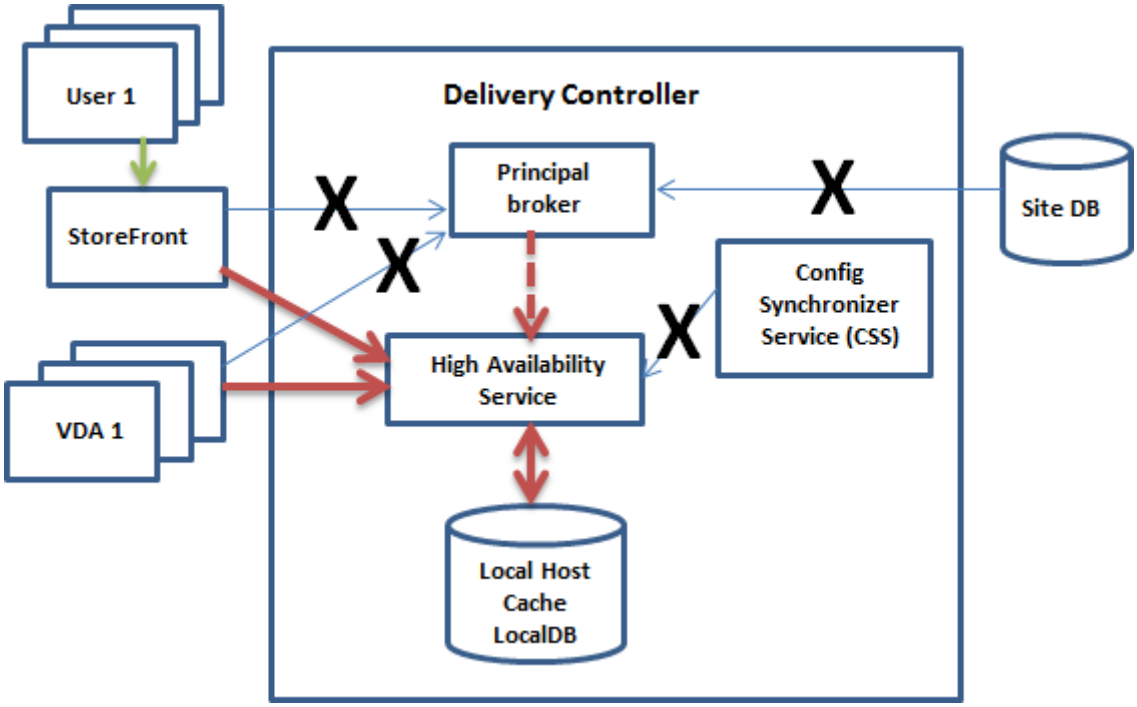
 

aux informations de la base de données du site. La base de données du cache d'hôte local est recréée chaque fois que la synchronisation se produit.

Microsoft SQL Server Express LocalDB (utilisé par la base de données du cache d'hôte local) est installé automatiquement lorsque vous installez un Controller (vous pouvez interdire cette installation lors de l'installation d'un Controller à partir de la ligne de commande.). La base de données du cache de l'hôte local ne peut pas être partagée entre les Controller. Vous n'avez pas besoin de sauvegarder la base de données du cache d'hôte local. Elle est recréée chaque fois qu'une modification de la configuration est détectée.

- Si aucune modification n'a été apportée depuis la dernière vérification, aucune donnée n'est copiée.

Le graphique suivant illustre les modifications apportées aux chemins de communication si le broker principal perd le contact avec la base de données du site (une panne commence).




**Durant une panne**

Lorsqu'une panne commence :

- Le broker secondaire démarre l'écoute et traite les demandes de connexion.
- Lorsque la panne commence, le broker secondaire ne dispose pas des données d'enregistrement de VDA, mais lorsqu'un VDA communique avec lui, un processus d'enregistrement est déclenché. Au cours de ce processus, le broker secondaire obtient également des informations de session sur ce VDA.

- Bien que le broker secondaire gère les connexions, le broker principal continue à surveiller la connexion. Lorsque la connexion est rétablie, le broker principal demande au broker secondaire d'arrêter l'écoute des informations de connexion, et le broker principal reprend les opérations de négociation de connexion. La prochaine fois qu'un VDA communique avec le broker principal, un processus d'enregistrement est déclenché. Le broker secondaire supprime les enregistrements de VDA restants de la panne précédente. Le service CSS reprend la synchronisation des informations lorsqu'il détecte des modifications de la configuration dans le déploiement.

Dans le cas peu probable où une panne démarre pendant une synchronisation, l'importation en cours est annulée et la dernière configuration connue est utilisée.

Le journal d'événements contient des informations sur les synchronisations et les pannes.

Aucun délai n'est imposé pour le fonctionnement en mode panne.

La transition entre le mode normal et le mode panne n'affecte pas les sessions existantes. Elle n'affecte que le lancement de nouvelles sessions.

Vous pouvez également déclencher intentionnellement une panne. Voir Forcer une panne pour savoir quand cela peut être nécessaire et comment procéder.

#### Sites disposant de plusieurs Controller

Parmi ses différentes tâches, le service CSS fournit régulièrement au broker secondaire des informations sur tous les Controller de la zone (si votre déploiement ne contient pas plusieurs zones, cette action affecte tous les Controller du site). Ces informations permettent à chaque broker secondaire de connaître tous les brokers secondaires homologues exécutés sur d'autres Controller de la zone.

Les brokers secondaires communiquent entre eux sur un canal distinct. Ces brokers utilisent une liste alphabétique des noms de domaine complet (FQDN) des machines qu'ils exécutent pour déterminer (sélectionner) le broker secondaire qui sera en charge des opérations de négociation dans la zone si une panne se produit. Durant la panne, tous les VDA s'enregistrent auprès du broker secondaire sélectionné. Les brokers secondaires non sélectionnés dans la zone rejettent activement les requêtes de connexion et d'enregistrement de VDA entrantes.

Si un broker secondaire sélectionné échoue lors d'une panne, un autre broker secondaire est sélectionné pour prendre le relais et les VDA s'enregistrent auprès du broker secondaire qui vient d'être sélectionné.

Durant une panne, si un Controller est redémarré :

- Si ce Controller n'est pas le broker sélectionné, le redémarrage n'a aucun impact.
- Si ce Controller est le broker sélectionné, un autre Controller est sélectionné, et par conséquent le VDA s'enregistre. Une fois que le Controller redémarré est sous tension, il reprend automa-

tiquement la négociation des connexions, et le VDA s'enregistre. Dans ce scénario, les performances peuvent être affectées lors des enregistrements.

Si vous mettez un Controller hors tension en fonctionnement normal et le remettez sous tension durant une panne, le cache d'hôte local ne peut pas être utilisé sur ce Controller s'il est sélectionné en tant que broker.

Le journal d'événements contient des informations sur les sélections.

### Fonctionnalités indisponibles durant une panne et autres différences

Aucun délai n'est imposé pour le fonctionnement en mode panne. Toutefois, Citrix recommande de restaurer la connectivité le plus rapidement possible.

Durant une panne :

- Vous ne pouvez pas utiliser Studio.
- Vous avez un accès limité au SDK PowerShell.
  - Vous devez d'abord :
    * Ajouter une clé de Registre `EnableCssTestMode` avec une valeur de 1 : `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    * Utiliser le port 89 : `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
  - Après avoir exécuté ces commandes, vous pouvez accéder à :
    * Toutes les applets de commande `Get-Broker*`.
- Les informations d'identification de l'hyperviseur ne peuvent pas être obtenues depuis Host Service. Toutes les machines se trouvent dans un état d'alimentation inconnu et aucune opération d'alimentation ne peut être émise. Toutefois, les machine virtuelle de l'hôte qui sont sous tension peuvent être utilisées pour les demandes de connexion.
- Une machine attribuée peut uniquement être utilisée si l'attribution s'est produite lors d'un fonctionnement normal. De nouvelles attributions ne peuvent pas être effectuées lors d'une panne.
- L'inscription et la configuration automatiques de machines Remote PC Access ne sont pas possibles. Toutefois, les machines qui ont été inscrites et configurées lors du fonctionnement normal peuvent être utilisées.

- Les utilisateurs d'applications et de bureaux hébergés sur le serveur peuvent utiliser plus de sessions que leurs limites de session configurées, si les ressources se trouvent dans des zones différentes.
- Les utilisateurs peuvent lancer des applications et bureaux uniquement à partir de VDA enregistrés dans la zone contenant le broker secondaire actuellement actif/sélectionné. Les lancements entre zones (depuis un broker secondaire dans une zone vers un VDA situé dans une autre zone) ne sont pas pris en charge durant une panne.
- Si une panne de base de données de site se produit avant le début d'un redémarrage programmé pour les VDA d'un groupe de mise à disposition, les redémarrages commencent à la fin de la panne. Cela peut donner des résultats inattendus. Pour plus d'informations, voir Redémarrages programmés retardés en raison d'une panne de la basede données.
- La préférence de zone ne peut pas être configurée. Si elle est configurée, les préférences ne sont pas prises en compte pour le lancement de la session.
- Les restrictions de balises dans lesquelles des balises sont utilisées pour désigner des zones ne sont pas prises en charge pour les lancements de session. Lorsque de telles restrictions de balises sont configurées et que l'option Contrôle avancé de l'état d'un magasin StoreFront est activée, le lancement des sessions peut échouer par intermittence.

### Prise en charge des applications et des bureaux

Le cache d'hôte local prend en charge les applications et les bureaux hébergés sur le serveur, et les bureaux statiques (attribués).

Le cache hôte local prend en charge les VDA de bureau dans les groupes de mise à disposition groupés, comme suit :

- Par défaut, les VDA de bureau à alimentation gérée appartenant à des groupes de mise à disposition regroupés en pool (créés par MCS ou Citrix Provisioning) dont la propriété `ShutdownDesktopsAfterUse` est activée ne sont pas disponibles pour les nouvelles connexions lors d'un événement Cache d'hôte local. Vous pouvez modifier cette valeur par défaut pour autoriser l'utilisation de ces bureaux pendant le cache d'hôte local.

  Toutefois, vous ne pouvez pas compter sur la gestion de l'alimentation durant la panne. (La gestion de l'alimentation reprend une fois que les opérations normales reprennent.) En outre, ces bureaux peuvent contenir des données de l'utilisateur précédent, car ils n'ont pas été redémarrés.
- Pour modifier le comportement par défaut, vous devez l'activer au niveau du site et pour chaque groupe de mise à disposition affecté. Exécutez les applets de commande PowerShell suivants.

À l'échelle du site :

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
```

Pour chaque groupe de mise à disposition affecté, exécutez la commande PowerShell suivante :

```
Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
 $true
```

Pour activer le paramètre de groupe de mise à disposition par défaut, exécutez la commande PowerShell suivante :

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

Ce paramètre s'applique à tous les nouveaux groupes de mise à disposition créés après son activation.

Pour activer ce paramètre pour les groupes de mise à disposition existants, exécutez la commande PowerShell suivante :

```
Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
 $true
```

L'activation de cette fonctionnalité dans le site et les groupes de mise à disposition n'affecte pas le fonctionnement de la propriété `ShutdownDesktopsAfterUse` configurée en fonctionnement normal. Lorsque cette fonctionnalité est activée, les VDA ne redémarrent pas automatiquement une fois l'événement LHC terminé. Les VDA de bureau à alimentation gérée et appartenant à des groupes de mise à disposition mis en pool peuvent conserver les données des sessions précédentes jusqu'au redémarrage du VDA. Cela peut se produire lorsqu'un utilisateur ferme sa session du VDA pendant des opérations autres que LHC ou que le redémarrage peut être déclenché manuellement.

> **Important :**
>
> Si ReuseMachinesWithoutShutdownInOutageAllowed au niveau du site et ReuseMachinesWithoutShutdownInOutage au niveau du groupe de mise à disposition ne sont pas activés, toutes les tentatives de lancement de session vers les VDA de bureau dont l'alimentation est gérée dans des groupes de mise à disposition regroupés échoueront lors d'un événement Cache hôte local.

#### Considérations sur la taille de la RAM

Le service LocalDB peut utiliser environ 1,2 Go de RAM (jusqu'à 1 Go pour le cache de base de données, plus 200 Mo pour l'exécution de SQL Server Express LocalDB). Le broker secondaire peut utiliser jusqu'à 1 Go de RAM si une panne dure longtemps avec un grand nombre d'ouvertures de session (par exemple, 12 heures avec 10 000 utilisateurs). Ces exigences de mémoire s'ajoutent aux exigences de RAM requises normalement pour le Controller, il se peut donc que vous deviez augmenter la quantité totale de capacité RAM.

Si vous utilisez une installation SQL Server Express pour la base de données du site, le serveur aura deux processus sqlserver.exe.

#### Considérations sur la configuration des sockets et des cœurs d'UC

Une configuration d'UC de Controller, notamment le nombre de cœurs disponibles pour SQL Server Express LocalDB, affecte directement les performances de cache d'hôte local, encore plus que l'allocation de mémoire. Cette charge de l'UC est observée uniquement au cours de la période de panne lorsque la base de données ne peut pas être contactée et que le service de broker secondaire est actif.

Bien que la base de données LocalDB puisse utiliser plusieurs cœurs (jusqu'à 4), elle est limitée à un seul socket. L'ajout de sockets ne permet pas d'améliorer les performances (par exemple, 4 sockets avec 1 cœur chacun). Citrix vous recommande plutôt d'utiliser plusieurs sockets avec plusieurs cœurs. Au cours des tests Citrix, une configuration 2x3 (2 sockets, 3 cœurs) a fourni de meilleures performances que les configurations 4x1 et 6x1.

#### Considérations sur le stockage

Lorsque les utilisateurs accèdent à des ressources pendant une panne, la taille de la base de données LocalDB augmente. Par exemple, lors d'un test d'ouverture/fermeture de session avec 10 ouvertures de session par seconde, la base de données a augmenté d'1 Mo toutes les 2-3 minutes. Lorsque le fonctionnement normal reprend, la base de données locale est recréée et l'espace disque est rétabli. Toutefois, le disque sur lequel la base de données LocalDB est installée doit avoir suffisamment d'espace pour permettre à la taille de la base de données d'augmenter durant une panne. Le cache d'hôte local entraîne également des E/S supplémentaires pendant une panne : environ 3 Mo d'écritures par seconde, avec plusieurs centaines de milliers de lectures.

#### Considérations sur les performances

Durant une panne, un seul broker secondaire gère toutes les connexions ; dans les sites (ou zones) qui équilibrent la charge entre plusieurs Controller en fonctionnement normal, le broker secondaire sélectionné peut être amené à prendre en charge beaucoup plus de requêtes que d'habitude durant une panne. Par conséquent, les demandes d'UC seront plus nombreuses. Chaque broker secondaire du site (zone) doit être en mesure de gérer la charge supplémentaire imposée par la base de données du cache hôte local et tous les VDA concernés, car le broker secondaire sélectionné lors d'une panne peut changer.

Limites de VDI :

- Dans un déploiement VDI à zone unique, jusqu'à 10 000 VDA peuvent être gérés efficacement au cours d'une panne.
- Dans un déploiement VDI multizone, jusqu'à 10 000 VDA par zone peuvent être gérés au cours d'une panne, avec un maximum de 40 000 VDA sur le site. Par exemple, chacun des sites suivants peut être géré de manière efficace durant une panne :
  - Un site avec quatre zones, chacune contenant 10 000 VDA.
  - Un site avec sept zones, une contenant 10 000 VDA et six contenant 5 000 VDA chacune.

Durant une panne, la gestion de la charge pour l'ensemble du site peut être affectée. Les calculateurs de charge (et plus particulièrement les règles du nombre de sessions) peuvent être dépassés.

Pendant que tous les VDA s'enregistrent avec un broker secondaire, il est possible que ce service ne dispose pas d'informations complètes sur les sessions en cours. Par conséquent, une demande de connexion d'un utilisateur pendant cet intervalle peut entraîner le démarrage d'une nouvelle session, même si la reconnexion à une session existante est possible. Cet intervalle (pendant lequel le nouveau broker secondaire reçoit les informations de session depuis tous les VDA dans le cadre du ré-enregistrement) est inévitable. Les sessions qui sont connectées lorsqu'une panne démarre ne sont pas affectées lors de l'intervalle de transition, mais les nouvelles sessions et les reconnexions de session peuvent l'être.

Cet intervalle se produit lorsque les VDA doivent s'enregistrer :

- Une panne démarre : lors de la migration depuis un broker principal vers un broker secondaire.
- Défaillance du broker secondaire durant une panne : lors de la migration depuis un broker secondaire qui a échoué vers un nouveau broker secondaire.
- Reprise après une panne : lorsque les opérations normales reprennent, et que le broker principal reprend le contrôle.

Vous pouvez réduire cet intervalle en réduisant la valeur de registre `HeartbeatPeriodMs` de Citrix Broker Protocol (valeur par défaut=600000 ms, c'est-à-dire 10 minutes). Cette valeur de pulsation est le double de l'intervalle que le VDA utilise pour les pings, donc la valeur par défaut entraîne un ping toutes les 5 minutes.

Par exemple, la commande suivante règle la pulsation sur cinq minutes (300000 millisecondes), ce qui entraîne un ping toutes les 2,5 minutes :

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
HeartbeatPeriodMs -PropertyType DWORD –Value 300000
```

Soyez prudent lorsque vous modifiez la valeur de pulsation. L'augmentation de la fréquence entraîne une plus grande charge sur les Controllers pendant le mode normal et le mode panne.

L'intervalle ne peut pas être entièrement éliminé, quelle que soit la rapidité avec laquelle les VDA s'enregistrent.

Le temps nécessaire à la synchronisation entre les brokers secondaires augmente avec le nombre d'objets (VDA, applications, groupes) Par exemple, la synchronisation de 5 000 VDA peut prendre plus de dix minutes.

#### Différences par rapport aux versions XenApp 6.x

Bien que cette implémentation du cache d'hôte local porte le même nom que la fonctionnalité de cache d'hôte local dans XenApp 6.x et les versions antérieures de XenApp, d'importantes améliorations y ont été apportées. Cette implémentation est plus solide et plus résistante à la corruption des données. Les besoins de maintenance ont été réduits, par exemple le besoin de commandes `dsmaint`périodiques a été éliminé. Ce cache d'hôte local est une implémentation complètement différente sur le plan technique.

### Gérer le cache d'hôte local

Pour que le cache d'hôte local fonctionne correctement, la stratégie d'exécution de PowerShell sur chaque Controller doit être définie sur RemoteSigned, Unrestricted ou Bypass.

#### SQL Server Express LocalDB

Le logiciel de base de données Microsoft SQL Server Express LocalDB que le cache d'hôte local utilise est installée automatiquement lorsque vous installez un Controller ou mettez à niveau un Controller à partir d'une version antérieure à la version 7.9. Seul le broker secondaire communique avec cette base de données. Vous ne pouvez pas utiliser les applets de commande PowerShell pour modifier quoi que ce soit dans cette base de données. La base de données LocalDB ne peut pas être partagée entre les Controllers.

Le logiciel de la base de données SQL Server Express LocalDB est installé que le cache d'hôte local soit activé ou non.

Pour empêcher son installation, installez ou mettez à niveau le Delivery Controller à l'aide de la commande `XenDesktopServerSetup.exe` et ajoutez l'option `/exclude "Local Host Cache Storage (LocalDB)"`. Cependant, n'oubliez pas que la fonctionnalité de cache d'hôte local ne fonctionnera pas sans la base de données, et vous ne pouvez pas utiliser une autre base de données avec le broker secondaire.

L'installation de cette base de données LocalDB ne détermine pas si vous devez installer SQL Server Express ou non pour l'utiliser en tant que base de données du site.

Pour plus d'informations sur le remplacement d'une version antérieure de SQL Server Express LocalDB par une version plus récente, consultez la section Remplacer SQL Server Express LocalDB.

#### Paramètres par défaut après l'installation et la mise à niveau du produit

Lors d'une nouvelle installation de Citrix Virtual Apps and Desktops (version 7.16 au minimum), le cache d'hôte local est activé.

Après une mise à niveau (vers la version 7.16 ou ultérieure), le cache d'hôte local est activé s'il y a moins de 10 000 VDA dans le déploiement entier.

#### Activer/désactiver le cache d'hôte local

- Pour activer le cache d'hôte local, entrez :

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  Pour déterminer si le cache d'hôte local est activé, entrez `Get-BrokerSite`. Vérifiez que la propriété `LocalHostCacheEnabled` est `True`.

- Pour désactiver le cache d'hôte local, entrez :

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

Rappel : à partir de XenApp and XenDesktop 7.16, la location de connexion (fonctionnalité antérieure au cache d'hôte local à partir de la version 7.6) a été supprimée du produit et n'est plus disponible.

### Vérifier que le cache d'hôte local fonctionne

Pour vérifier que le cache d'hôte local est configuré et fonctionne correctement :

- Assurez-vous que les importations de synchronisation se déroulent correctement. Vérifiez les journaux d'événements.
- Assurez-vous que la base de données LocalDB SQL Server Express a été créée sur chaque Delivery Controller. Cela confirme que le broker secondaire peut prendre le relais, si nécessaire.
  - Sur le serveur Delivery Controller, accédez à `C:\Windows\ServiceProfiles\NetworkService`.
  - Vérifiez que `HaDatabaseName.mdf` et `HaDatabaseName_log.ldf` sont créés.
- Forcez une panne sur les Delivery Controller. Après avoir vérifié que le cache d'hôte local fonctionne, n'oubliez pas de remettre tous les Controller en mode normal. Cela peut prendre environ 15 minutes.

### Journaux d'événements

Les journaux d'événements consignent les synchronisations et les pannes. Dans les journaux de l'observateur d'événements, le mode panne est appelé *mode HA.**

**Config Synchronizer Service :**

Pendant une opération normale, les événements suivants peuvent se produire lorsque le CSS importe les données de configuration dans la base de données Cache hôte local à l'aide du broker Cache hôte local.

- 503 : Citrix Config Sync Service a reçu une configuration mise à jour. Cet événement indique le début du processus de synchronisation.
- 504 : Citrix Config Sync Service a importé une configuration mise à jour. L'importation de la configuration s'est terminée avec succès.
- 505 : Échec d'une importation par Citrix Config Sync Service. L'importation de la configuration n'a pas réussi. Si une configuration précédente réussie est disponible, elle est utilisée en cas de panne. Cependant, elle sera obsolète à partir de la configuration actuelle. Si aucune configuration précédente n'est disponible, le service ne peut pas participer à l'intermédiation de session pendant une panne. Dans ce cas, consultez la section Dépannage et contactez le support Citrix.
- 507 : Citrix Config Sync Service a abandonné une importation car le système est en mode d'arrêt et le broker Cache d'hôte local est utilisé pour la négociation de connexions. Le service a reçu une nouvelle configuration, mais l'importation a été abandonnée en raison d'une panne. Il s'agit du comportement attendu.
- 510 : Aucune donnée de configuration du service de configuration reçue depuis le service de configuration principal.
- 517 : Un problème s'est produit lors de la communication avec le broker principal.
- 518 : Le script Config Sync a été abandonné car le Broker secondaire (High Availability Service) n'est pas en cours d'exécution.

**High Availability Service :**

Ce service est également connu sous le nom de broker Cache d'hôte local.

- 3502 : une panne s'est produite et le broker Cache d'hôte local effectue des opérations de broker.
- 3503 : une panne a été résolue et le fonctionnement normal est rétabli.
- 3504 : indique le broker Cache d'hôte local qui a été sélectionné, ainsi que les autres brokers Cache d'hôte local impliqués dans la sélection.
- 3507 : fournit une mise à jour de l'état du cache d'hôte local toutes les 2 minutes, ce qui indique que le mode de cache d'hôte local est actif sur le broker sélectionné. Contient un résumé de la panne, notamment sa durée, l'enregistrement du VDA et les informations de session.
- 3508 : annonce que le cache d'hôte local n'est plus actif sur le broker sélectionné et que les opérations normales ont été rétablies. Contient un résumé de la panne, notamment sa durée, le nombre de machines enregistrées lors de l'événement de cache d'hôte local et le nombre de lancements réussis lors de l'événement.
- 3509 : indique que le cache d'hôte local est actif sur le ou les brokers non sélectionnés. Indique la durée de l'interruption toutes les 2 minutes, ainsi que le broker sélectionné.

- 3510 : Annonce que le cache d'hôte local n'est plus actif sur le ou les brokers non sélectionnés. Contient la durée de la panne et indique le broker sélectionné.

### Forcer une interruption

Vous pouvez souhaiter délibérément forcer une interruption.

- Si votre réseau s'interrompt et reprend de manière répétée. Forcer une panne jusqu'à la résolution des problèmes réseau empêche le basculement en continu entre les modes de fonctionnement normal et de panne (et les fréquentes rafales d'enregistrements de VDA qui en résultent).
- Pour tester un plan de récupération d'urgence.
- Pour vous assurer que le cache d'hôte local fonctionne correctement.
- Lorsque vous remplacez ou effectuez une maintenance sur le serveur de base de données du site.

Pour forcer une panne, modifiez le registre de chaque serveur contenant un Delivery Controller. Dans `HKLM\Software\Citrix\DesktopServer\LHC`, créez et définissez `OutageModeForced` comme `REG_DWORD` sur `1`. Ce réglage demande au broker de cache d'hôte local d'entrer en mode panne, quel que soit l'état de la base de données Si vous définissez la valeur sur `0`, le broker Cache d'hôte local sort du mode d'interruption.

Pour vérifier les événements, surveillez le fichier journal `Current_HighAvailabilityService` dans `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityService` .

### Dépannage

Plusieurs outils de dépannage sont disponibles lorsque l'importation d'une synchronisation dans la base de données Cache d'hôte local échoue et qu'un événement 505 est signalé.

**Traçage CDF :** contient les options des modules `ConfigSyncServer` et `BrokerLHC`. Ces options, ainsi que d'autres modules de broker, sont susceptibles d'identifier le problème.

**Rapport :** en cas d'échec d'une importation de synchronisation, vous pouvez générer un rapport. Ce rapport s'arrête à l'objet qui a causé l'erreur. Cette fonctionnalité de rapport affecte la vitesse de synchronisation, Citrix vous recommande donc de la désactiver lorsqu'elle n'est pas utilisée.

Pour activer et générer un rapport de traçage CSS, entrez la commande suivante :

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

Le rapport HTML est publié sur `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html`.

Une fois le rapport généré, entrez la commande suivante pour désactiver la fonctionnalité de rapport :

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

**Exporter la configuration du broker :** fournit la configuration exacte à des fins de débogage.

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

Par exemple, `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

#### Commandes PowerShell du cache d'hôte local

Vous pouvez gérer le cache d'hôte local (LHC ou Local Host Cache) sur vos Delivery Controller à l'aide des commandes PowerShell.

Le module PowerShell se trouve à l'emplacement suivant sur les Delivery Controller :

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **Important :**
>
> Exécutez ce module uniquement sur les Delivery Controller.

**Importer le module PowerShell** Pour importer le module, exécutez la commande suivante sur votre Delivery Controller.

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

**Commandes PowerShell pour gérer le cache d'hôte local (LHC)** Les commandes suivantes vous aident à activer et à gérer le mode LHC sur les Delivery Controller.

| Applets de commande | Fonction |
| --- | --- |
| `Enable-LhcForcedOutageMode` | Permet de placer le broker en mode LHC. Les fichiers de base de données du LHC doivent avoir été créés avec succès par le service ConfigSync pour que `Enable-LhcForcedOutageMode`fonctionne correctement. Cette applet de commande force uniquement le LHC sur le Delivery Controller sur lequel il a été exécuté. Pour que le LHC soit actif, cette commande doit être exécutée sur tous les Delivery Controller de la zone. |
| `Disable-LhcForcedOutageMode` | Permet de faire sortir le broker du mode LHC. Cette applet de commande désactive uniquement le mode LHC sur le Delivery Controller sur lequel elle a été exécutée. `Disable-LhcForcedOutageMode` doit être exécuté sur tous les Delivery Controller de la zone. |
| `Set-LhcConfigSyncIntervalOverride` | Permet de définir l'intervalle auquel Citrix Config Synchronizer Service (CSS) vérifie les modifications de configuration sur le site. L'intervalle de temps peut aller de 60 secondes (une minute) à 3 600 secondes (une heure). Ce paramètre s'applique uniquement au Delivery Controller sur lequel il a été exécuté. Pour des raisons de cohérence entre les Delivery Controller, pensez à exécuter cette applet de commande sur chaque Delivery Controller. Par exemple : `Set-LhcConfigSyncIntervalOverride -Seconds 1200` |

| Applets de commande | Fonction |
| --- | --- |
| `Clear-LhcConfigSyncIntervalOverride` | Pemet de définir l'intervalle auquel Citrix Config Synchronizer Service (CSS) vérifie les modifications de configuration sur le site, à la valeur par défaut de 300 secondes (cinq minutes). Ce paramètre s'applique uniquement au Delivery Controller sur lequel il a été exécuté. Pour des raisons de cohérence entre les Delivery Controller, pensez à exécuter cette applet de commande sur chaque Delivery Controller. |
| `Enable-LhcHighAvailabilitySDK` | Permet d'accéder à toutes les applets de commande `Get-Broker*` du Delivery Controller sur lequel il a été exécuté. |
| `Disable-LhcHighAvailabilitySDK` | Permet de désactiver l'accès aux applets de commande du broker dans le Delivery Controller sur lequel il a été exécuté. |

**Remarque :**

- Utilisez le port 89 lors de l'exécution des applets de commande `Get-Broker*` sur le Delivery Controller. Par exemple :
  - `Get-BrokerMachine -AdminAddress localhost:89`
- Lorsqu'il n'est pas en mode LHC, le broker LHC du Delivery Controller ne contient que les informations de configuration.
- En mode LHC, le broker LHC du Delivery Controller sélectionné contient les informations suivantes :
  - États des ressources
  - Détails de la session
  - Enregistrements de VDA
  - Informations de configuration

## Surveiller et gérer les machines et les sessions à l'aide de la fonction de recherche

June 27, 2024

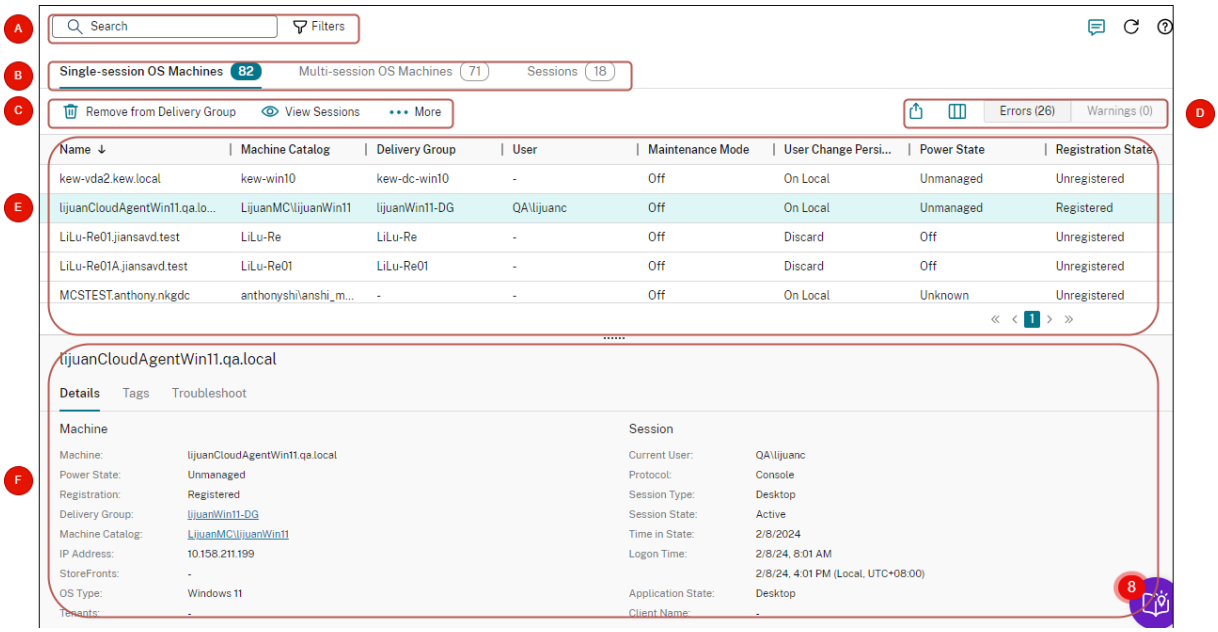
 

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Cet article explique comment surveiller et gérer les machines et les sessions à l'aide du nœud **Configuration complète > Rechercher**.

## En savoir plus sur le nœud

Le nœud **Rechercher** fournit un emplacement central pour la surveillance et la gestion des machines et des sessions utilisateur.




| Légende | Zone | Description |
|---|---|---|
| A | Barre de recherche | Propose une recherche rapide et une recherche basée sur des filtres qui vous permettent de définir des critères de recherche complexes. Pour plus d'informations, consultez la section Rechercher des instances. |

| Légende | Zone | Description |
| --- | --- | --- |
| B | Onglets de type | Affiche des onglets pour répertorier les machines par type ou répertorier toutes les sessions. Le nombre d'instances apparaît dans les noms des onglets. |
| C | Actions au niveau de l'instance | Affiche les actions que vous pouvez effectuer sur les *instances sélectionnées* (machines ou sessions). Pour plus d'informations, consultez les sections Actions de la machine et Actions de session. |
| D | Actions de niveau liste | Affiche les actions que vous pouvez effectuer sur la *liste* actuelle<br>-Icône **Exporter** : permet d'exporter la liste des instances affichées dans la vue principale vers un fichier CSV.<br>-Icône **Colonnes à afficher** : permet de personnaliser l'affichage principal de la liste. |
| E | Vue principale | Affiche les instances et leurs propriétés. Vous pouvez personnaliser la vue principale en sélectionnant l'icône **Colonnes à afficher**. Pour plus d'informations sur les colonnes disponibles et leurs descriptions, consultez les sections Colonnes de machine et Colonnes de session.<br>Étiquette **Erreurs** : activez cette étiquette pour afficher uniquement les machines non enregistrées présentant des erreurs dans la vue principale. Pour afficher les détails du problème, accédez à l'onglet **Dépannage** dans le volet **Détails**.<br>Étiquette **Avertissements** : activez cette étiquette pour afficher uniquement les machines non enregistrées présentant des avertissements dans la vue principale. Pour afficher les détails du problème, accédez à l'onglet **Dépannage** dans le volet **Détails**. |
| F | Volet de détails | Affiche les informations suivantes **Détails**.<br>Détails de l'instance sélectionnée (machine ou session)<br>Balises appliquées à la machine sélectionnée<br>Détails des erreurs ou des avertissements relatifs à la machine sélectionnée, y compris les problèmes, les causes possibles et les solutions suggérées |

## Rechercher des instances

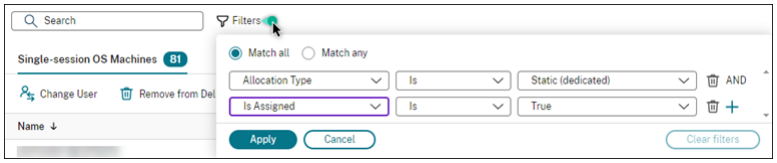
Utilisez la fonction de recherche pour localiser des machines et des sessions spécifiques :

- Rechercher à l'aide de filtres
- Enregistrer le jeu de filtres actuel pour une recherche rapide
- Épingler un champ de filtre dans la barre de recherche
- Effectuer une recherche à l'aide de la zone de recherche rapide
- Conseils pour améliorer la recherche

### Rechercher à l'aide de filtres

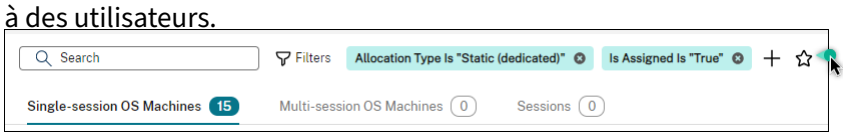
Par exemple, pour localiser toutes les machines avec OS mono-session qui sont *statiques* et *attribuées à des utilisateurs*, procédez comme suit :

1. Dans l'onglet **Machines avec OS mono-session**, cliquez sur l'icône **Filtres**. Le panneau Filtres s'affiche.
2. Ajoutez les critères de filtre nécessaires.




3. Sélectionnez **Correspondance exacte** (opérateur ET) si vous souhaitez que la recherche renvoie des résultats correspondant à tous les critères du filtre. Sélectionnez **Correspondance partielle** (opérateur OU) si vous souhaitez que la recherche renvoie des résultats correspondant à l'un des critères de filtre.
4. Cliquez sur **Appliquer**.

   La liste filtrée affiche toutes les machines avec OS mono-session qui sont statiques et attribuées à des utilisateurs.



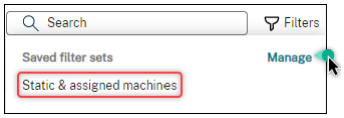

### Enregistrer le jeu de filtres actuel pour une recherche rapide

Par exemple, pour enregistrer le filtre défini pour les machines avec système d'exploitation mono-session qui sont statiques et attribuées à des utilisateurs pour une utilisation ultérieure, procédez comme suit :

1. Après avoir effectué une recherche basée sur un filtre, cliquez sur l'icône **Étoile** dans la barre de recherche, comme illustré dans la figure précédente.
2. Sur la page qui s'affiche, entrez un nom pour le jeu de filtres (par exemple, *Machines statiques et attribuées*).
3. Cliquez sur **Enregistrer**.

   Le jeu de filtres enregistré apparaît dans la liste de l'historique de recherche lorsque vous cliquez sur la zone de recherche.

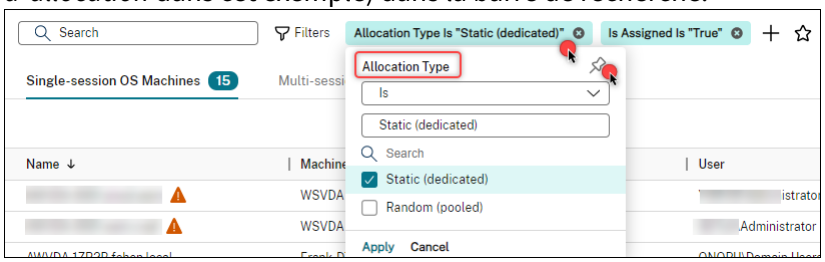



> **Remarque :**
>
> Les jeux de filtres sont enregistrés pour chaque compte utilisateur. Pour gérer les ensembles de filtres enregistrés, sélectionnez **Gérer**.

### Épingler un champ de filtre dans la barre de recherche

Épinglez les *champs* de filtre fréquemment utilisés dans la barre de recherche pour y accéder facilement. Par exemple, après avoir effectué une recherche basée sur un filtre, vous souhaitez épingler le champ **Type d'allocation** dans la barre de recherche. Procédez comme suit :

1. Cliquez sur le *paramètre de filtre* dans la barre de recherche.
2. Dans le panneau qui s'affiche, cliquez sur l'icône **Épingler** pour épingler le champ de filtre (*Type d'allocation* dans cet exemple) dans la barre de recherche.




### Effectuer une recherche à l'aide de la zone de recherche rapide

La zone de recherche rapide permet de rechercher facilement des instances en fonction des propriétés de nom ou des jeux de filtres enregistrés. Les étapes détaillées sont les suivantes :

1. Cliquez sur la zone de recherche. Les recherches récentes et les jeux de filtres enregistrés apparaissent dans la liste déroulante. Vous pouvez cliquer sur une recherche précédente ou sur un jeu de filtres pour effectuer une recherche rapide.

2. Pour démarrer une nouvelle recherche, entrez un nom complet ou partiel parmi les options suivantes :

    - Nom de la machine ou nom DNS
    - Nom du catalogue de machines
    - Nom du groupe de mise à disposition
    - Nom d'utilisateur de la session
    - Nom du client de la session
    - Nom convivial de la machine virtuelle hébergeant la session, tel qu'il est utilisé par son hyperviseur
    - Nom du serveur d'hébergement

**Conseils pour améliorer la recherche**

Lorsque vous utilisez la fonction de recherche, tenez compte des conseils suivants :

- Sur le nœud **Rechercher**, sélectionnez n'importe quelle colonne pour trier les éléments.
- Pour afficher des caractéristiques supplémentaires dans l'écran où vous pouvez rechercher et trier, sélectionnez **Colonnes à afficher** ou cliquez sur une colonne et sélectionnez **Colonnes à afficher**. Dans la fenêtre **Colonnes à afficher**, cochez la case en regard des éléments que vous souhaitez afficher, puis sélectionnez **Enregistrer** pour quitter.

    > **Remarque :**
    >
    > Les colonnes qui dégradent les performances sont indiquées par la mention **Dégrade les performances**.

- Pour localiser une machine utilisateur connectée à une machine, utilisez le **client (IP)** et **Est**, puis entrez l'adresse IP de la machine.
- Pour localiser les sessions actives, utilisez **État de session**, **Est** et **Connecté**.
- Pour répertorier toutes les machines d'un groupe de mise à disposition, sélectionnez **Groupes de mise à disposition** dans le volet de gauche. Sélectionnez le groupe, puis sélectionnez **Afficher les machines** dans la barre d'actions ou dans le menu contextuel.

Gardez à l'esprit les considérations suivantes lorsque vous effectuez des opérations de tri :

- Tant que le nombre d'éléments ne dépasse pas 5 000, vous pouvez cliquer sur n'importe quelle colonne pour trier les éléments qu'elle contient. Lorsque le nombre dépasse 5 000, vous pouvez trier uniquement par nom ou par utilisateur actuel (en fonction de l'onglet sur lequel vous vous trouvez). Pour faciliter le tri, utilisez des filtres pour réduire le nombre d'éléments à 5 000 ou moins.

- Lorsque le nombre d'éléments est supérieur à 500 mais inférieur à 5 000 :
  - Nous mettons en cache toutes les données localement pour améliorer les performances de tri. Dans les onglets **Machines avec OS mono-session** et **Machines avec OS multi-session**, nous mettons en cache les données la première fois que vous cliquez sur une colonne (n'importe quelle colonne sauf la colonne **Nom**) pour effectuer un tri. Dans l'onglet **Sessions**, nous mettons en cache les données la première fois que vous cliquez sur une colonne (n'importe quelle colonne à l'exception de la colonne **Utilisateur actuel**) pour effectuer un tri. Par conséquent, le tri prend plus de temps. Pour des performances plus rapides, triez par nom ou par utilisateur actuel, ou utilisez des filtres pour réduire le nombre d'éléments.
  - Le message suivant sous le tableau indique que les données sont mises en cache : Dernière actualisation : <`the time when you refreshed the table`>. Dans ce cas, les opérations de tri sont basées sur des éléments précédemment chargés. Ces éléments peuvent ne pas être à jour. Pour les mettre à jour, cliquez sur l'icône d'actualisation.

### Personnaliser les colonnes à afficher

Créez une vue principale personnalisée pour afficher les propriétés et les états essentiels à vos opérations quotidiennes. Les étapes détaillées sont les suivantes :

1. Dans le nœud **Rechercher**, sélectionnez l'onglet **Machines avec OS à sessions multiples**, **Machines avec OS mono-session** ou **Sessions** selon vos besoins.
2. Cliquez sur l'icône **Colonnes à afficher** dans la barre d'action et sélectionnez les colonnes.

   Pour plus d'informations sur les colonnes disponibles et leurs descriptions, consultez les sections Colonnes de machine et Colonnes de session.

Lorsque vous sélectionnez des colonnes, vous pouvez voir des colonnes portant l'étiquette **Dégrade les performances**. La sélection de ces colonnes risque de dégrader les performances de la console. Tenez compte des considérations suivantes :

- Une fois la personnalisation terminée, le tableau est actualisé pour afficher les colonnes sélectionnées. Leur présence peut entraîner des retards lorsque vous actualisez le tableau.
- Lorsque vous actualisez le navigateur ou que vous vous déconnectez de la console, puis que vous vous reconnectez, un message s'affiche pour vous demander si vous souhaitez conserver ces colonnes. Si vous choisissez de les conserver, vous ne pouvez pas actualiser le tableau plus d'une fois par minute afin d'optimiser les performances de la console. Pour des actualisations plus fréquentes, supprimez toutes les colonnes qui dégradent les performances.

## Gérer les machines et les sessions

Utilisez les actions du nœud Rechercher pour résoudre les problèmes liés aux machines et aux sessions ou pour traiter les demandes des utilisateurs.

### À savoir

Vous pouvez gérer les machines à différents niveaux :

- Au niveau de chaque machine. Utilisez le nœud **Rechercher** pour localiser les machines cibles et effectuer des actions.
- Au niveau du catalogue de machines. Par exemple, pour modifier les images principales d'un catalogue, supprimer des machines d'un catalogue ou ajouter des machines à un catalogue. Pour de plus amples informations, consultez l'article Gérer des catalogues de machines.
- Au niveau du groupe de mise à disposition. Par exemple, pour activer ou désactiver le mode de maintenance pour les machines d'un groupe. Pour de plus amples informations, consultez la section Gérer les groupes de mise à disposition.

Outre le niveau de session individuel, vous pouvez également gérer les sessions au niveau du groupe de mise à disposition. Par exemple, pour configurer le pré-lancement de session et l'attente de session pour un groupe de mise à disposition. Pour de plus amples informations, consultez la section Gérer les groupes de mise à disposition.

#### Exécuter des actions sur des machines ou des sessions

Pour gérer les machines ou les sessions au niveau de chaque instance, procédez comme suit :

1. Dans le nœud **Rechercher**, sélectionnez l'onglet **Machines avec OS à sessions multiples**, **Machines avec OS mono-session** ou **Sessions**.
2. Sélectionnez une ou plusieurs instances selon vos besoins.
3. Dans la barre d'actions ou dans le menu contextuel, sélectionnez une action en fonction des problèmes que vous rencontrez avec ces instances ou en fonction des demandes des utilisateurs.

   Pour plus d'informations sur les actions disponibles et leurs descriptions, consultez les sections Actions de machine et Actions de session.

> **Remarque :**

> Si vous sélectionnez deux instances ou plus, seules les actions qui s'appliquent à toutes ces instances sont disponibles.

### Exporter les données de machine ou de session vers des fichiers CSV

Exportez la liste des instances (machines ou sessions) affichées sur un onglet (jusqu'à 30 000 éléments) vers un fichier CSV. Les étapes détaillées sont les suivantes :

1. Dans le nœud **Rechercher**, sélectionnez l'onglet **Machines avec OS à sessions multiples**, **Machines avec OS mono-session** ou **Sessions** selon vos besoins.
2. Cliquez sur l'icône **Exporter** dans le coin supérieur droit.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **Continuer**.

   L'exportation peut prendre plusieurs minutes. Le fichier se trouve dans le dossier de téléchargement par défaut de votre navigateur.

> **Remarque :**
>
> Sur chaque onglet du nœud **Rechercher**, vous ne pouvez pas effectuer une autre exportation tant qu'une exportation est en cours.

## Actions et colonnes de machine

June 27, 2024

Cet article répertorie les actions et les colonnes de machine avec des descriptions à titre de référence.

### Actions

Consultez les actions que vous pouvez effectuer sur les machines et leurs descriptions.

| Action | Description | S'applique à |
|---|---|---|
| Supprimer d'un groupe de mise à disposition | Supprimer une machine d'un groupe de mise à disposition | Mono-session et multi-session |
| Ajouter au groupe de mise à disposition | Ajoutez une machine à un groupe de mise à disposition. | Mono-session et multi-session |

| Action | Description | S'applique à |
| --- | --- | --- |
| Afficher les sessions | Affichez les sessions en cours d'exécution sur une machine. | Mono-session et multi-session |
| Gérer les balises | Ajoutez et gérez des balises pour une machine. Pour plus d'informations sur les cas d'utilisation standard des balises, consultez la sectionBalises. | Mono-session et multi-session |
| Activer le mode de maintenance | Placez une machine en mode de maintenance avant d'appliquer des correctifs ou pour le dépannage.<br>Ce mode empêche l'établissement de nouvelles connexions à cette machine. L'utilisateur peut se connecter à des sessions existantes sur cette machine, mais ne peut pas y démarrer de nouvelles sessions. | Mono-session et multi-session |
| Désactiver le mode de maintenance | Désactivez le mode de maintenance d'une machine. | Mono-session et multi-session |
| Mettre à niveau le VDA | Mettez à niveau le VDA pour une machine. | Machines avec système d'exploitation mono-session ou multi-session répondant à certaines exigences : En savoir plus. |
| Fermer la session | Forcez la fermeture de session d'une machine. | Mono-session et multi-session |
| Supprimer | Supprimez une machine virtuelle d'un catalogue de machines tout en la laissant intacte sur l'hyperviseur ou le service cloud. | Mono-session et multi-session |
| Changer d'utilisateur | Attribuez une machine à un utilisateur spécifique. | Machines *statiques* mono-session. |
| Démarrer | Démarrez une machine. | Mono-session et multi-session |
| Arrêter | Arrêtez une machine. | Mono-session et multi-session |

| Action | Description | S'applique à |
|---|---|---|
| Redémarrer | Redémarrez une machine. | Mono-session et multi-session |
| Suspendre | Placez une machine en état d'hibernation ou de suspension. Lorsque vous suspendez une machine, les serveurs Delivery Controller stockent le contenu de la mémoire dans un fichier avant d'arrêter la machine. | Machines avec OS mono-session |
| Reprendre | Reprenez une machine suspendue. Lorsque vous redémarrez une machine suspendue, les serveurs Delivery Controller démarrent la machine et la restaurent à son état précédent. | Machines avec OS mono-session |
| Forcer le redémarrage | Forcez le redémarrage d'une machine. | Machines avec OS mono-session |
| Forcer l'arrêt | Forcez l'arrêt d'une machine. | Machines avec OS mono-session |

## Colonnes

Afficher toutes les colonnes de machines et leurs descriptions par type :

- Machine
- Détails de la machine
- Applications
- Hébergement
- Connexion
- Enregistrement
- Détails de la session
- Session

### Machine

Colonnes de la catégorie **Machine**.

| Colonne | Description | S'applique à |
| --- | --- | --- |
| Nom | Nom d'hôte DNS de la machine. | Mono-session et multi-session |
| Catalogue de machines | Nom du catalogue auquel appartient la machine. | Mono-session et multi-session |
| Groupe de mise à disposition | Nom du groupe de mise à disposition auquel appartient la machine. | Mono-session et multi-session |
| Nom d'affichage de l'utilisateur | Nom complet des utilisateurs associés à la machine (généralement au format `Firstname Lastname`). Les utilisateurs associés sont les utilisateurs actuels pour les machines partagées et les utilisateurs attribués pour les machines dédiées. | Mono-session et multi-session |
| Utilisateur | Nom d'utilisateur des utilisateurs associés à la machine (au format « domaine\utilisateur »). Les utilisateurs associés sont les utilisateurs actuels pour les machines partagées et les utilisateurs attribués pour les machines dédiées. | Mono-session et multi-session |
| Nom d'utilisateur principal | Nom d'utilisateur principal des utilisateurs associés à la machine (au format « utilisateur@domaine »). Les utilisateurs associés sont les utilisateurs actuels pour les machines partagées et les utilisateurs attribués pour les machines dédiées. | Mono-session et multi-session |

| Colonne | Description | S'applique à |
| --- | --- | --- |
| Nom d'affichage du bureau | Nom publié de la machine initialement utilisée pour lancer la session. Il s'agit du nom affiché sur l'application Citrix Workspace ou StoreFront. **Remarque :** pour modifier l'affichage d'un bureau, vous devez disposer de l'autorisation **Mettre à jour la machine**, car la modification du nom d'affichage implique la mise à jour des propriétés de la machine. | Mono-session uniquement |
| Conditions de bureau | Liste des conditions de bureau restantes pour la machine. Valeurs possibles : Unknown, CPU, ICALatency et UPMLogonTime. | Mono-session et multi-session |
| Type d'allocation | Type d'allocation de la machine : **Permanent** lorsqu'elle est attribuée à un utilisateur de façon permanente. **Aléatoire** lorsqu'elle est attribuée de manière aléatoire. | Mono-session et multi-session |
| Mode de maintenance | Indique si la machine est en mode de maintenance. | Mono-session et multi-session |
| Paramètre de connexion Windows | Mode d'ouverture de session signalé par Windows. Valeurs possibles : Ouverture de session activée, Drainage, Drainage jusqu'au redémarrage et Ouverture de session désactivée. | Multi-session uniquement |

| Colonne | Description | S'applique à |
| --- | --- | --- |
| Est attribué | Indique si un bureau dédié a été attribué à un utilisateur ou à un client (nom/adresse). Il peut être attribué aux utilisateurs de manière explicite ou lors de la première utilisation de la machine. | Mono-session et multi-session |
| Est physique | Indique si la machine est physique. La valeur `True` indique que la machine est physique, c'est-à-dire que son alimentation n'est pas gérée par les serveurs Delivery Controller. La valeur `False` indique le contraire. | Mono-session et multi-session |
| Type de provisioning | Indique la méthode de provisioning de la machine. Valeurs possibles Manuel : non provisionné à l'aide de PVS ou MCS. PVS : provisionné à l'aide de PVS (machines physiques, lames et machines virtuelles) MCS : provisionné à l'aide de MCS (machines virtuelles uniquement) | Mono-session et multi-session |
| Redémarrage programmé | État de toute opération de redémarrage planifiée de la machine. Valeurs possibles Aucun : aucun redémarrage n'est planifié. En attente : en attente de redémarrage, mais disponible pour utilisation. Vidage en attente : redémarrage en attente, mais indisponible pour de nouvelles sessions. Les reconnexions à des connexions existantes sont toujours autorisées. En cours : en cours de redémarrage planifié. Naturel : redémarrage naturel en cours. La machine est en attente de redémarrage. | Mono-session et multi-session |
| Zone | Nom de la zone dans laquelle se trouve la machine. | Mono-session et multi-session |
| État | État général du bureau associé à la machine, dérivé de différents états spécifiques tels que l'état de la session, l'état d'enregistrement et l'état d'alimentation. | Mono-session et multi-session |

| Colonne | Description | S'applique à |
| --- | --- | --- |
| | États possibles : Désactivé, Non enregistré, Disponible, Déconnecté, En cours d'utilisation et Préparation. | |
| Balises | Liste des balises associées à la machine. | Mono-session et multi-session |
| Mise à niveau de VDA | État de la machine pour les actions de mise à niveau du package VDA.<br>Valeurs possibles : MissingUpgradeType, UpgradeScheduled, UpgradeAvailable, UpToDate et Unknown. | Mono-session et multi-session |
| Prise en charge de la suspension | Indique si la machine prend en charge les actions d'alimentation (Suspendre et Reprendre). | Mono-session et multi-session |
| Indice de charge | Indice de charge actuel. Pour plus d'informations, accédez à En savoir plus. | Multi-session uniquement |
| État de drainage | Indique si la machine est en cours de drainage et s'arrêtera à la fin de toutes les sessions. La valeur true s'affiche uniquement pour les machines multi-session gérées par alimentation.<br>**Remarque :** la machine ne s'arrête pas si elle est en mode de maintenance. Elle ne s'arrête qu'après la désactivation du mode de maintenance. | Multi-session uniquement |

**Détails de la machine**

Colonnes de la catégorie **Détails de la machine**.

| Colonne | Description | S'applique à |
| --- | --- | --- |
| Version de l'agent | Version de Citrix Virtual Delivery Agent (VDA) installée sur la machine. | Mono-session et multi-session |
| Adresse IP | Adresse IP de la machine. | Mono-session et multi-session |
| Est attribué | Indique si un bureau dédié a été attribué à un utilisateur ou à un client (nom/adresse). Il peut être attribué aux utilisateurs de manière explicite ou lors de la première utilisation de la machine. | Mono-session et multi-session |
| Type d'OS | Type de système d'exploitation exécuté sur la machine. | Mono-session uniquement |

### Applications

Colonnes de la catégorie **Applications**.

| Colonne | Description | S'applique à |
| --- | --- | --- |
| Application en cours d'utilisation | Liste des applications utilisées sur la machine (affichées en tant que noms de navigateur). | Mono-session et multi-session |
| Applications publiées | Liste des applications publiées par la machine (affichées en tant que noms de navigateur). | Mono-session et multi-session |

### Connexions

Colonnes de la catégorie **Connexions**.

| Colonne | Description | S'applique à |
| --- | --- | --- |
| Client (IP) | Adresse IP du client connecté à la machine. | Mono-session uniquement |
| Client | Nom d'hôte du client connecté à la machine. | Mono-session uniquement |

| Colonne | Description | S'applique à |
| --- | --- | --- |
| Version du plug-in | Version de l'application Citrix Workspace sur le client connecté. | Mono-session uniquement |
| Connecté via | Nom d'hôte de la connexion entrante, généralement une passerelle, un routeur ou un client. | Mono-session uniquement |
| Connecté via (IP) | Adresse IP de la connexion entrante, généralement une passerelle, un routeur ou un client. | Mono-session uniquement |
| Type de connexion | Protocole utilisé pour la session. Valeurs possibles : HDX, RDP et Console. Remarque : le champ est laissé vide pour les sessions de console sur les VDA XenDesktop 5. | Mono-session uniquement |
| Heure de la dernière connexion (UTC) | Heure de la dernière tentative de connexion détectée qui a échoué ou réussi. | Mono-session et multi-session |
| Utilisateur de la dernière connexion | Nom SAM (au format « DOMAINE\utilisateur ») de l'utilisateur qui a tenté d'établir la dernière connexion à la machine. Si le nom SAM n'est pas disponible, le SID est utilisé. | Mono-session et multi-session |
| Secure ICA actif | Indique si SecureICA est actif sur la session en cours. Toujours NULL pour les machines multi-session. | Mono-session et multi-session |

### Hébergement

Colonnes de la catégorie **Hébergement**.

| Colonne | Description | S'applique à |
| --- | --- | --- |
| VM | Nom convivial de la machine hébergée qui exécute la session, tel qu'il est utilisé par son hyperviseur. Il ne correspond pas nécessairement au nom DNS ou AD de la machine. | Mono-session et multi-session |
| Nom du serveur d'hébergement | Nom DNS de l'hyperviseur qui héberge la machine si elle est gérée. | Mono-session et multi-session |
| Connexion | Nom de la connexion hôte attribuée à la machine hébergeant la session. | Mono-session et multi-session |
| En attente de mise à jour | Indique si l'image de machine virtuelle d'une machine hébergée est obsolète et doit être mise à jour avec une nouvelle image au prochain redémarrage de la machine. | Mono-session et multi-session |
| Persistance des modifications de l'utilisateur | Indique le mode de gestion des modifications apportées par les utilisateurs, notamment si les modifications sont persistantes<br>Local : persistant. Les modifications apportées par les utilisateurs sont enregistrées localement.<br>Aucun : non persistant. Les modifications apportées par les utilisateurs ne sont pas enregistrées. | Mono-session et multi-session |
| Action d'alimentation en attente | Indique s'il y a des actions d'alimentation en attente pour la machine.<br>Aucun, Redémarrer, Démarrer, Arrêter, Suspendre, Reprendre, Réinitialiser, Désactiver, Activer, Désactivation en cours, Suspension et Reprise. | Mono-session et multi-session |
| État d'alimentation | État d'alimentation de la machine.<br>Inconnu, Non géré, Indisponible, Suspendu, Activation en cours, Désactivation en cours, Suspension et Reprise. | Mono-session et multi-session |

| Colonne | Description | S'applique à |
| --- | --- | --- |
| Arrêt après utilisation | Applicable uniquement aux machines mono-session gérées par alimentation. Indique si la machine est corrompue et s'arrêtera à la fin de toutes les sessions.<br>**Remarque :** la machine ne s'arrête pas si elle est en mode de maintenance. Elle ne s'arrêtera qu'après la désactivation du mode de maintenance. | Mono-session uniquement |

**Enregistrement**

Colonnes de la catégorie **Enregistrement**.

| Colonne | Description | S'applique à |
| --- | --- | --- |
| Dernier échec d'enregistrement | Raison du dernier désenregistrement de la machine auprès du broker. | Mono-session et multi-session |

| Colonne | Description | S'applique à |
| --- | --- | --- |
| | Les valeurs possibles sont les suivantes : AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError et BrokerRegistrationLimitReached. | |
| Heure du dernier échec d'enregistrement (UTC) | Heure du dernier désenregistrement de la machine. | Mono-session et multi-session |
| État d'enregistrement | État d'enregistrement de la machine. Valeurs possibles : Non enregistré, Initialisation, Enregistré et Erreur de l'agent. | Mono-session et multi-session |

| Colonne | Description | S'applique à |
| --- | --- | --- |
| État d'erreur | État récapitulatif de l'état de panne actuel de la machine. Valeurs possibles Aucune : aucune panne. La machine est saine. FailedToStart : échec du démarrage. La dernière opération de mise sous tension de la machine a échoué. StuckOnBoot : bloquée au démarrage. La machine n'a pas pu démarrer après avoir été mise sous tension. Non enregistrée. la machine n'a pas pu s'enregistrer dans le délai prévu ou son enregistrement a été rejeté. MaxCapacity. Capacité maximale. La machine fonctionne à pleine capacité. | Mono-session et multi-session |

**Détails de la session**

Colonnes de la catégorie **Détails de la session**.

| **Colonne** | **Description** | **S'applique à** |
| --- | --- | --- |
| Lancer via | Nom d'hôte du serveur StoreFront utilisé pour lancer la session négociée par broker. Toujours NULL pour les machines multi-session. | Mono-session et multi-session |
| Lancé via (IP) | Adresse IP du serveur StoreFront utilisé pour lancer la session négociée par broker. Toujours NULL pour les machines multi-session. | Mono-session et multi-session |
| Heure de modification de la session (UTC) | Heure de la dernière modification d'état de la session en cours. | Mono-session uniquement |
| Filtres SmartAccess | Balises SmartAccess pour la session en cours. Toujours NULL pour les machines multi-session. | Mono-session et multi-session |

**Session**

Colonnes de la catégorie **Session**.

| Colonne | Description | S'applique à |
|---|---|---|
| État de la session | État de la session en cours. Valeurs possibles : Autre, Préparation de la session, Connecté, Actif, Déconnecté, Reconnexion, Session non négociée par broker et Inconnu. | Mono-session uniquement |
| Utilisateur actuel | Nom de l'utilisateur de la session en cours (au format « DOMAINE\utilisateur »). | Mono-session uniquement |
| Heure de début (UTC) | Heure de début de la session en cours. | Mono-session uniquement |
| Nombre de sessions | Nombre de sessions sur la machine. | Multi-session uniquement |

## Actions et colonnes de session

June 27, 2024

Cet article répertorie les actions et les colonnes de machine avec des descriptions à titre de référence.

### Actions

Consultez les actions que vous pouvez effectuer sur les sessions et leurs descriptions.

| Action | Description | S'applique aux sessions sur |
|---|---|---|
| Fermer la session | Déconnectez un utilisateur d'une session. | Machines avec OS mono-session ou OS multi-session |
| Envoyer un message | Envoyez un message à l'utilisateur d'une session. | Machines avec OS mono-session ou OS multi-session |

| Action | Description | S'applique aux sessions sur |
|---|---|---|
| Afficher les machines | Affichez la machine d'hébergement d'une session. | Machines avec OS mono-session ou OS multi-session |
| Déconnecter | Déconnectez une session. Si une session se déconnecte, elle reste active et ses applications continuent d'être exécutées, mais la machine utilisateur ne communique plus avec DaaS. | Machines avec OS mono-session ou OS multi-session |
| Arrêter la machine | Arrêtez la machine associée à une session. | Machines avec OS mono-session |
| Redémarrer la machine | Redémarrez la machine associée à une session. | Machines avec OS mono-session |

### Colonnes

Affichez les colonnes des sessions et leurs descriptions.

| Colonne | Description |
|---|---|
| Utilisateur actuel | Nom de l'utilisateur, nom d'utilisateur principal (UPN) de l'utilisateur. |
| Nom | Nom d'hôte DNS de la machine hébergeant la session. |
| Groupe de mise à disposition | Nom du groupe de mise à disposition contenant la machine hébergeant la session. |
| Catalogue de machines | Nom du catalogue de machines contenant la machine hébergeant la session. |
| Version de l'agent | Version de Citrix Virtual Delivery Agent (VDA) installée sur la machine hébergeant la session. |
| Application en cours d'utilisation | Liste des applications utilisées au cours de la session, identifiées par leur nom administratif. |
| Négocié par broker autonome | Indique s'il s'agit d'une session HDX établie par une connexion directe sans broker. |
| Heure de négociation (UTC) | Heure à laquelle la session a été négociée par broker. |
| Nom d'utilisateur de broker | Nom de l'utilisateur du broker. |

| Colonne | Description |
| --- | --- |
| Client (IP) | Adresse IP du client connecté à la session. |
| Client | Nom d'hôte du client connecté à la session. |
| Version du plug-in | Version de l'application Citrix Workspace exécutée sur le client connecté à la session. |
| Connecté via | Nom d'hôte des connexions entrantes, généralement une passerelle, un routeur ou un client. |
| Connecté via (IP) | Adresse IP de la connexion entrante, généralement une passerelle, un routeur ou un client. |
| Type d'allocation | Indique si la session est partagée ou dédiée. |
| Masqué | Indique si la session est masquée pour l'utilisateur et ne doit pas être reconnectée. |
| VM | Nom convivial de la machine virtuelle hébergeant la session, tel qu'il est utilisé par son hyperviseur. Il ne correspond pas nécessairement au nom DNS ou AD de la machine. |
| Nom du serveur d'hébergement | Nom DNS de l'hyperviseur qui héberge la machine hébergeant la session. |
| Connexion | Nom de la connexion hôte attribuée à la machine hébergeant la session. |
| En attente de mise à jour | Indique si l'image de machine virtuelle d'une machine hébergée est obsolète et doit être mise à jour avec une nouvelle image au prochain redémarrage de la machine. |
| Mode de maintenance | Indique si la machine hébergeant la session est en mode de maintenance. |
| Adresse IP | Adresse IP de la machine hébergeant la session. |
| Est physique | Indique si la machine hébergeant la session est physique. La valeur `True` indique que la machine est physique, c'est-à-dire que son alimentation n'est pas gérée par les serveurs Delivery Controller. La valeur `False` indique le contraire. |

| Colonne | Description |
| --- | --- |
| Lancer via | Nom d'hôte du serveur StoreFront utilisé pour lancer la session. Ce champ est vide si la session a été lancée via Workspace. |
| Lancé via (IP) | Adresse IP du serveur StoreFront utilisé pour lancer la session. Ce champ est vide si la session a été lancée via Workspace. |
| Type d'OS | Chaîne d'identification du système d'exploitation hébergeant la session. |
| Persistance des modifications de l'utilisateur | Indique le mode de gestion des modifications apportées par les utilisateurs, notamment si les modifications sont persistantes<br>Local : persistant. Les modifications apportées par les utilisateurs sont enregistrées localement.<br>Abandonner : non-persistant. Les modifications apportées par l'utilisateur sont abandonnées. |
| Type de connexion | Protocole utilisé pour la session, tel que HDX, RDP ou Console.<br>**Remarque :** le champ est laissé vide pour les sessions de console sur les VDA XenDesktop 5. |
| Type de provisioning | Indique la méthode de provisioning de la machine hébergeant la session<br>Manuel : non provisionné à l'aide de PVS ou MCS.<br>PVS : provisionné par PVS (machines physiques, lames et machines virtuelles).<br>MCS : provisionné par MCS (machines virtuelles uniquement). |
| Secure ICA actif | Indique si SecureICA est actif sur la session. |
| État de la session | État de la session. Valeurs possibles : Connecté, Actif ou Déconnecté. D'autres états peuvent se produire pour les sessions sur des machines dont les niveaux fonctionnels sont antérieurs à L7, tels que Préparation de la session, Reconnexion, Session non négociée par broker, Autre et Inconnu. |
| Heure de modification de la session | Heure de la modification d'état de la session la plus récente. |
| État de l'application | État des applications dans la session. Valeurs possibles : Avant connexion, Pré-démarré, Actif, Bureau, Persistance et Aucune application. |
| Support de session | Indique si la machine hébergeant la session prend en charge plusieurs sessions ou une seule session. |

| Colonne | Description |
| --- | --- |
| Zone | Nom de la zone où se trouve la machine hébergeant la session. |
| Filtres SmartAccess | Balises SmartAccess pour la session. |
| Heure de début (UTC) | Indique l'heure de début de la session. |
| État | État récapitulatif de la machine. Valeurs possibles : Non enregistré, Déconnecté ou En cours d'utilisation. |
| Dernière modification de l'état (UTC) | Indique depuis combien de temps la session se trouve dans son état actuel. |
| Delivery Controller | Nom d'hôte DNS du contrôleur auprès duquel la machine hébergeant la session est enregistrée. |
| Nom d'affichage de l'utilisateur | Nom complet de l'utilisateur. |
| Nom d'affichage du bureau | Nom publié de la machine initialement utilisée pour lancer la session. Il s'agit du nom affiché sur l'application Citrix Workspace ou StoreFront. Pour les sessions d'application, il s'agit du nom de la première application lancée dans la session, même si cette application a été fermée depuis. Le nom reste inchangé même si la ressource est renommée ou supprimée ultérieurement. |

## Gérer les clés de sécurité

June 27, 2024

> **Important :**
>
> - Vous devez utiliser cette fonctionnalité en conjonction avec StoreFront 1912 LTSR CU2 ou version ultérieure.
> - La fonctionnalité Secure XML n'est prise en charge que sur Citrix ADC et Citrix Gateway version 12.1 et versions ultérieures.
>
> **Remarque :**

> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Cette fonctionnalité vous permet d'autoriser uniquement les machines StoreFront et Citrix Gateway approuvées à communiquer avec des Delivery Controller. Une fois cette fonctionnalité activée, toutes les requêtes qui ne contiennent pas la clé sont bloquées. Utilisez cette fonctionnalité pour ajouter une couche de sécurité supplémentaire afin de vous protéger contre les attaques provenant du réseau interne.

Voici un flux de travail général pour utiliser cette fonctionnalité :

1. Activer Web Studio pour afficher les paramètres de fonctionnalités
2. Configurer les paramètres du site
3. Configurer les paramètres dans StoreFront
4. Configurer les paramètres dans Citrix ADC

### Activer Web Studio pour afficher les paramètres de fonctionnalités

Par défaut, les paramètres des clés de sécurité sont masqués dans Web Studio. Pour autoriser Web Studio à les afficher, utilisez le SDK PowerShell comme suit :

1. Exécutez le kit de développement logiciel SDK Citrix Virtual Apps and Desktops PowerShell.
2. Dans une fenêtre de commandes, exécutez les commandes suivantes :
    - `Add-PSSnapIn Citrix*`. Cette commande ajoute les composants logiciels enfichables Citrix.
    - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

Pour plus d'informations sur le SDK PowerShell, consultez SDK et API.

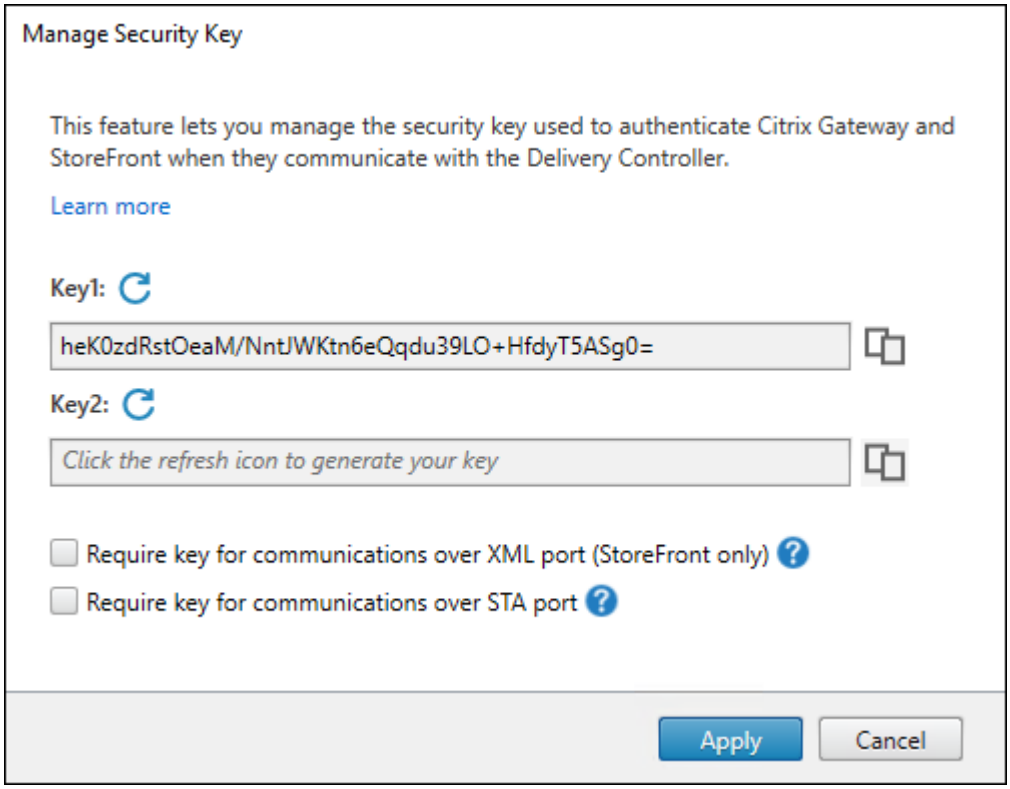
### Configurer les paramètres du site

Vous pouvez utiliser Web Studio ou PowerShell pour configurer les paramètres de clé de sécurité de votre site.

**Utiliser Web Studio**

1. Connectez-vous à Web Studio et sélectionnez **Paramètres** dans le volet de gauche.
2. Localisez la vignette **Gérer la clé de sécurité** et cliquez sur **Modifier**. La page **Gérer la clé de sécurité** s'affiche.




3. Cliquez sur l'icône d'actualisation pour générer les clés.

> **Important :**
>
> - Deux clés sont disponibles. Vous pouvez utiliser la même clé ou des clés différentes pour les communications via les ports XML et STA. Nous vous recommandons d'utiliser une seule clé à la fois. La clé inutilisée est utilisée uniquement pour la rotation de la clé.
> - Ne cliquez pas sur l'icône Actualiser pour mettre à jour la clé déjà utilisée. Si vous le faites, une interruption de service se produira.

4. Sélectionnez les instances où une clé est requise pour les communications :
   - **Exiger une clé pour les communications via le port XML (StoreFront uniquement)**. Si cette option est sélectionnée, une clé est requise pour authentifier les communications via le port XML. StoreFront communique avec Citrix Cloud via ce port. Pour plus d'informations sur la modification du port XML, consultez l'article Centre de connaissances CTX127945.

- **Exiger une clé pour les communications via le port STA**. Si cette option est sélectionnée, une clé est requise pour authentifier les communications via le port STA. Citrix Gateway et StoreFront communiquent avec Citrix Cloud via ce port. Pour plus d'informations sur la modification du port STA, consultez l'article Centre de connaissances CTX101988.

5. Cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

#### Utiliser PowerShell

Voici des étapes PowerShell équivalentes aux opérations Web Studio.

1. Exécutez le kit de développement logiciel distant SDK Citrix Virtual Apps and Desktops Remote PowerShell.
2. Dans une fenêtre de commandes, exécutez la commande suivante :
   - `Add-PSSnapIn Citrix*`
3. Exécutez les commandes suivantes pour générer une clé et configurer Key1 :
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Exécutez les commandes suivantes pour générer une clé et configurer Key2 :
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. Exécutez l'une des commandes suivantes ou les deux pour activer l'utilisation d'une clé dans l'authentification des communications :
   - Pour authentifier les communications via le port XML :
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - Pour authentifier les communications via le port STA :
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

Consultez l'aide de la commande PowerShell pour plus d'informations et la syntaxe.

### Configurer les paramètres dans StoreFront

Après avoir effectué la configuration de votre site, vous devez configurer les paramètres requis dans StoreFront à l'aide de PowerShell.

Sur le serveur StoreFront, exécutez les commandes PowerShell suivantes :

| | |
|---|---|
| Pour configurer la clé pour les communications via le port XML, utilisez la commande [Set-STFStoreFarm | https://developer-docs.citrix.com/fr-fr/storefront-powershell-sdk/current-release/Set-STFStoreFarm.html]. Par exemple |

```
$store = Get-STFStoreService -VirtualPath [Path to store]
$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
    name]
Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true -
    XMLValidationSecret [secret]
<!--NeedCopy-->
```

Entrez les valeurs appropriées pour les paramètres suivants :

- `Path to store`
- `Resource feed name`
- `secret`

Pour configurer la clé des communications via le port STA, utilisez les commandes `New-STFSecureTicketAuthority` et `Set-STFRoamingGateway`. Par exemple :

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]
$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL] -
    StaValidationEnabled $true -StaValidationSecret [secret]
$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL] -
    StaValidationEnabled $true -StaValidationSecret [secret]
Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
    $sta1,$sta2
<!--NeedCopy-->
```

Entrez les valeurs appropriées pour les paramètres suivants :

- `Gateway name`
- `STA URL`
- `Secret`

Consultez l'aide de la commande PowerShell pour plus d'informations et la syntaxe.

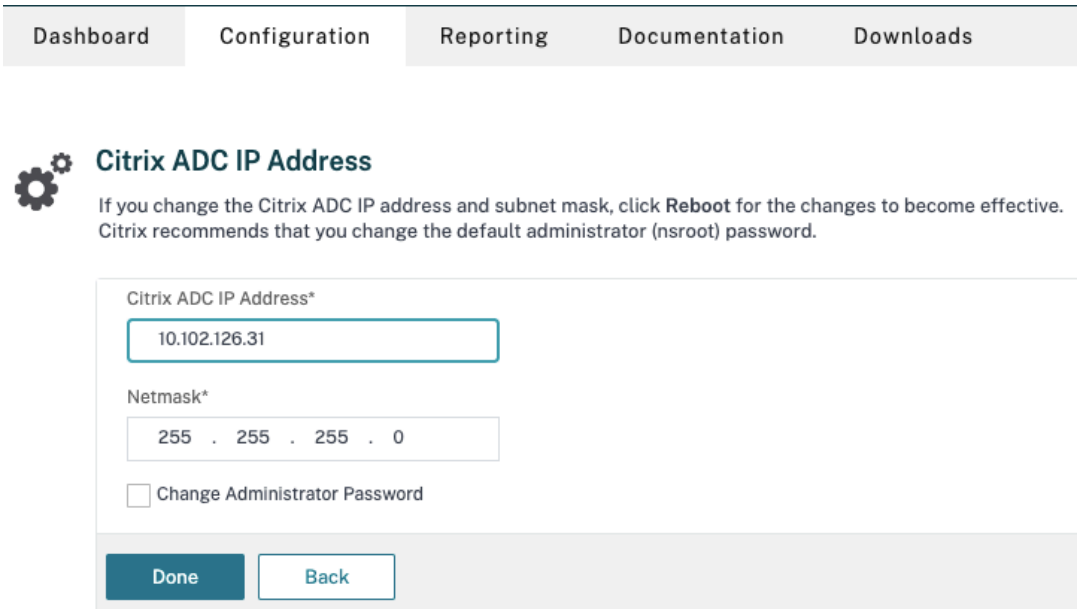
### Configurer les paramètres dans Citrix ADC

> **Remarque :**
>
> La configuration de cette fonctionnalité dans Citrix ADC n'est pas requise sauf si vous utilisez Citrix ADC comme passerelle. Si vous utilisez Citrix ADC, procédez comme suit :

1. Assurez-vous que la configuration préalable suivante est déjà en place :

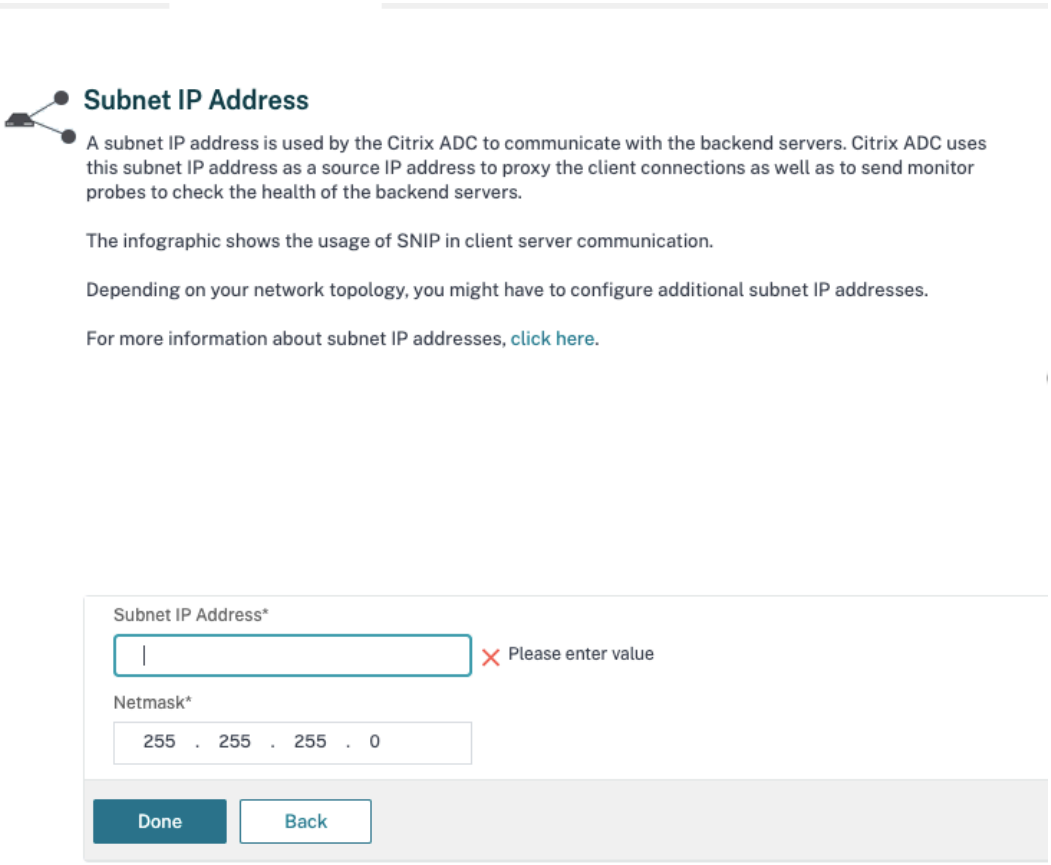
 

- Les adresses IP associées à Citrix ADC suivantes sont configurées.
  - Adresse IP Citrix ADC Management (NSIP) permettant d'accéder à la console Citrix ADC. Pour plus d'informations, consultez la section Configuration de l'adresse NSIP.



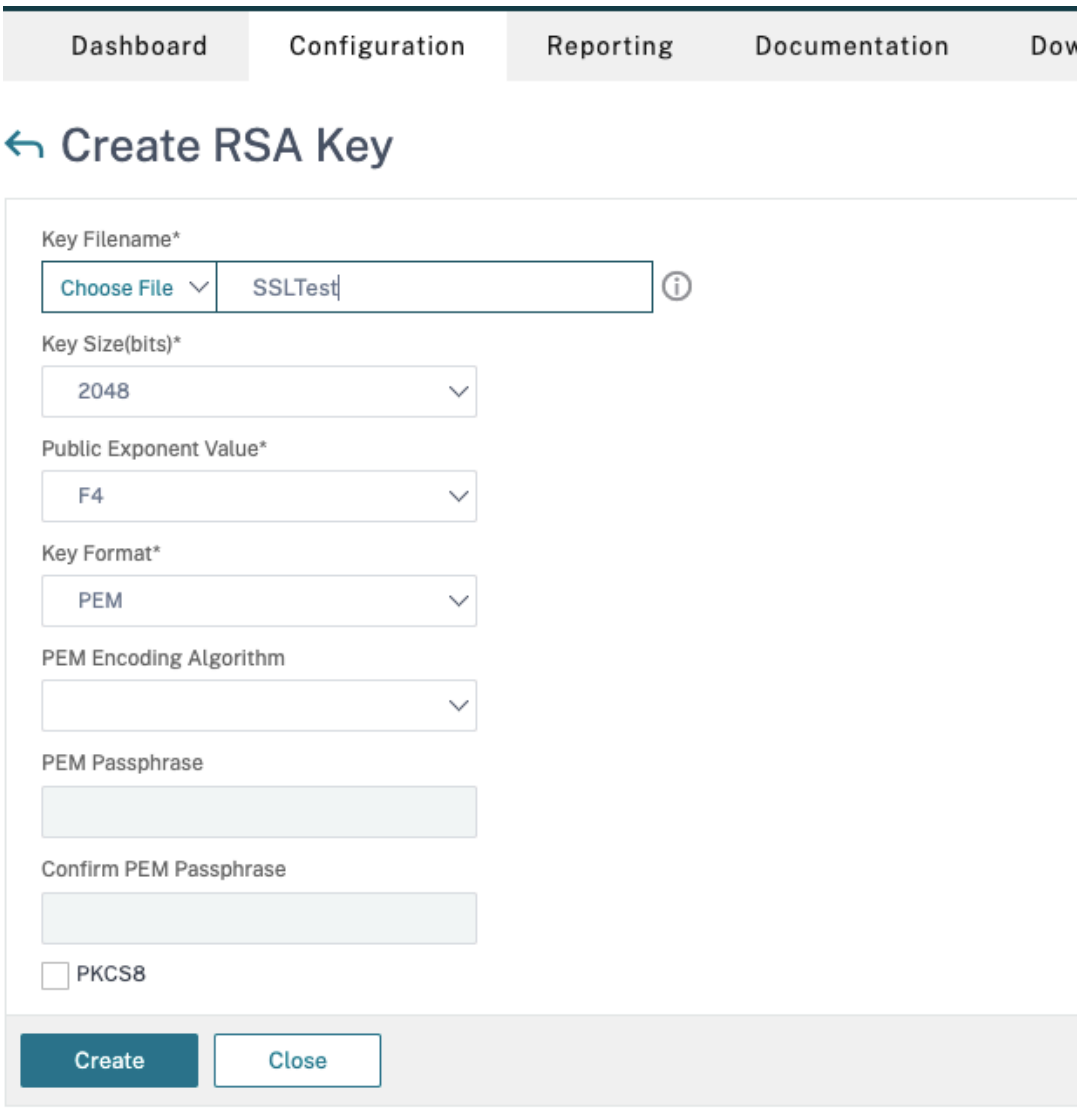

  - Adresse IP de sous-réseau (SNIP) permettant la communication entre l'appliance Citrix ADC et les serveurs principaux. Pour plus d'informations, consultez la section Configuration des adresses IP de sous-réseau.
  - Adresse IP virtuelle Citrix Gateway et adresse IP virtuelle de l'équilibreur de charge pour se connecter à l'appliance ADC pour le lancement de session. Pour plus d'informations, consultez la section Créer un serveur virtuel.



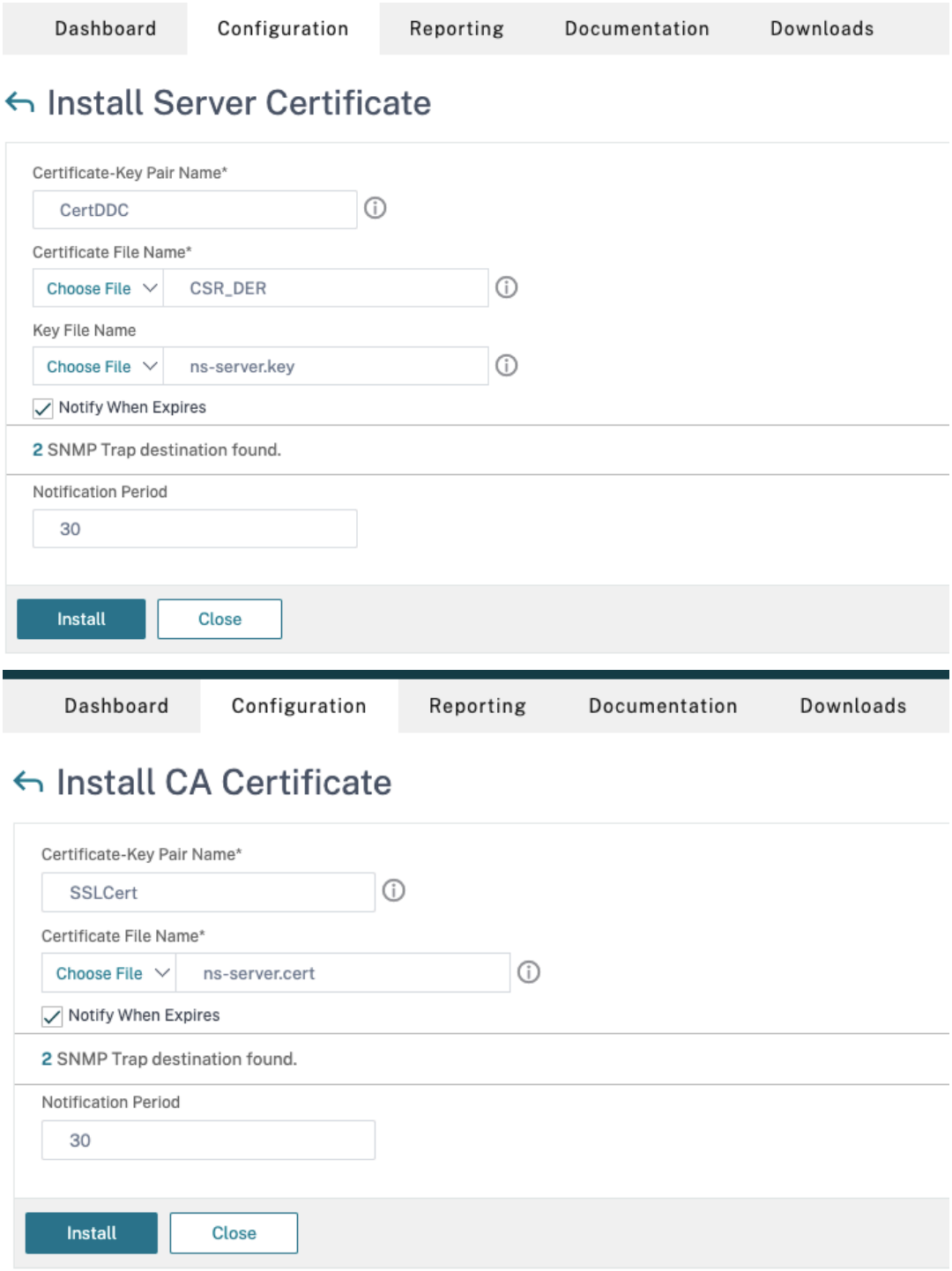

- Les modes et fonctionnalités requis dans l'appliance Citrix ADC sont activés.
  - Pour activer les modes, dans l'interface graphique Citrix ADC, accédez à **Système > Paramètres > Configurer mode**.
  - Pour activer les fonctionnalités, dans l'interface graphique Citrix ADC, accédez à **Système > Paramètres > Configurer fonctionnalités de base**.
- Les configurations liées aux certificats sont terminées.
  - La demande de signature de certificat (CSR) est créée. Pour plus d'informations, consultez la section Créer un certificat.



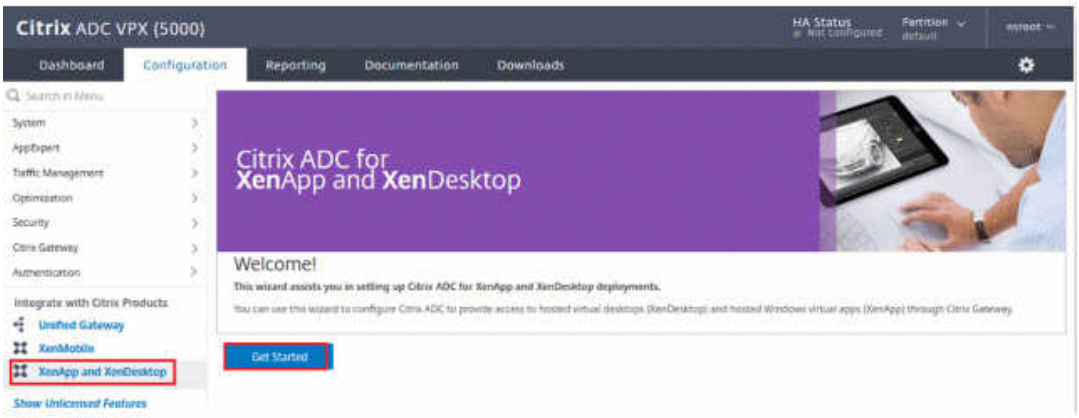

- Les certificats du serveur et de l'autorité de certification ainsi que les certificats racine sont installés. Pour plus d'informations, consultez la section Installer, lier et mettre à jour.




- Une instance de Citrix Gateway a été créée pour Citrix Virtual Desktops. Testez la connectivité en cliquant sur le bouton **Tester STA** pour vérifier que les serveurs virtuels sont en ligne. Pour plus d'informations, consultez la section Configuration de Citrix ADC pour Citrix Virtual Apps and Desktops.

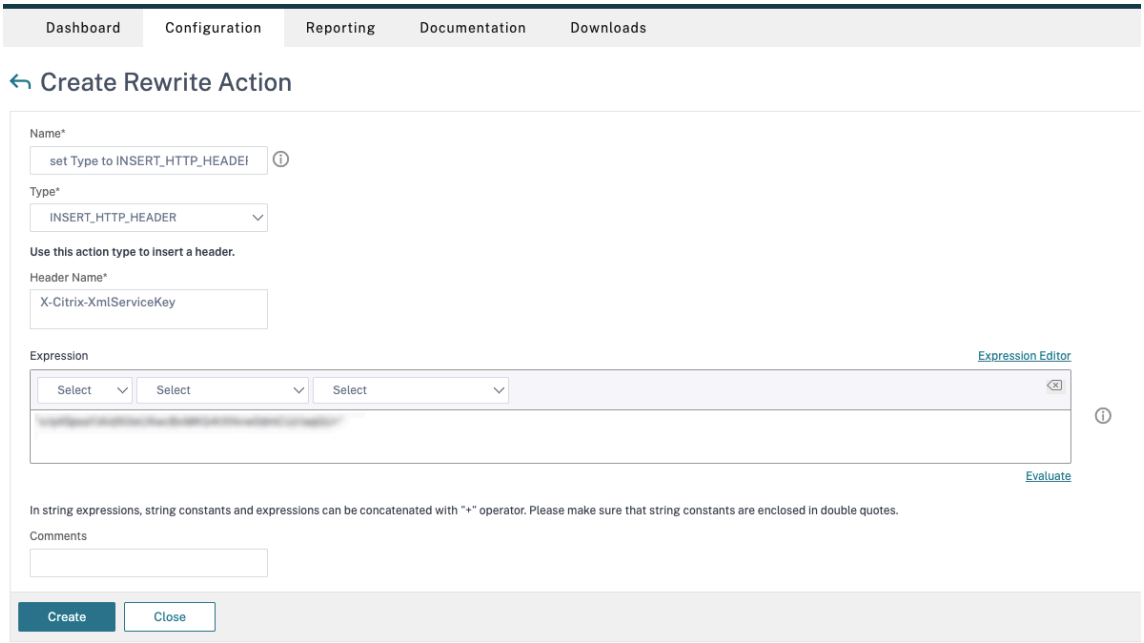
 




2. Ajoutez une action de réécriture. Pour plus d'informations, consultez la section Configuration d'une action de réécriture.

   a) Accédez à **AppExpert > Réécrire > Actions**.

   b) Cliquez sur **Add** pour ajouter une nouvelle action de réécriture. Vous pouvez nommer l'action « set Type to INSERT_HTTP_HEADER ».



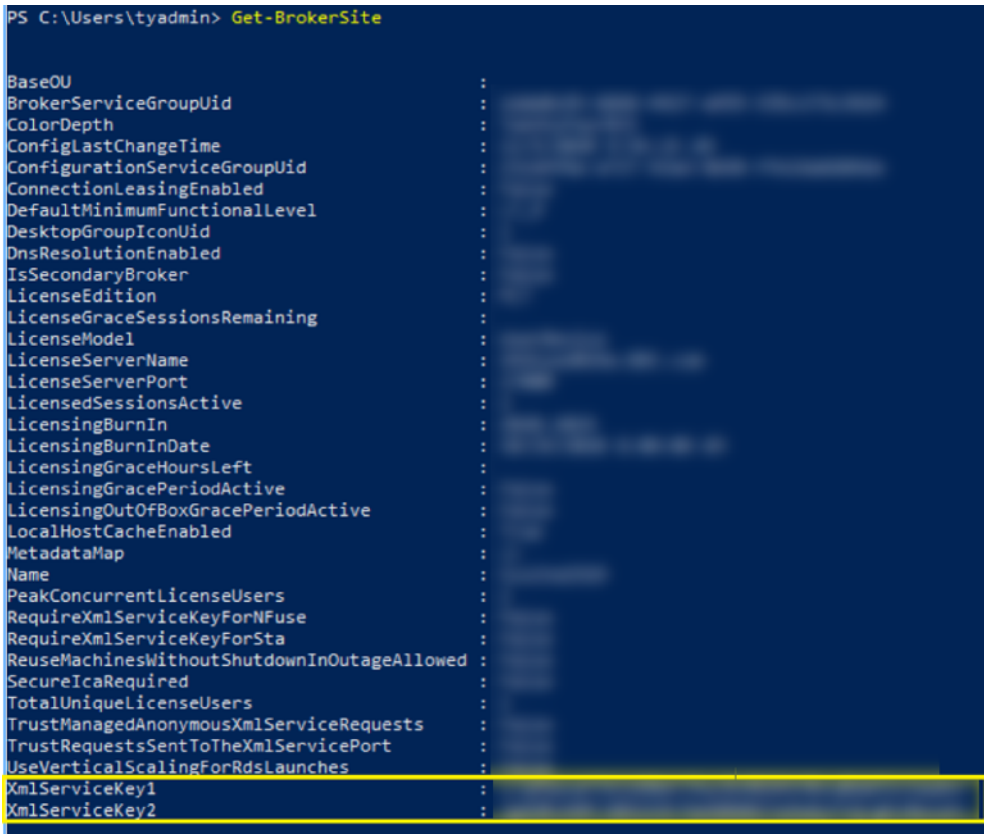

   a) Dans **Type**, sélectionnez **INSERT_HTTP_HEADER**.

   b) Dans **Header Name**, entrez X-Citrix-XmlServiceKey.

   c) Dans **Expression**, ajoutez <XmlServiceKey1 value> avec les guillemets. Vous pou-

vez copier la valeur XmlServiceKey1 à partir de votre configuration Desktop Delivery Controller.

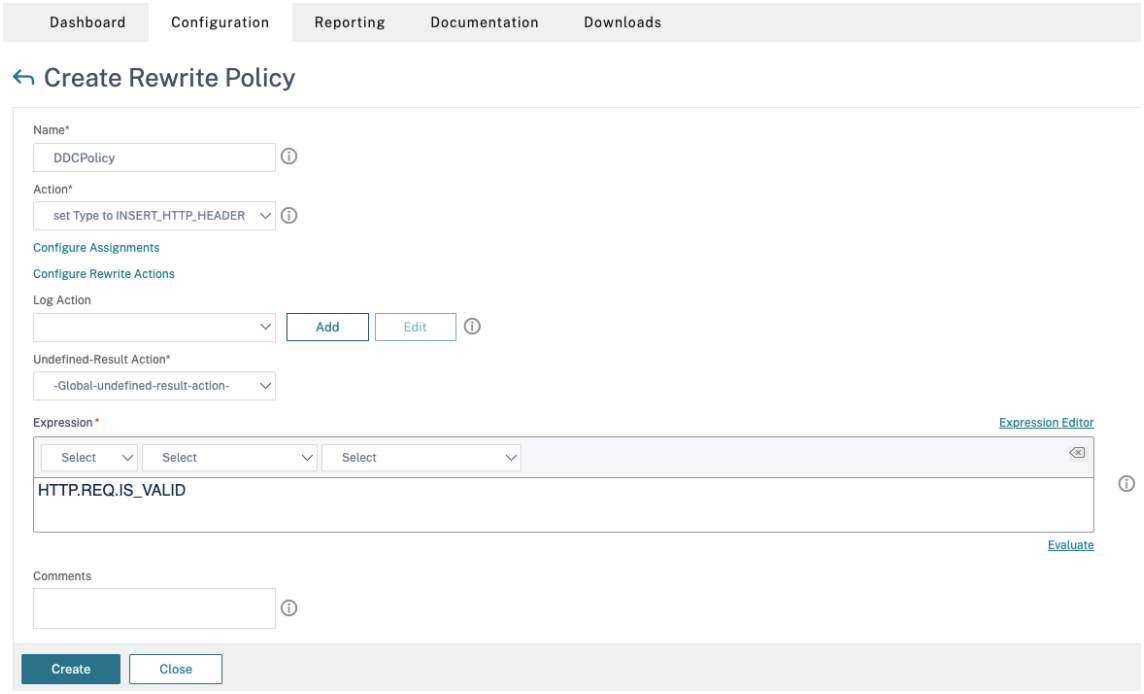



3. Ajoutez une stratégie de réécriture. Pour plus d'informations, consultez la section Configuration d'une stratégie de réécriture.

   a) Accédez à **AppExpert > Réécrire > Stratégies**.

   b) Cliquez sur **Add** pour ajouter une nouvelle stratégie.




a) Dans **Action**, sélectionnez l'action créée à l'étape précédente.
b) Dans **Expression**, ajoutez HTTP.REQ.IS_VALID.
c) Cliquez sur **OK**.

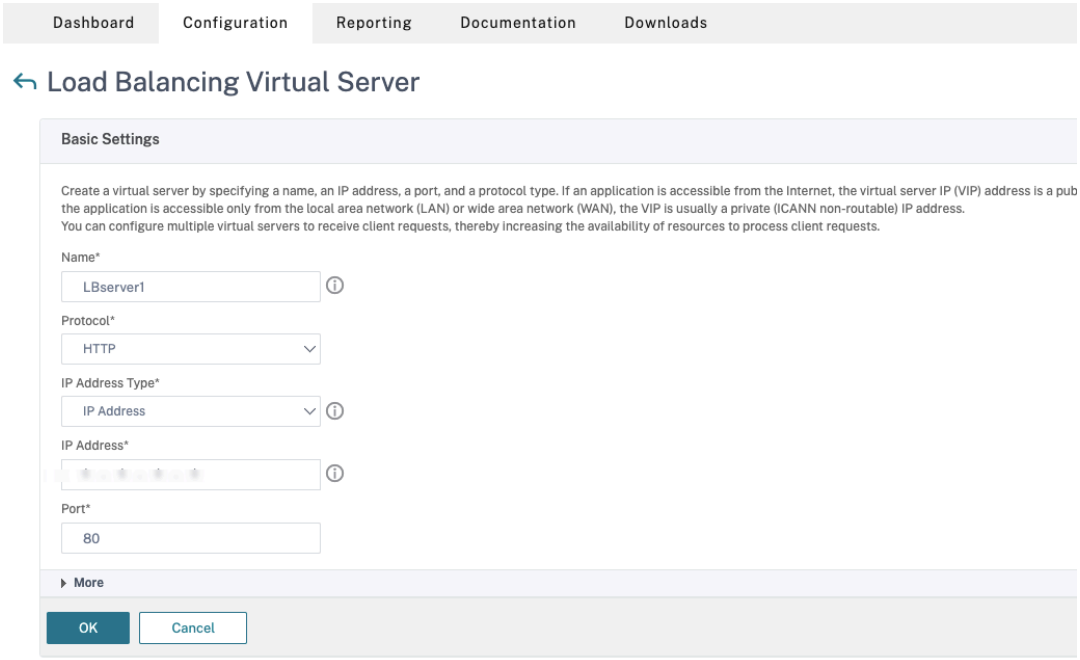
4. Configurez l'équilibrage de charge. Vous devez configurer un serveur virtuel d'équilibrage de charge par serveur STA. Sinon, les sessions ne parviennent pas à se lancer.

   Pour plus d'informations, consultez la section Configurer l'équilibrage de charge de base.

   a) Créez un serveur virtuel d'équilibrage de charge.

      - Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs**.
      - Dans la page **Virtual Servers**, cliquez sur **Add**.

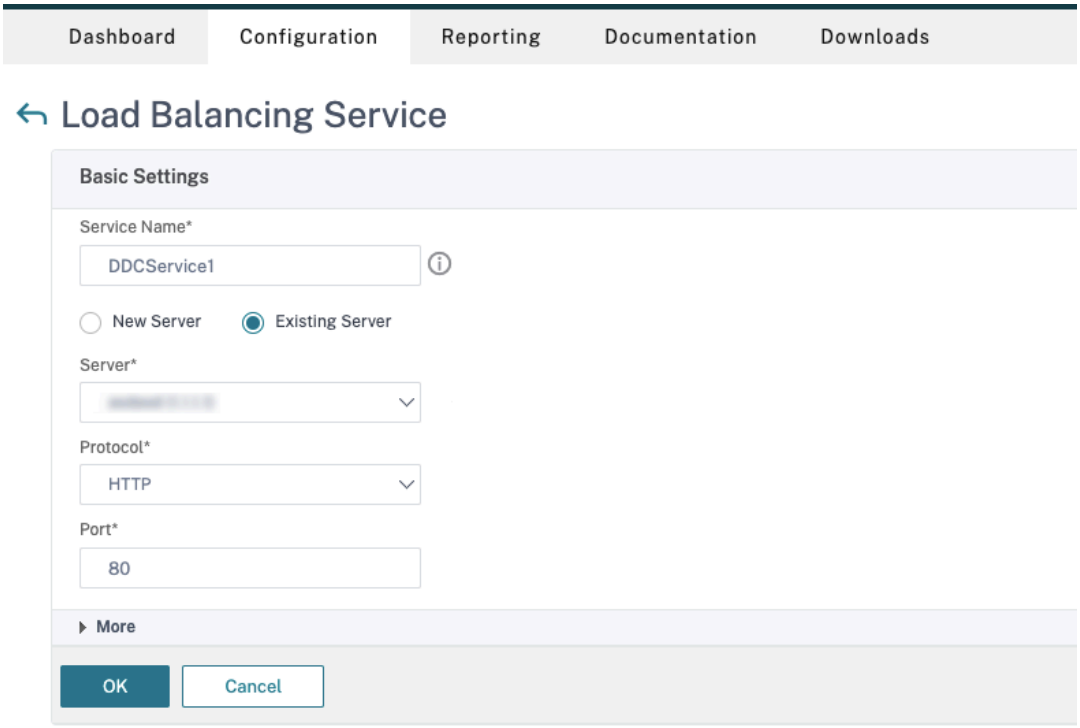
 




- Dans **Protocol**, sélectionnez **HTTP**.
- Ajoutez l'adresse IP virtuelle d'équilibrage de charge et sélectionnez **80** dans **Port**.
- Cliquez sur **OK**.

b) Créez un service d'équilibrage de charge.

- Accédez à **Gestion du trafic > Équilibrage de charge > Services**.

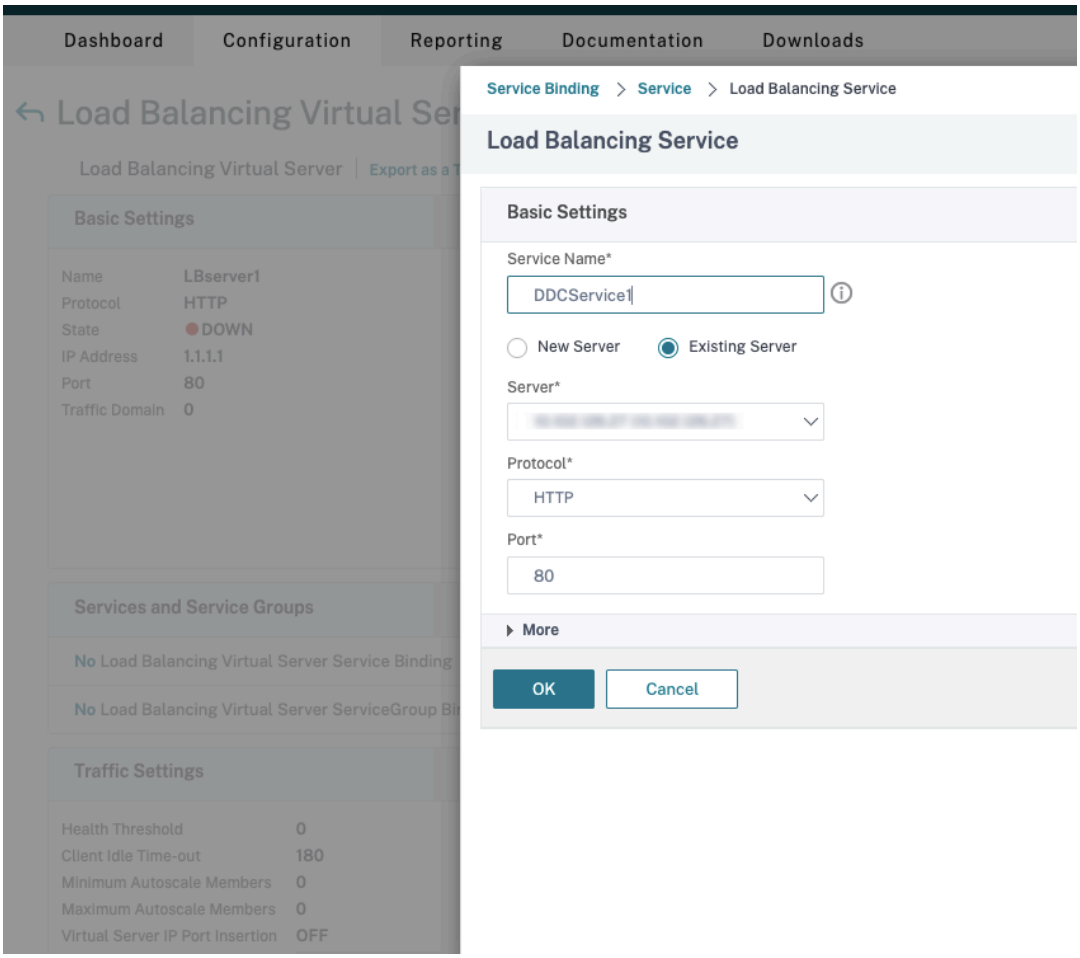


- Dans **Existing Server**, sélectionnez le serveur virtuel créé à l'étape précédente.
- Dans **Protocol**, sélectionnez **HTTP** et dans **Port**, sélectionnez **80**.
- Cliquez sur **OK**, puis cliquez sur **Done**.

c) Liez le service au serveur virtuel.

- Sélectionnez le serveur virtuel créé précédemment, puis cliquez sur **Edit**.
- Dans **Services and Service Groups**, cliquez sur **No Load Balancing Virtual Server Service Binding**.

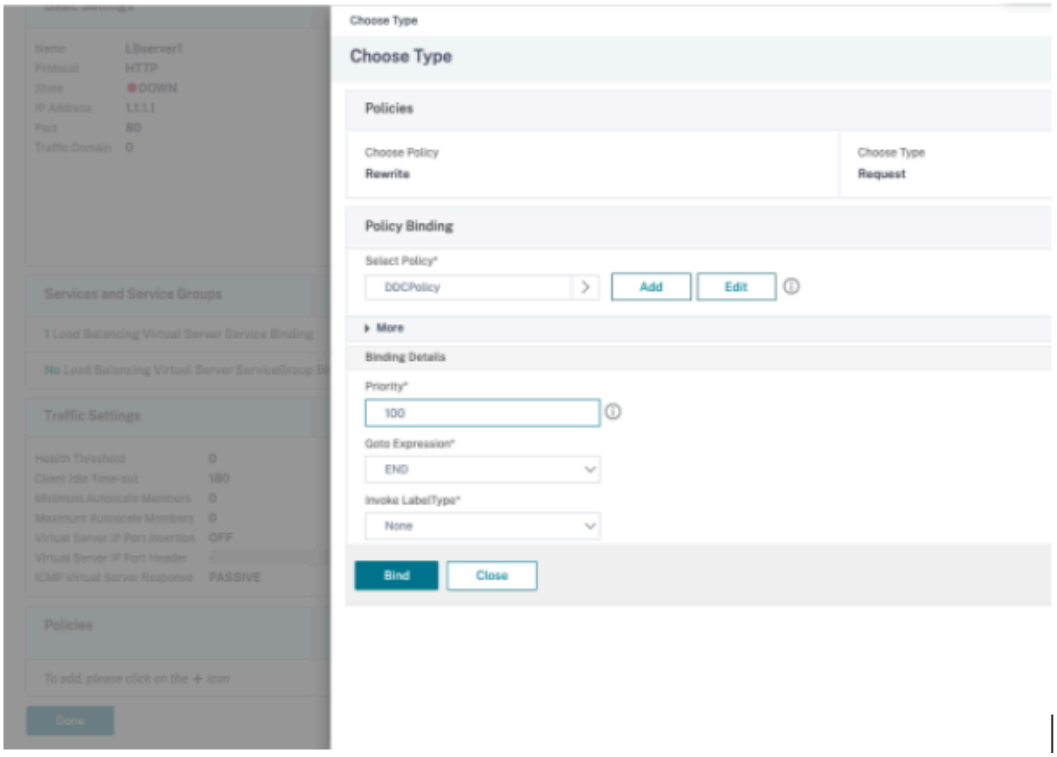



- Dans **Service Binding**, sélectionnez le service créé précédemment.
- Cliquez sur **Bind**.

d) Liez la stratégie de réécriture créée précédemment au serveur virtuel.

- Sélectionnez le serveur virtuel créé précédemment, puis cliquez sur **Edit**.
- Dans **Advanced Settings**, cliquez sur **Policies**, puis dans la section **Policies**, cliquez sur **+**.

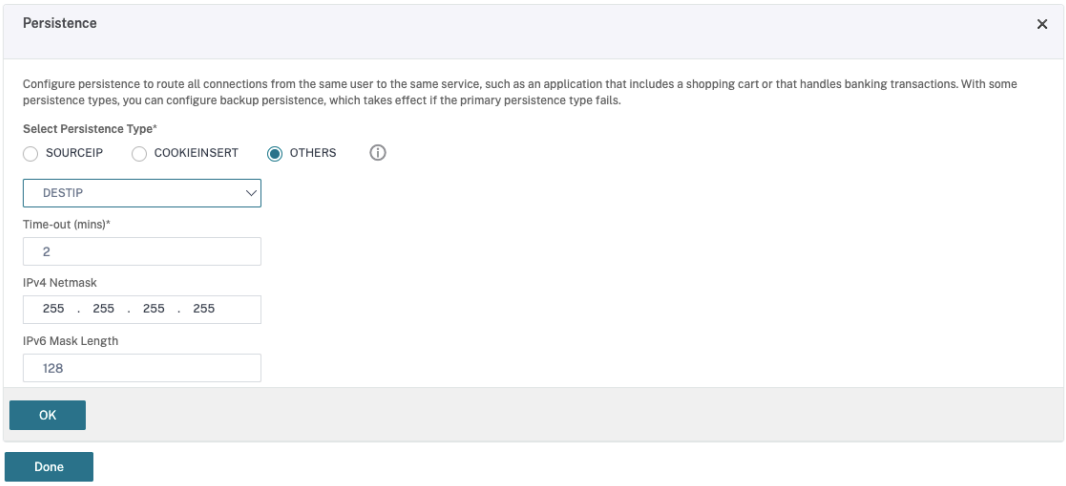
 




- Dans **Choose Policy**, sélectionnez **Rewrite** et, dans **Choose Type**, sélectionnez **Request**.
- Cliquez sur **Continuer**.
- Dans **Select Policy**, sélectionnez la stratégie de réécriture créée précédemment.
- Cliquez sur **Bind**.
- Cliquez sur **Terminé**.

e) Configurez la persistance du serveur virtuel, si nécessaire.

- Sélectionnez le serveur virtuel créé précédemment, puis cliquez sur **Edit**.
- Dans **Advanced Settings**, cliquez sur **Persistence**.



- Sélectionnez **Others** comme type de persistance.
- Sélectionnez **DESTIP** pour créer des sessions de persistance basées sur l'adresse IP du service sélectionné par le serveur virtuel (adresse IP de destination).
- Dans **IPv4 Netmask**, ajoutez un masque de réseau identique à celui du DDC.
- Cliquez sur **OK**.

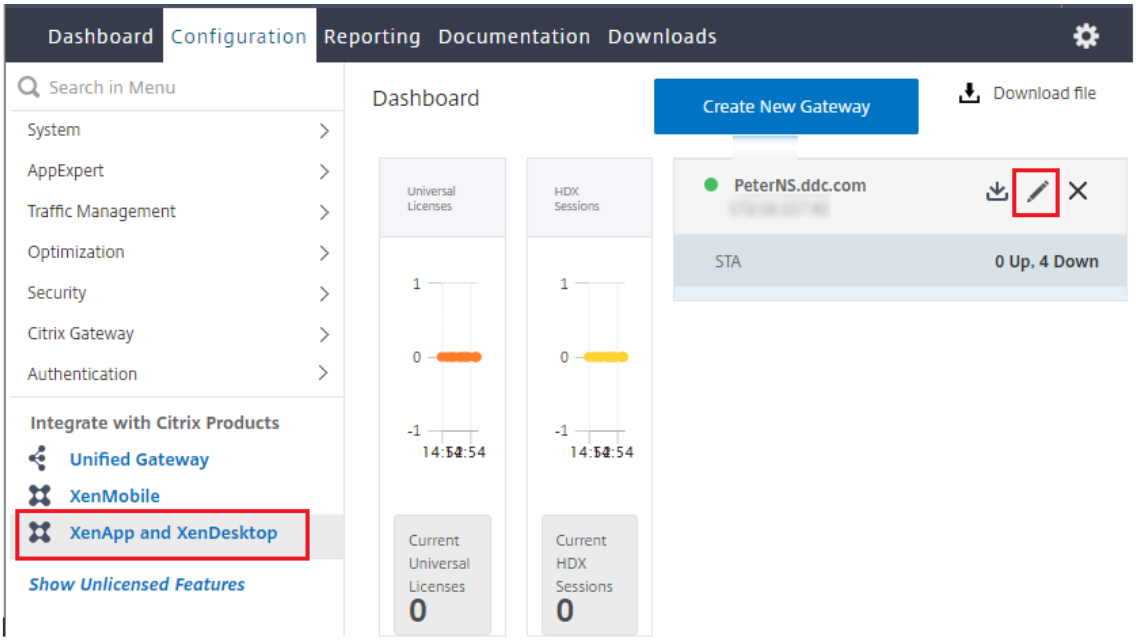
f) Répétez également ces étapes pour l'autre serveur virtuel.

**Modification de la configuration si l'appliance Citrix ADC est déjà configurée avec Citrix Virtual Desktops**

Si vous avez déjà configuré l'appliance Citrix ADC avec Citrix Virtual Desktops, pour utiliser la fonctionnalité Secure XML, vous devez apporter les modifications de configuration suivantes.

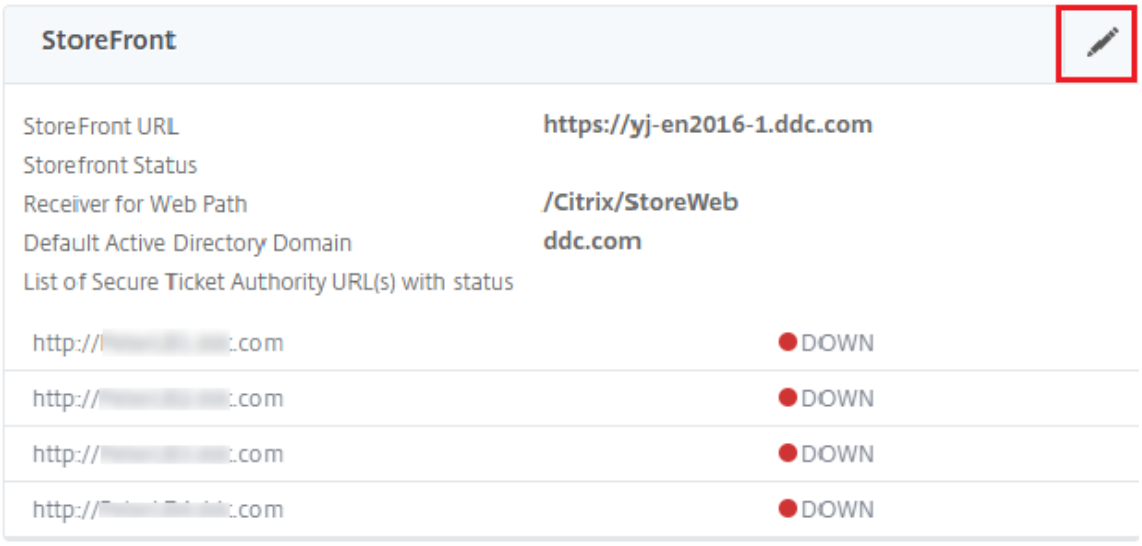
- Avant le lancement de la session, modifiez l'**URL Security Ticket Authority** de la passerelle pour utiliser les noms de domaine complets des serveurs virtuels d'équilibrage de charge.
- Assurez-vous que le paramètre `TrustRequestsSentToTheXmlServicePort` est défini sur False. Par défaut, le paramètre `TrustRequestsSentToTheXmlServicePort` est défini sur False. Toutefois, si le client a déjà configuré Citrix ADC pour Citrix Virtual Desktops, le paramètre `TrustRequestsSentToTheXmlServicePort` est défini sur True.

1. Dans l'interface graphique Citrix ADC, accédez à **Configuration > Intégrer aux produits Citrix**, puis cliquez sur **XenApp et XenDesktop**.
2. Sélectionnez l'instance de passerelle et cliquez sur l'icône de modification.




3. Dans le volet StoreFront, cliquez sur l'icône de modification.

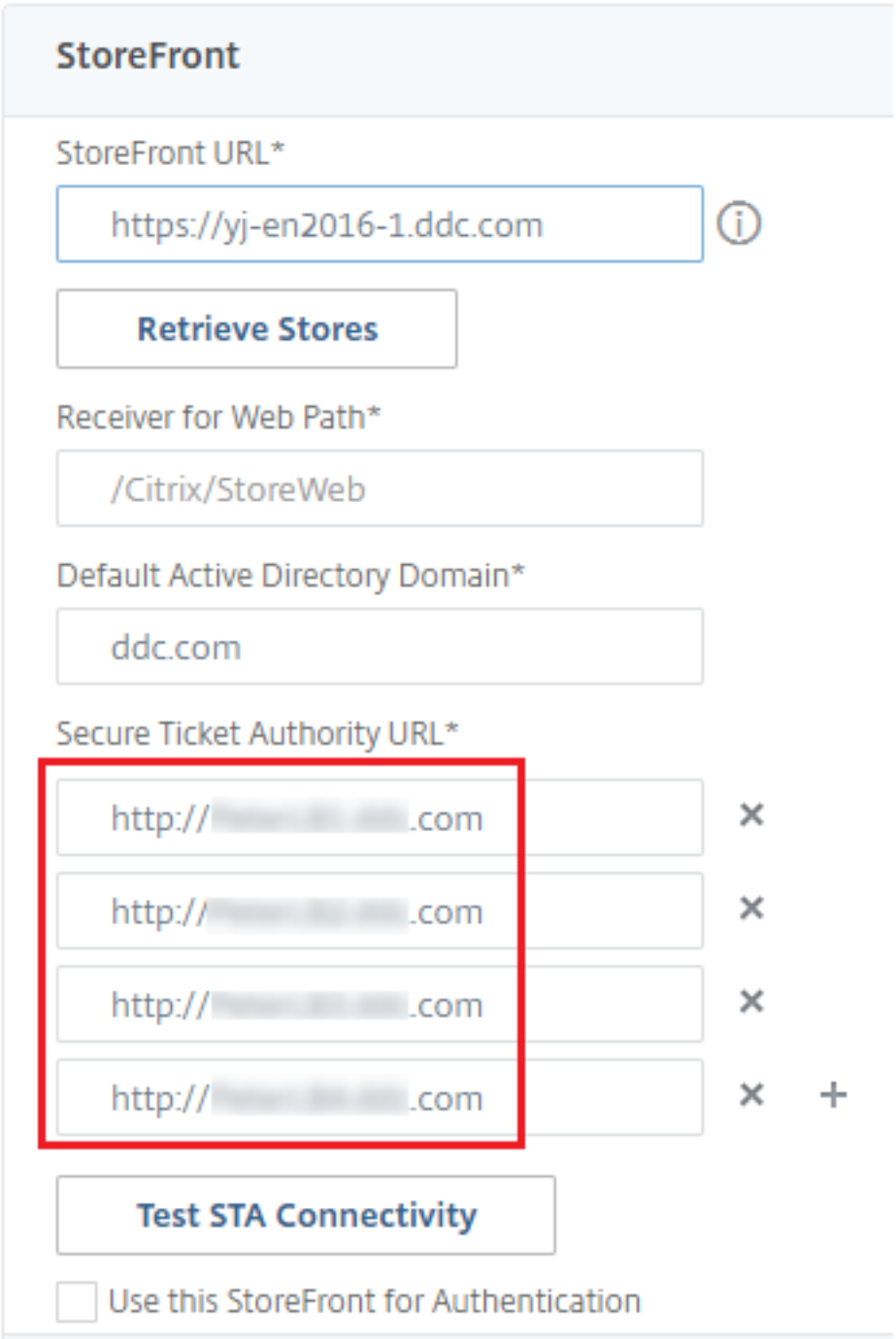
 




4. Ajoutez l'**URL Secure Ticket Authority**.

   - Si la fonctionnalité Secure XML est activée, l'URL STA doit être l'URL du service d'équilibrage de charge.
   - Si la fonctionnalité Secure XML est désactivée, l'URL STA doit être l'URL de STA (adresse du DDC) et le paramètre TrustRequestsSentToTheXmlServicePort sur le DDC doit être défini sur True.




## Paramètres de résilience des sessions

June 27, 2024

La gestion de l'activité de session est critique pour offrir la meilleure expérience utilisateur possible.

La perte de connectivité due à des réseaux non fiables, à des durées de latence réseau extrêmement variables ou à des limitations en termes de portée des appareils sans fil, peuvent faire naître une certaine frustration chez les utilisateurs. Le passage rapide d'un appareil à l'autre et l'accès aux mêmes applications à chaque ouverture de session est une priorité pour de nombreux travailleurs mobiles, tels que les professionnels de la santé.

Les fonctionnalités décrites dans cet article optimisent la fiabilité des sessions, réduire les désagréments, les temps d'arrêt et la perte de productivité ; à l'aide de ces fonctionnalités, les utilisateurs mobiles peuvent passer rapidement et facilement d'un périphérique à un autre.

## Fiabilité de session

La fiabilité de session maintient les sessions actives sur l'écran de l'utilisateur lorsque la connectivité au réseau est interrompue. L'utilisateur peut donc visualiser l'application jusqu'à ce que la connexion au réseau reprenne.

Cette fonction est particulièrement utile pour les utilisateurs mobiles utilisant des connexions sans fil. Par exemple, lorsqu'un utilisateur connecté via une connexion sans fil entre dans un tunnel ferroviaire, la connexion est momentanément interrompue. D'ordinaire, la session se déconnecte et disparaît de l'écran de l'utilisateur ; ce dernier est alors contraint de se reconnecter à la session déconnectée. Grâce à la fiabilité de session, la session reste active sur la machine. Pour indiquer que la connexion est interrompue, l'affichage fourni à l'utilisateur est figé et le curseur prend la forme d'un sablier jusqu'à ce que la connexion soit rétablie de l'autre côté du tunnel. L'utilisateur a toujours accès à l'affichage de l'application durant l'interruption et peut reprendre l'interaction avec l'application lorsque la connexion réseau est rétablie. La fonction de fiabilité de session permet aux utilisateurs de se reconnecter sans avoir à s'authentifier de nouveau.

Les utilisateurs de l'application Citrix Workspace ne peuvent pas remplacer le paramètre du Controller.

Vous pouvez utiliser la fonction de fiabilité de session avec le protocole TLS (Transport Layer Security). TLS crypte uniquement les données envoyées entre la machine utilisateur et Citrix Gateway.

Activez et configurez la fonction de fiabilité de session avec les paramètres de stratégie suivants :

- Le paramètre de stratégie Connexions de fiabilité de session autorise ou interdit la fiabilité de session.
- Le paramètre de stratégie Expiration de délai de la fiabilité de session est réglé par défaut sur 180 secondes, ou trois minutes. Même si vous pouvez étendre la durée pendant laquelle la fonction de fiabilité de session maintient une session ouverte, cette fonctionnalité est conçue pour aider l'utilisateur et le but de cette fonctionnalité est d'éviter à l'utilisateur de devoir s'authentifier à nouveau. Si vous augmentez la durée pendant laquelle une session reste ouverte, vous augmentez le risque qu'un utilisateur distrait s'éloigne de sa machine cliente. Il est alors possible

que des utilisateurs non autorisés accèdent à sa session.
- Les connexions entrantes de fiabilité de session utilisent le port 2598, à moins que vous ne changiez le numéro de port défini dans le paramètre de stratégie Numéro de port de la fiabilité de session.
- Pour empêcher les utilisateurs de se reconnecter à des sessions interrompues sans avoir à se réauthentifier, utilisez la fonction Reconnexion automatique des clients. Vous pouvez configurer le paramètre de stratégie Authentification de la reconnexion automatique des clients pour inviter les utilisateurs à s'authentifier à nouveau lors de la reconnexion aux sessions interrompues.

Si vous utilisez la fonction de fiabilité de session et la fonction de reconnexion automatique des clients, ces fonctions agissent l'une après l'autre. La fonction de fiabilité de session ferme (ou déconnecte) la session utilisateur après la période spécifiée dans le paramètre de stratégie Expiration de délai de la fiabilité de session. Ensuite, les paramètres définis pour la fonction de reconnexion automatique des clients s'appliquent et la fonction tente d'opérer la reconnexion de l'utilisateur à la session déconnectée.

### Reconnexion automatique des clients

Avec la fonction Reconnexion automatique des clients, l'application Citrix Workspace peut détecter les déconnexions de session ICA involontaires et reconnecter automatiquement les utilisateurs à leurs sessions. Lorsque cette fonctionnalité est activée sur le serveur, les utilisateurs n'ont pas besoin de se reconnecter manuellement pour continuer à travailler.

Pour les sessions d'application, l'application Citrix Workspace essaie de se reconnecter à la session jusqu'à ce que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion.

Pour les sessions de bureau, l'application Citrix Workspace tente de se reconnecter à la session pendant une période de temps spécifiée, à moins que la reconnexion réussisse ou que l'utilisateur annule la tentative de reconnexion. Par défaut, cette durée est de cinq minutes. Pour modifier cette période, modifiez le paramètre de registre suivant sur la machine utilisateur (où `seconds` est le nombre de secondes après lesquelles aucune tentative de reconnexion de la session n'est effectuée).

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

Activez et configurez la fonction de reconnexion automatique des clients avec les paramètres de stratégie suivants :

- **Reconnexion automatique des clients :** active ou désactive la reconnexion automatique par l'application Citrix Workspace après l'interruption d'une connexion.
- **Authentification de la reconnexion automatique des clients :** active ou désactive l'authentification utilisateur après la reconnexion automatique.

- **Journalisation de la reconnexion automatique des clients :** active ou désactive la journalisation des événements de reconnexion dans le journal d'événements. Par défaut, la journalisation est désactivée. Lorsqu'il est activé, le Journal système du ou des serveurs reçoit les informations relatives aux échecs et aux succès des tentatives de reconnexion automatique. Chaque serveur stocke des informations sur les événements de reconnexion dans son propre journal système. Le site ne fournit pas de journal combinant les événements de reconnexion de tous les serveurs.

> **Remarque :**
>
> La reconnexion automatique des clients sans réauthentification n'est prise en charge que pour l'authentification par mot de passe. Si vous utilisez le service d'authentification fédérée ou l'authentification par carte à puce, la reconnexion automatique des clients sans réauthentification n'est pas prise en charge. Dans ce cas, les utilisateurs sont redirigés vers l'écran de connexion.

La fonction de reconnexion automatique des clients intègre un mécanisme permettant une authentification basée sur les informations d'identification cryptées de l'utilisateur. Lorsqu'un utilisateur ouvre une session initiale, le serveur crypte et stocke les informations d'identification de l'utilisateur en mémoire. Le serveur crée et envoie un cookie contenant la clé de cryptage à l'application Citrix Workspace. L'application Citrix Workspace transmet la clé au serveur pour reconnexion. Celui-ci décrypte les informations d'identification et les transmet au système d'ouverture de session Windows pour authentification. Lorsqu'un cookie expire, l'utilisateur doit à nouveau fournir ses informations d'identification pour se reconnecter à sa session.

Si le paramètre Authentification de la reconnexion automatique des clients est sélectionné, aucun cookie n'est utilisé. Au lieu de cela, les utilisateurs voient s'afficher une boîte de dialogue leur demandant de fournir leurs informations d'identification lorsque l'application Citrix Workspace tente de se reconnecter automatiquement.

Pour une protection optimale des informations d'identification et des sessions des utilisateurs, utilisez le cryptage pour toutes les communications entre les clients et le site.

Désactivez la reconnexion automatique des clients sur l'application Citrix Workspace pour Windows en utilisant le fichier icaclient.adm. Pour de plus amples informations, consultez la documentation relative à votre version de l'application Citrix Workspace pour Windows.

Les paramètres des connexions affectent également la fonction de reconnexion automatique des clients.

- Par défaut, la fonction Reconnexion automatique des clients est activée via les paramètres de stratégie au niveau du site, comme décrit ci-dessus. Les utilisateurs n'ont pas besoin de se réauthentifier. Toutefois, si la connexion TCP ICA d'un serveur est configurée pour réinitialiser les sessions dont une liaison de communication a été interrompue, la reconnexion automatique n'a pas lieu. La fonction de reconnexion automatique des clients fonctionne uniquement si le

serveur déconnecte les sessions en cas d'interruption ou d'expiration de délai d'une connexion. Dans ce contexte, la connexion TCP ICA fait référence au port virtuel d'un serveur (et non à une connexion réseau) utilisé pour les sessions sur les réseaux TCP/IP.

- Par défaut, la connexion TCP ICA d'un serveur est configurée pour déconnecter les sessions en cas d'interruption ou d'expiration de délai de leurs connexions. Les sessions déconnectées restent intactes dans la mémoire du système et sont disponibles pour la reconnexion par l'application Citrix Workspace
- La connexion peut être configurée pour réinitialiser ou fermer les sessions dont les connexions sont interrompues ou dont le délai a expiré. Lorsqu'une session est réinitialisée, la tentative de reconnexion initie une nouvelle session. L'utilisateur ne retrouve pas l'application dans l'état où elle était avant la reconnexion ; l'application est relancée.
- Si le serveur est configuré pour réinitialiser les sessions, la fonction de reconnexion automatique des clients crée une nouvelle session. Ce processus nécessite que les utilisateurs fournissent leurs informations d'identification pour ouvrir une session sur le serveur.
- La reconnexion automatique peut échouer si l'application Citrix Workspace ou le plug-in transmettent des informations d'identification incorrectes, ce qui peut se produire lors d'une attaque, ou si le serveur estime qu'une durée trop longue s'est écoulée depuis qu'il a détecté une connexion interrompue.

### Persistance ICA

L'activation de la fonctionnalité de persistance ICA empêche la déconnexion des connexions rompues. Lorsque cette option est activée, si le serveur ne détecte aucune activité, cette fonctionnalité empêche les Services Bureau à distance de déconnecter cette session. Les exemples d'absence d'activité incluent aucun changement d'horloge, aucun mouvement de la souris, aucune mise à jour de l'écran. Le serveur envoie des paquets de persistance à quelques secondes d'intervalle pour détecter si la session est active. Si la session n'est plus active, le serveur marque la session en tant que déconnectée.

> **Important :**
>
> Cependant, la persistance ICA fonctionne uniquement si vous n'utilisez pas la fiabilité de session. La fiabilité de session dispose de ses propres mécanismes pour empêcher les connexions interrompues d'être déconnectées. Ne configurez la persistance ICA que pour les connexions qui n'utilisent pas la fiabilité de session.

Les réglages effectués dans la page Persistance ICA ont priorité sur les réglages correspondants configurés dans la Stratégie de groupe Windows.

Activez et configurez les paramètres de persistance ICA avec les paramètres de stratégie suivants :

- **Délai d'expiration de persistance ICA :** spécifie l'intervalle (1-3600 secondes) utilisé pour envoyer des messages de persistance ICA. Ne configurez pas cette option si vous voulez que votre

logiciel de contrôle de réseau ferme les connexions inactives dans les environnements pour lesquels les interruptions de connexion sont si peu fréquentes que la reconnexion des utilisateurs aux sessions n'est pas un problème.

L'intervalle par défaut est de 60 secondes : les paquets de persistance ICA sont envoyés aux machines utilisateur toutes les 60 secondes. Si une machine utilisateur ne répond pas après 60 secondes, l'état des sessions ICA correspondantes passe à Déconnectée.

- **Persistances ICA :** envoie ou empêche l'envoi de messages de persistance ICA.

### Contrôle de l'espace de travail

Le contrôle de l'espace de travail permet aux bureaux et aux applications de suivre un utilisateur d'un appareil à un autre. Cette itinérance permet à un utilisateur d'accéder à tous les bureaux ou d'ouvrir des applications à partir de n'importe quel emplacement simplement en ouvrant une session, sans avoir à redémarrer les bureaux ou applications sur chaque machine. Par exemple, le contrôle de l'espace de travail permet aux employés d'un centre hospitalier de se déconnecter rapidement d'une station de travail pour se reconnecter à une autre et d'accéder aux mêmes applications chaque fois qu'ils ouvrent une session. Si vous configurez le contrôle de l'espace de travail de la sorte, le personnel médical peut se déconnecter de plusieurs applications sur une machine cliente et s'y reconnecter sur une autre machine cliente.

Le contrôle de l'espace de travail affecte les activités suivantes :

- **Ouverture de session :** par défaut, le contrôle de l'espace de travail permet aux utilisateurs de se reconnecter automatiquement à tous les bureaux et applications en cours d'exécution lors de l'ouverture de session, sans avoir à les rouvrir manuellement. Via le contrôle de l'espace de travail, les utilisateurs peuvent ouvrir des bureaux ou applications déconnectés ainsi que des applications ou bureaux qui sont actifs sur une autre machine cliente. La déconnexion d'une application ou d'un bureau n'interrompt pas son exécution sur le serveur. Si des utilisateurs itinérants doivent maintenir la connexion avec certaines applications ou certains bureaux sur une machine cliente tandis qu'ils se reconnectent à d'autres applications ou bureaux sur une autre machine cliente, vous pouvez configurer le comportement de reconnexion de façon à n'ouvrir que les applications ou bureaux dont ils se sont déconnectés.
- **Reconnexion :** après avoir ouvert une session sur le serveur, les utilisateurs peuvent se reconnecter à tous leurs bureaux ou applications à tout moment en cliquant sur le bouton Se reconnecter. Par défaut, cette option ouvre les applications et bureaux qui sont déconnectés ainsi que ceux actuellement exécutés sur une autre machine cliente. Vous pouvez configurer cette option de façon à ce qu'elle n'ouvre que les applications ou bureaux précédemment déconnectés par l'utilisateur.
- **Fermeture de session :** pour les utilisateurs ouvrant des bureaux ou applications via StoreFront, vous pouvez configurer la commande **Fermer la session** afin de fermer la session utilisa-

teur de StoreFront ainsi que toutes les sessions actives ou uniquement la session de StoreFront.

- **Déconnexion :** les utilisateurs peuvent se déconnecter simultanément de toutes les applications et tous les bureaux en cours d'exécution sans avoir à déconnecter chaque application ou bureau individuellement.

Le contrôle de l'espace de travail est disponible uniquement pour les utilisateurs de l'application Citrix Workspace pour accéder aux bureaux et applications via une connexion Citrix StoreFront. Par défaut, le contrôle de l'espace de travail est désactivé pour les sessions de bureau virtuel, mais activé pour les applications hébergées. Le partage de session ne se produit pas par défaut entre les bureaux publiés et toute application publiée exécutée au sein de ces bureaux.

Lorsqu'un utilisateur passe à une nouvelle machine cliente, les stratégies utilisateur, les mappages des lecteurs clients et la configuration des imprimantes changent en conséquence. Les stratégies et les mappages sont appliqués en fonction de la machine cliente à partir de laquelle l'utilisateur a ouvert la session. Par exemple, un membre du personnel se déconnecte d'un appareil dans la salle d'urgence, puis se connecte à un poste de travail du laboratoire de radiographie. Les stratégies, les mappages d'imprimante et les mappages de lecteur client appropriés pour la session dans le laboratoire de radiographie sont mis en œuvre au démarrage.

Vous pouvez personnaliser les imprimantes qui s'affichent pour les utilisateurs lorsqu'ils changent d'emplacement. Vous pouvez également contrôler si les utilisateurs peuvent imprimer sur des imprimantes locales, la quantité de bande passante consommée lorsque les utilisateurs se connectent à distance, ainsi que d'autres aspects de leur expérience d'impression.

Pour plus d'informations sur l'activation et la configuration du contrôle de l'espace de travail pour les utilisateurs, consultez la documentation StoreFront.

### Itinérance de session

> **Remarque :**
>
> Les informations suivantes vous aident à configurer l'itinérance de session à l'aide de PowerShell. Vous pouvez utiliser Web Studio à la place. Pour de plus amples informations, consultez la section Gérer les groupes de mise à disposition.

Par défaut, les sessions sont partagées entre les machines clientes de l'utilisateur. Lorsque l'utilisateur ouvre une session et bascule sur une autre machine, la même session est utilisée et les applications sont disponibles sur les deux machines. Les applications suivent, quelle que soit la machine ou que les sessions en cours existent ou non. Souvent, les imprimantes et les autres ressources attribuées à l'application suivent également.

Bien que ce comportement par défaut offre de nombreux avantages, il n'est pas toujours idéal. Vous pouvez désactiver l'itinérance de session à l'aide du SDK du PowerShell.

Exemple 1 : un professionnel de la santé utilise deux machines ; il remplit un formulaire d'assurance sur un PC de bureau et recherche des informations sur le patient sur une tablette.

- Si l'itinérance de session est activée, les applications s'affichent toutes les deux sur les deux machines (une application lancée sur une machine est visible sur toutes les machines en cours d'utilisation). Ce comportement peut ne pas répondre aux exigences de sécurité.
- Si l'itinérance de session est désactivée, le dossier du patient ne s'affiche pas sur le PC de bureau et le formulaire d'assurance ne s'affiche pas sur la tablette.

Exemple 2 : un chef de production lance une application sur le PC de son bureau. Le nom et l'emplacement de la machine déterminent les imprimantes et autres ressources qui sont disponibles pour cette session. Plus tard dans la journée, il se rend dans un bureau situé dans un autre bâtiment pour une réunion pour laquelle il devra utiliser une imprimante.

- Si l'itinérance de session est activée, le chef de production ne peut probablement pas accéder aux imprimantes à proximité de la salle de réunion, car les applications qu'il a démarrées plus tôt dans son bureau ont entraîné l'attribution d'imprimantes et d'autres ressources situées près de cet emplacement.
- Si l'itinérance de session est désactivée, lorsqu'il ouvre une session sur une autre machine (en utilisant les mêmes informations d'identification), une nouvelle session est démarrée et les imprimantes et ressources à proximité sont disponibles.

#### Configurer l'itinérance de session

Pour configurer l'itinérance de session, utilisez les applets de commande de règle de stratégie d'admissibilité suivantes avec la propriété « SessionReconnection ». Facultativement, vous pouvez également spécifier la propriété LeasingBehavior.

Pour les sessions de bureau :

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Pour les sessions d'application :

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Où `value` peut être l'un des éléments suivants :

- **Always :** les sessions sont toujours itinérantes, quelle que soit la machine cliente et que la session soit connectée ou déconnectée. Il s'agit de la valeur par défaut.
- **DisconnectedOnly :** se reconnecte uniquement aux sessions déconnectées ; sinon, démarre une nouvelle session (vous pouvez activer l'itinérance de session entre les machines clientes

en les déconnectant, ou en utilisant le contrôle de l'espace de travail pour activer explicitement l'itinérance). Une session connectée active sur une autre machine cliente n'est jamais utilisée. Au lieu de cela, une nouvelle session est lancée.
- **SameEndpointOnly :** un utilisateur obtient une session unique pour chaque machine cliente qu'il utilise. L'itinérance est complètement désactivée. Les utilisateurs peuvent se reconnecter uniquement à la machine qui a été utilisée précédemment pour la session.

La propriété « LeasingBehavior » est décrite ci-dessous.

**Effets d'autres paramètres :**

La désactivation de l'itinérance de session est affectée par la limite d'application **Autoriser une seule instance par utilisateur** définie dans les propriétés de l'application dans le groupe de mise à disposition.

- Si vous désactivez l'itinérance de session, désactivez la limite d'application « Autoriser une seule instance par utilisateur ».
- Si vous activez la limite d'application « Autoriser une seule instance par utilisateur », ne configurez pas les deux valeurs qui permettent de nouvelles sessions sur de nouvelles machines.

### Intervalle d'ouverture de session

Si une machine virtuelle contenant un VDA de bureau se ferme avant la fin du processus d'ouverture de session, vous pouvez attribuer plus de temps au processus. La valeur par défaut pour 7.6 et versions ultérieures est de 180 secondes (la valeur par défaut pour 7.0-7.5 est de 90 secondes).

Sur la machine (ou l'image principale utilisée dans un catalogue de machines), définissez la clé de registre suivante :

Clé :`HKLM\SOFTWARE\Citrix\PortICA`

- Valeur : `AutoLogonTimeout`
- Type : `DWORD`
- Spécifiez une durée en secondes, au format décimal, dans la plage 0-3600.

Si vous modifiez une image principale, mettez à jour le catalogue.

Ce paramètre s'applique uniquement aux machines virtuelles dotées de VDA de bureau. Microsoft contrôle le délai de connexion sur les machines dotées de VDA de serveur.

## Paramètres

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Vous pouvez utiliser Web Studio pour gérer les paramètres suivants :

- Gérer l'authentification
- Programme d'amélioration de l'expérience du client Citrix
- Supprimer Delivery Controller
- Changer la base de données de journalisation
- Définir la date et l'heure
- Centralisez la gestion du site
- Activer l'attribution automatique de plusieurs utilisateurs pour Remote PC Access
- Activer la résolution DNS
- Activer l'approbation XML
- Gérer la clé de sécurité
- Définir le délai d'inactivité pour la console Studio

## Gérer l'authentification

Par défaut, les utilisateurs s'authentifient auprès de Web Studio à l'aide de leurs informations d'identification de domaine (nom d'utilisateur et mot de passe). Vous pouvez activer l'authentification Windows intégrée afin que les utilisateurs puissent accéder à Studio avec leurs informations d'identification Windows, via Kerberos ou NTLM. La désactivation de la connexion avec les informations d'identification du domaine n'est pas prise en charge.

> **Important**
>
> L'authentification Windows intégrée ne fonctionne pas lorsque Web Studio est configuré en tant que proxy pour les Delivery Controller.

Une fois que vous avez activé l'option **Authentification Windows intégrée**, la prochaine fois que vos utilisateurs se connecteront, ils seront automatiquement connectés. En tant qu'utilisateur, si vous ne parvenez pas à vous connecter automatiquement, suivez ces étapes pour configurer votre navigateur Web afin d'autoriser l'authentification Windows intégrée.

Pour Google Chrome :

1. Dans le panneau de configuration, sélectionnez Options Internet.
2. Sélectionnez l'onglet **Avancé**.
3. Sélectionnez **Activer l'authentification Windows intégrée**.
4. Sélectionnez l'onglet **Sécurité**.
5. Sélectionnez **Intranet local > Sites > Avancé**.
6. Dans la zone **Ajouter ce site Web à la zone** :
    - Si le studio Web et le Delivery Controller résident sur le même serveur, tapez l'URL de l'hôte exécutant le studio Web.
    - Si ce n'est pas le cas, saisissez un domaine générique. Exemple : si le Delivery Controller se trouve dans `ddc.domain.com`, tapez `*.domain.com`.
7. Cliquez sur **Ajouter > Fermer**

Pour Mozilla Firefox :

1. Dans le navigateur, tapez `about:config` dans le champ URL.
2. Dans le champ de **recherche**, tapez `network negotiate`.
3. Cliquez avec le bouton droit sur **network.negotiate-auth.trusted-uris** et sélectionnez **Edit**.
4. Dans le champ **Enter string value** :
    - Si Studio Web et le Delivery Controller résident sur le même serveur, ajoutez une liste d'URL et/ou d'alias séparés par des virgules faisant référence au nom du serveur hébergeant le studio Web.
    - Si ce n'est pas le cas, ajoutez les URL de cette façon. Exemple : si le Delivery Controller se trouve dans `ddc.domain.com`, tapez `*.domain.com`.

Après avoir configuré votre navigateur, vous pouvez cliquer sur **Connexion intégrée Windows** sur la page de connexion pour réessayer.

Lorsque Studio Web et le Delivery Controller sont installés sur des machines différentes, pour que l'authentification Windows intégrée fonctionne, vous devez activer **Autoriser l'accès entre origines**.

Procédez comme suit pour activer **Autoriser l'accès entre origines** :

1. Cochez la case **Autoriser l'accès entre origines**.
2. Ajoutez l'URL du serveur Web Studio à la liste d'autorisation.
3. Dans le champ **Entrez une URL**, entrez l'URL. Cliquez sur **Ajouter** pour en ajouter d'autres si nécessaire.

> **Remarque**
>
> - L'URL doit suivre le format correct :`<scheme>://<hostname>`. Assurez-vous qu'il ne comporte aucun chemin ni aucune barre oblique de fin.
> - Les adresses IP et les noms de domaine complets sont pris en charge. Lorsque vous ajoutez une URL, assurez-vous qu'elle correspond à la manière dont vous accédez à Studio Web. Par exemple, si vous accédez à Studio Web à l'aide d'une adresse IP, ajoutez l'URL basée sur l'adresse IP à la liste.
> - Si vous utilisez un port autre que celui par défaut, assurez-vous d'inclure le numéro de port.

4. Cliquez sur **Ajouter** pour en ajouter d'autres si nécessaire.
5. Lorsque vous avez terminé, cliquez sur **OK** pour enregistrer et quitter.

### Définir le fuseau horaire

Pour personnaliser le format de date et d'heure en fonction de vos préférences, procédez comme suit :

1. Connectez-vous à Web Studio et sélectionnez **Paramètres** dans le volet de gauche.
2. Localisez la vignette **Date et heure** et cliquez sur **Modifier** pour configurer les options suivantes :
    - **Format de l'heure :**
        - Sélectionnez cette option pour afficher l'heure au format 12 heures (9 h 00, par exemple) ou 24 heures (21 h 00, par exemple).
    - **Format de la date :**
        - Configurez le format de date en fonction de vos préférences, comme AAAA/MM/JJ.
    - **Fuseau horaire :**
        - **UTC :** affiche la date et l'heure en UTC sur toute l'interface utilisateur. Si vous passez la souris sur la date et l'heure, ces informations sont affichées dans votre fuseau horaire local.
        - **Fuseau horaire local :** affichez la date et l'heure selon votre fuseau horaire local sur toute l'interface utilisateur. Si vous passez la souris sur la date et l'heure, ces informations sont affichées en UTC.

> **Remarque :**
>
> Ces paramètres sont spécifiques à chaque compte utilisateur.

### Activer la résolution DNS

Pour présenter des noms DNS plutôt que des adresses IP dans le fichier ICA, procédez comme suit :

1. Connectez-vous à Web Studio et sélectionnez **Paramètres** dans le volet de gauche.
2. Activez le paramètre **Activer la résolution DNS**.

### Définir le délai d'inactivité pour la console Studio

Vous pouvez définir la durée d'inactivité après laquelle les administrateurs sont automatiquement déconnectés de la console Studio.

1. Connectez-vous à Web Studio et sélectionnez **Paramètres** dans le volet de gauche.
2. Entrez une durée comprise entre 10 minutes et 24 heures.
3. Pour appliquer ce paramètre, actualisez la page ou déconnectez-vous, puis reconnectez-vous.

### Centralisez la gestion du site

Cette fonctionnalité vous permet d'utiliser une console Web Studio pour gérer plusieurs sites Citrix Virtual Apps and Desktops. Pour en savoir plus, voir Activer la gestion sur plusieurs sites.

## Balises

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

## Introduction

Les balises sont des chaînes qui identifient les éléments tels que les machines, les applications, les bureaux, les groupes de mise à disposition, les groupes d'applications et les stratégies. Après la création d'une balise, puis son ajout à un élément, vous pouvez configurer certaines opérations pour qu'elles s'appliquent uniquement aux éléments avec une balise spécifique.

- La recherche personnalisée s'affiche dans Web Studio.

  Par exemple, pour afficher uniquement les applications qui ont été optimisées pour les testeurs, créez une balise appelée « test », puis ajoutez (appliquez) cette balise à ces applications. Vous pouvez maintenant filtrer la recherche Web Studio avec la balise « test ».

- Publiez des applications à partir d'un groupe d'applications ou des bureaux spécifiques à partir d'un groupe de mise à disposition, prenant en compte un seul sous-ensemble de machines dans les groupes de mise à disposition sélectionnés. C'est ce qu'on appelle une *restriction de balise*.

  Avec les restrictions de balise, vous pouvez utiliser des machines existantes pour plusieurs tâches de publication, éliminant ainsi les coûts associés avec le déploiement et la gestion de machines supplémentaires. L'utilisation d'une restriction de balise équivaut à diviser (ou partitionner) des machines dans un groupe de mise à disposition. Cette fonctionnalité est semblable, mais pas identique, aux groupes de travail dans les versions de XenApp antérieures à 7.x.

  L'utilisation d'un groupe d'applications ou de bureaux avec une restriction de balise peut s'avérer utile pour isoler et dépanner un sous-ensemble de machines dans un groupe de mise à disposition.

- Programmez des redémarrages périodiques pour un sous-ensemble de machines dans un groupe de mise à disposition.

  L'utilisation d'une restriction de balise pour les machines vous permet d'utiliser de nouvelles applets de commande PowerShell pour configurer plusieurs programmes de redémarrage pour des sous-ensembles de machines dans un groupe de mise à disposition. Pour des exemples et de plus amples informations, consultez la section Gérer des groupes d'applications.

- Personnalisez l'application (attribution) de stratégies Citrix à un sous-ensemble de machines dans des groupes de mise à disposition, des types de groupe de mise à disposition ou des unités d'organisation qui ont (ou n'ont pas) une balise spécifique.

  Par exemple, si vous souhaitez appliquer une stratégie Citrix uniquement aux postes de travail les plus puissants, ajoutez une balise nommée « haute puissance » à ces machines. Ensuite, sur la page **Attribuer la stratégie** de l'assistant Créer une stratégie, sélectionnez cette balise ainsi que la case à cocher **Activer**. Vous pouvez également ajouter une balise à un groupe de mise à

disposition, puis appliquer une stratégie Citrix à ce groupe. Pour plus d'informations, consultez la section Créer des stratégies.

Vous pouvez appliquer des balises à :

- Machines
- Applications
- Catalogues de machines (PowerShell uniquement ; voir Balises sur les catalogues de machines)
- Groupes de mise à disposition
- Groupes d'applications

Une restriction de balise peut être configurée lors de la création ou de la modification des éléments suivants dans Web Studio :

- Un bureau d'un groupe de mise à disposition partagé
- Un groupe d'applications

## Restrictions de balise pour un bureau ou un groupe d'applications

Une restriction de balise implique plusieurs étapes :

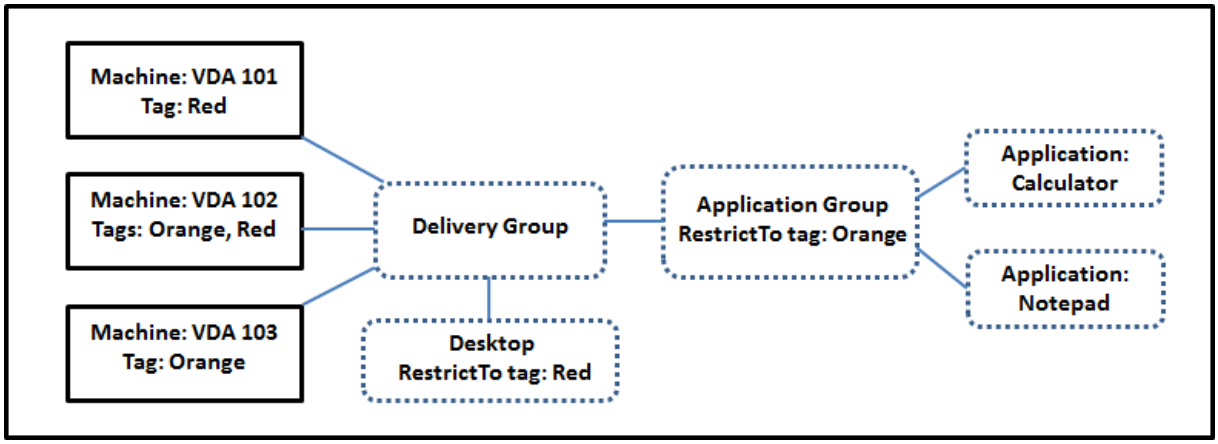
- Créer une balise, puis l'ajouter (appliquer) sur les machines.
- Créer ou modifier un groupe avec la restriction de balise (en d'autres termes, « restreindre les démarrages aux machines avec la balise x »).

Une restriction de balise étend le processus de sélection de machine du broker. Le broker sélectionne une machine dans un groupe de mise à disposition associé en fonction de la stratégie d'accès, des listes d'utilisateurs configurées, de la préférence de zone et de la disponibilité, ainsi que de la restriction de balise (le cas échéant). Pour les applications, le broker retourne sur d'autres groupes de mise à disposition dans l'ordre de priorité, appliquant les mêmes règles de sélection de machine pour chaque groupe de mise à disposition pris en compte.

### Exemple 1 : disposition simple

Cet exemple présente une configuration simple qui utilise des restrictions de balise pour limiter les machines qui sont prises en compte pour certains lancements de bureau et d'application. Le site dispose d'un groupe de mise à disposition partagé, d'un bureau publié et d'un groupe d'applications configuré avec deux applications.




- Des balises ont été ajoutées à chacune des trois machines (VDA 101-103).
- Le bureau du groupe de mise à disposition partagé a été créé avec une restriction de balise nommée « Rouge ». Un bureau ne peut être lancé que sur les machines de ce groupe de mise à disposition qui ont la balise « Rouge » : VDA 101 et 102.
- Le groupe d'applications a été créé avec la restriction de balise « Orange », de sorte que chacune de ses applications (calculatrice et Bloc-notes) puisse être lancée uniquement sur les machines de ce groupe de mise à disposition qui ont la balise « Orange » : VDA 102 et 103.

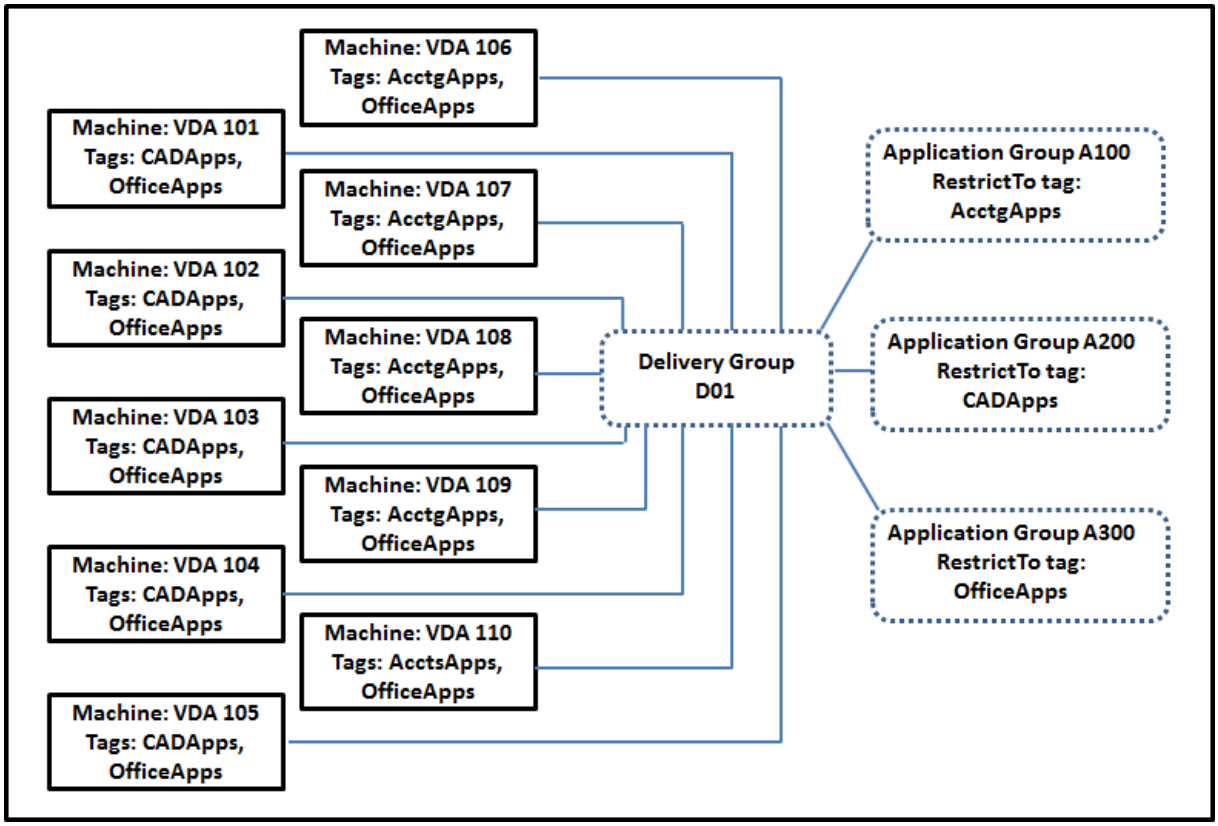
La machine VDA 102 a les deux balises (Rouge, Orange), elle sera donc prise en compte pour démarrer les applications et le bureau.

#### Exemple 2 : disposition plus complexe

Cet exemple contient plusieurs groupes d'applications qui ont été créés avec restrictions de balise. Cela permet de mettre à disposition un plus grand nombre d'applications avec moins de machines que nécessaire si uniquement des groupes de mise à disposition sont utilisés.

La section Comment configurer l'exemple 2 présente les étapes utilisées pour créer et appliquer les balises, puis configurer les restrictions de balise dans cet exemple.




Cet exemple utilise 10 machines (VDA 101 à 110), un groupe de mise à disposition (D01) et trois groupes d'applications (A100, A200, A300). Si vous appliquez des balises à chaque machine, puis spécifiez des restrictions de balise lors de la création de chaque groupe d'applications :

- Les utilisateurs du service Comptabilité (Acctg) du groupe peuvent accéder aux applications dont ils ont besoin sur cinq machines (VDA 101 à 105)
- Les concepteurs CAD du groupe peuvent accéder aux applications dont ils ont besoin sur cinq machines (VDA 106 à 110)
- Les utilisateurs du groupe qui ont besoin d'applications Office peuvent accéder aux applications Office sur 10 machines (VDA 101 à 110)

Seules 10 machines sont utilisées, avec un seul groupe de mise à disposition. L'utilisation de groupes de mise à disposition uniquement (sans groupes d'applications) nécessiterait deux fois plus de machines, car une machine peut appartenir à un seul groupe de mise à disposition.

### Gérer les balises et restrictions de balise

Les balises sont créées, ajoutées (appliquées), modifiées et supprimées des éléments sélectionnés via l'action **Gérer les balises** dans Web Studio.

(Exception : les balises utilisées pour les attributions de stratégie sont créées, modifiées et supprimées

via l'action **Gérer les balises** dans Web Studio. Toutefois, les balises sont appliquées (attribuées) lorsque vous créez la stratégie. Voir Créer des stratégies pour plus de détails.)

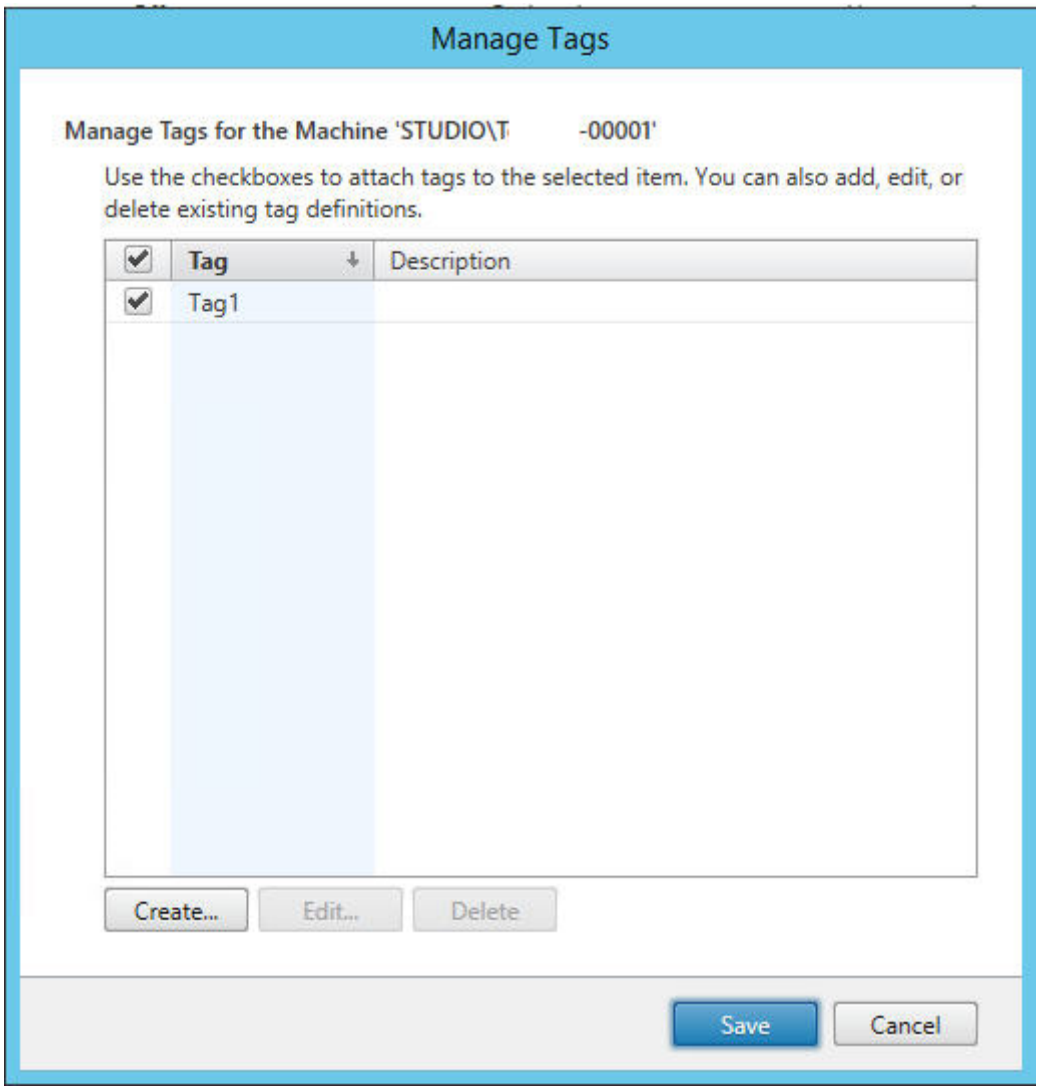
Les restrictions de balise sont configurées lorsque vous créez ou modifiez des bureaux dans des groupes de mise à disposition, et lorsque vous créez et modifiez des groupes d'applications.

#### Utiliser la boîte de dialogue Gérer les balises dans Web Studio

Dans Web Studio, sélectionnez les éléments auxquels vous souhaitez appliquer une balise (une ou plusieurs machines, applications, un bureau, un groupe de mise à disposition ou un groupe d'applications), puis sélectionnez **Gérer les balises** dans la barre d'actions. La boîte de dialogue répertorie toutes les balises qui ont été créées dans le site, et pas seulement pour les éléments sélectionnés.

- Une case à cocher sélectionnée indique que la balise a déjà été ajoutée aux éléments sélectionnés. (Dans la capture d'écran ci-dessous, la balise appelée « Tag1 » est appliquée à la machine sélectionnée.)
- Si vous avez sélectionné plusieurs éléments, une case à cocher contenant un trait indique que certains, mais pas tous les éléments sélectionnés, ont une balise.




Les options suivantes sont disponibles dans la boîte de dialogue **Gérer les balises**. Veillez à consulter les Précautions lors de l'utilisation de balises.

- **Pour créer une balise :**

  Cliquez sur **Créer**. Entrez un nom et une description. Les noms de balise doivent être uniques et ne sont pas sensibles à la casse. Cliquez ensuite sur **OK**. (La création d'une balise ne l'applique pas automatiquement à tous les éléments que vous avez sélectionnés. Utilisez les cases à cocher pour appliquer la balise).

- **Pour ajouter (appliquer) une ou plusieurs balises :**

  Activez la case à cocher en regard du nom de la balise. Si vous sélectionnez plusieurs éléments et que la case à cocher en regard d'une balise contient un trait (pour indiquer que la balise est déjà appliquée à certains, mais pas à tous les éléments sélectionnés), l'activation de la case affecte toutes les machines sélectionnées.

Si vous essayez d'ajouter une balise à une ou plusieurs machines, et que cette balise est actuellement utilisée comme restriction dans un groupe d'applications, vous êtes averti que cette action rendra ces machines disponibles pour le démarrage. Si c'est votre intention, continuez.

- **Pour retirer une ou plusieurs balises :**

  Désactivez la case à cocher en regard du nom de ma balise. Si vous sélectionnez plusieurs éléments et que la case à cocher en regard d'une balise contient un trait (pour indiquer que la balise est déjà appliquée à certains, mais pas à tous les éléments sélectionnés), la désactivation de la case retire la balise de toutes les machines sélectionnées.

  Si vous tentez de retirer une balise d'une machine qui utilise cette balise comme restriction, un message d'avertissement vous indique que cela peut affecter les machines qui seront prises en compte pour le démarrage. Si c'est votre intention, continuez.

- **Pour modifier une balise :**

  Sélectionnez une balise, puis cliquez sur **Modifier**. Entrez un nouveau nom, une description ou les deux. Vous pouvez modifier une seule balise à la fois.

- **Pour supprimer une ou plusieurs balises :**

  Sélectionnez les balises, puis cliquez sur **Supprimer**. La boîte de dialogue Supprimer les balises indique le nombre d'éléments qui utilisent actuellement les balises sélectionnées (par exemple « 2 machines »). Cliquez sur un élément pour afficher des informations supplémentaires. Par exemple, le fait de cliquer sur un élément « 2 machines » affiche les noms des deux machines auxquelles cette balise est appliquée. Confirmez que vous souhaitez supprimer les balises.

  Vous ne pouvez pas utiliser Web Studio pour supprimer une balise qui est utilisée comme restriction. Vous devez d'abord modifier le groupe d'applications et retirer la restriction de balise ou sélectionner une autre balise.

Lorsque vous avez terminé dans la boîte de dialogue **Gérer les balises**, cliquez sur **Enregistrer**.

Pour voir si des balises sont appliquées sur une machine : sélectionnez **Groupes de mise à disposition** dans le volet de gauche. Sélectionnez un groupe de mise à disposition dans le volet central, puis sélectionnez **Afficher les machines** dans la barre d'actions. Sélectionnez une machine dans le volet central, puis sélectionnez l'onglet **Balises** dans le panneau **Détails**.

#### Gérer les restrictions de balise

La configuration d'une restriction de balise est un processus à plusieurs étapes : vous devez d'abord créer la balise et l'ajouter (l'appliquer) aux machines. Ensuite, vous devez ajouter la restriction au groupe d'applications ou au bureau.

- **Créer et appliquer la balise :**

Créez la balise, puis ajoutez-la (appliquez-la) aux machines affectées par la restriction de balise, à l'aide des actions **Gérer les balises** décrites précédemment.

- **Pour ajouter une restriction de balise à un groupe d'applications :**

  Créez ou modifiez le groupe d'applications. Sur la page **Groupes de mise à disposition**, sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise dans la liste déroulante.

- **Pour modifier ou retirer la restriction de balise sur un groupe d'applications :**

  Modifiez le groupe. Sur la page **Groupes de mise à disposition**, sélectionnez une autre balise à partir de la liste ou supprimez la restriction de balise complètement en désactivant le paramètre **Restreindre les lancements aux machines dotées de balises**.

- **Pour ajouter une restriction de balise à un bureau :**

  Créez ou modifiez un groupe de mise à disposition. Cliquez sur **Ajouter** ou **Modifier** sur la page **Bureaux**. Dans la boîte de dialogue Ajouter un bureau, sélectionnez **Restreindre les lancements aux machines dotées de balises**, puis sélectionnez la balise dans le menu.

- **Pour modifier ou retirer la restriction de balise sur un groupe de mise à disposition :**

  Modifiez le groupe. Sur la page Bureaux, cliquez sur **Modifier**. Dans la boîte de dialogue, sélectionnez une autre balise à partir de la liste ou supprimez la restriction de balise complètement en désactivant le paramètre **Restreindre les lancements aux machines dotées de balises**.

#### Précautions lors de l'utilisation de balises

Une balise appliquée à un élément peut avoir plusieurs fonctions, donc n'oubliez pas que l'ajout, le retrait et la suppression d'une balise peut avoir des effets indésirables. Vous pouvez utiliser une balise pour trier l'affichage des machines dans le champ de recherche de Web Studio. Vous pouvez utiliser la même balise comme restriction lors de la configuration d'un groupe d'applications ou d'un bureau. Seules les machines appartenant aux groupes de mise à disposition spécifiés qui sont associés à cette balise sont prises en compte pour le lancement.

Lorsque vous essayez d'ajouter une balise à des machines après que cette balise a été configurée en tant que restriction de balise pour un bureau ou un groupe d'applications, un avertissement apparaît. L'ajout de cette balise peut rendre les machines disponibles pour lancer d'autres applications ou bureaux. Si c'est votre intention, continuez. Sinon, vous pouvez annuler l'opération.

Par exemple, supposons que vous créez un groupe d'applications avec la restriction de balise « Red ». Plus tard, vous ajoutez plusieurs autres machines au groupe de mise à disposition utilisé par ce groupe d'applications. Si vous essayez d'ajouter la balise « Red » à ces machines, Web Studio affiche un message similaire au suivant : « La balise « Red » est utilisée en tant que restriction sur les groupes d'applications suivants. Si vous ajoutez cette balise, les machines sélectionnées pourront peut-être

lancer des applications dans ces groupes d'applications. » Vous pouvez ensuite confirmer ou annuler l'ajout de cette balise à ces machines supplémentaires.

De même, si un groupe d'applications utilise une balise pour restreindre les démarrages, Web Studio vous avertit que vous ne pouvez pas supprimer la balise tant que vous ne modifiez pas le groupe pour la retirer comme restriction. (Si vous étiez autorisé à supprimer une balise qui est utilisée comme restriction dans un groupe d'applications, cela pourrait permettre le démarrage des applications sur toutes les machines des groupes de mise à disposition associés au groupe d'applications.) La même interdiction s'applique si la balise est actuellement utilisée comme restriction pour les démarrages de bureau. Après avoir modifié le groupe d'applications ou les bureaux du groupe de mise à disposition pour retirer cette restriction de balise, vous pouvez supprimer la balise.

Les machines peuvent ne pas toutes avoir le même ensemble d'applications. Un utilisateur peut appartenir à plusieurs groupes d'applications, chacun avec une restriction de balise différente et des ensembles de machines différents ou se chevauchant. Le tableau suivant explique comment la prise en compte des machines est décidée.

| Lorsqu'une application a été ajoutée à | Ces machines dans les groupes de mise à disposition sélectionnés sont prises en compte pour le démarrage |
|---|---|
| Un groupe d'applications sans restriction de balise | Toutes les machines |
| Un groupe d'applications avec restriction de balise A | Les machines sur lesquelles est appliquée la balise A |
| Deux groupes d'applications, l'un avec la restriction de balise A et l'autre avec la restriction de balise B | Les machines qui ont une balise A et une balise B. Si aucune n'est disponible, les machines qui ont une balise A ou B |
| Deux groupes d'applications, l'un avec la restriction de balise A et l'autre sans restriction de balise | Les machines qui ont la balise A ; si aucune n'est disponible, toute machine |

Si vous avez utilisé une restriction de balise dans un programme de redémarrage de machine, les modifications que vous apportez qui affectent les applications ou les restrictions de balise affecteront le prochain cycle de redémarrage de machine. Les cycles de redémarrage en cours d'exécution lorsque les modifications sont effectuées ne seront pas affectés.

#### Comment configurer - Exemple 2

La séquence suivante illustre les étapes permettant de créer et d'appliquer des balises, puis de configurer des restrictions de balise pour les groupes d'applications illustrés dans le deuxième exemple.

Les VDA et les applications ont déjà été installés sur les machines et le groupe de mise à disposition a été créé.

Créez et appliquez des balises aux machines :

1. Dans Web Studio, sélectionnez le groupe de mise à disposition D01, puis sélectionnez **Afficher les machines** dans la barre d'actions.
2. Sélectionnez les VDA de machine 101-105, puis sélectionnez **Gérer les machines** dans la barre d'actions.
3. Dans la boîte de dialogue Gérer les balises, cliquez sur **Créer** puis créez une balise nommée `CADApps`. Cliquez sur **OK**.
4. Cliquez à nouveau sur **Créer** et créez une balise nommée OfficeApps. Cliquez sur **OK**.
5. Toujours dans la boîte de dialogue **Gérer les balises**, ajoutez (appliquez) les balises qui viennent d'être créées aux machines sélectionnées en activant les cases à cocher en regard de chaque nom de balise (`CADApps` et `OfficeApps`). Lorsque vous avez terminé, fermez la boîte de dialogue.
6. Sélectionnez le groupe de mise à disposition D01, sélectionnez **Afficher les machines** dans la barre d'actions.
7. Sélectionnez les VDA de machine 106-110, puis sélectionnez **Gérer les machines** dans la barre d'actions.
8. Dans la boîte de dialogue **Gérer les balises**, cliquez sur **Créer**. Créez une balise nommée `AcctgApps`. Cliquez sur **OK**.
9. Appliquez la balise `AcctgApps` qui vient d'être créée et la balise `OfficeApps` aux machines sélectionnées en cliquant sur les cases à cocher en regard de chaque nom de balise, puis fermez la boîte de dialogue.

Créez les groupes d'applications avec des restrictions de balise.

1. Dans Web Studio, sélectionnez **Applications** dans le volet de gauche, sélectionnez l'onglet **Groupes d'applications**, puis sélectionnez **Créer groupe d'applications** dans la barre d'actions. L'assistant Créer groupe d'applications démarre.
2. Sur la page **Groupes de mise à disposition** de l'assistant, sélectionnez Groupe de mise à disposition D01. Sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise `AcctgApps` dans la liste.
3. Suivez les instructions de l'assistant, en spécifiant les utilisateurs de la comptabilité et les applications de comptabilité. (Lors de l'ajout de l'application, choisissez la source **Depuis le menu Démarrer**, qui recherche l'application sur les machines dotées de la balise `AcctgApps`.) Sur la page **Résumé**, nommez le groupe `A100`.
4. Répétez ces étapes pour créer un groupe d'applications `A200`, en spécifiant les machines auxquelles est appliquée la balise `CADApps`, ainsi que les utilisateurs et applications appropriés.
5. Répétez les étapes permettant de créer un groupe d'applications `A300`, en spécifiant les machines auxquelles est appliquée la balise `OfficeApps`, ainsi que les utilisateurs et applica-

tions appropriés.

#### Balises sur les catalogues de machines

Vous pouvez utiliser des balises sur les catalogues de machines. La séquence globale de création d'une balise et de son application à un catalogue est la même que celle décrite précédemment. Toutefois, l'application de balises aux catalogues n'est prise en charge que via l'interface PowerShell. Vous ne pouvez pas utiliser Web Studio pour appliquer une balise à un catalogue ou supprimer une balise d'un catalogue. Les affichages du catalogue dans Web Studio n'indiquent pas si une balise est appliquée.

Résumé : vous pouvez utiliser Web Studio ou PowerShell pour créer ou supprimer une balise à utiliser sur un catalogue. Utilisez PowerShell pour appliquer la balise au catalogue.

Voici quelques exemples d'utilisation de balises avec des catalogues :

- Un groupe de mise à disposition a des machines provenant de plusieurs catalogues, mais vous souhaitez qu'une opération (telle qu'un programme de redémarrage) affecte uniquement les machines d'un catalogue spécifique. L'application d'une balise à ce catalogue permet de le faire.
- Dans un groupe d'applications, vous souhaitez limiter les sessions d'application aux machines d'un catalogue spécifique. L'application d'une balise à ce catalogue permet de le faire.

Applets de commande PowerShell concernées :

- Vous pouvez passer des objets catalogue à des applets de commande telles que `Add-BrokerTag` et `Remove-BrokerTag`.
- `Get-BrokerTagUsage` indique le nombre de catalogues contenant des balises.
- `Get-BrokerCatalog` a une propriété nommée `Tags`.

Par exemple, les applets de commande suivantes ajoutent une balise nommée `fy2018` au catalogue nommé `acctg` :
`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`. (La balise a été précédemment créée à l'aide de Web Studio ou de PowerShell.)

Consultez l'aide de l'applet de commande PowerShell pour plus d'informations et la syntaxe.

### Balises automatiques (Technical Preview)

Le balisage automatique permet aux administrateurs de définir et de supprimer automatiquement des balises sur différents objets Citrix Virtual Apps and Desktops en fonction de règles personnalisées. Cette amélioration élimine le besoin de gérer différents scripts qui s'exécutent périodiquement pour optimiser l'environnement.

### Cas d'utilisation

Grâce au balisage automatique, vous pouvez mettre en œuvre des règles liées aux moteurs de votre activité, telles que la réduction des coûts, l'optimisation de l'infrastructure et l'augmentation de la consommation. Voici certains des cas d'utilisation :

- **Récupérer les VDI inutilisés** : pour libérer les charges de travail dédiées qui n'ont pas été utilisées depuis plus d'un nombre de jours préconfiguré vers le pool disponible.
- **Supprimer l'encombrement des applications** : pour réduire l'encombrement des applications en identifiant les applications qui n'ont pas été utilisées pendant plus d'un nombre de jours préconfiguré.
- **Groupes de mise à disposition avec un niveau fonctionnel inférieur à X** : pour rechercher des groupes de mise à disposition dont le niveau fonctionnel est inférieur à un niveau fonctionnel spécifique.
- **Utilisateurs inactifs** : pour récupérer les ressources des utilisateurs qui ne se sont pas connectés depuis plus d'un nombre de jours préconfiguré.

### Commandes PowerShell

Vous pouvez créer des balises automatiques à l'aide des commandes PowerShell. Une fois qu'une balise automatique est créée, elle est évaluée à une fréquence de 600 secondes. Pour plus d'informations, consultez New-BrokerAutoTagRule.

**Exemples** `New-BrokerAutoTagRule` utilise le même type d'objet et les mêmes paramètres de filtre que l'applet de commande `Get-BrokerMachine`. Pour plus d'informations, consultez Get-BrokerMachine.

1. Balisez les VDI dédiés qui n'ont pas été utilisés depuis plus de 30 jours avec l'ID 123 :

   a) Définissez une balise pour baliser les VDI inutilisés, par exemple **Unused-VDI**.

      - Nom de la balise : Unused-VDI
      - ID de la balise : 123

   b) Créez la règle de balisage automatique pour baliser les machines inutilisées. Définissez les paramètres de la règle :

      - Nom : nom générique de la règle.
      - Type d'objet : Machine.
      - Texte de la règle : machines attribuées statiques dont la dernière connexion date de plus de 30 jours ou n'a aucune valeur.
      - ID de balise : ID de balise que vous souhaitez associer, 123.

```
New-BrokerAutoTagRule -Name 'UnusedVdi' -ObjectType 'Machine'
 -RuleText "-AllocationType Static -IsAssigned $true -Filter
 { SummaryState -ne `"InUse`" -and ( LastConnectionTime -lt
'-30' -or LastConnectionTime -eq `$null )} " -TagUid 123<!--
NeedCopy-->
```

c) Vérifiez les machines marquées de la balise **Unused-VDI** et libérez-les.

2. Pour baliser les groupes de mise à disposition dont le niveau fonctionnel est inférieur à X (en utilisant **L7_20** comme niveau fonctionnel seuil) :

```
New-BrokerAutoTagRule -Name 'LowFL'-ObjectType 'DesktopGroup'-RuleText
 "-Filter { MinimumFunctionalLevel -lt 'L7_20' } "-TagUid 123
```

1. Pour baliser les applications visibles par l'utilisateur publiées sans dossier :

```
New-BrokerAutoTagRule -Name 'NoFolder'-ObjectType 'Application'-
RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} "-TagUid
 123
```

### Informations supplémentaires

Post de blog : How to assign desktops to specific servers (Comment attribuer des postes de travail à des serveurs spécifiques).

## Profils utilisateur

June 27, 2024

Par défaut, Citrix Profile Management est installé de manière silencieuse sur les images principales lorsque vous installez Virtual Delivery Agent, mais vous n'avez pas à utiliser Profile Management en tant que solution de profils.

Afin de répondre aux besoins variés de vos utilisateurs, vous pouvez utiliser les stratégies Citrix Virtual Apps and Desktops pour appliquer un comportement de profil différent aux machines dans chaque groupe de mise à disposition. Par exemple, un groupe de mise à disposition peut nécessiter des profils obligatoires Citrix, dont le modèle est stocké dans un emplacement réseau, mais un autre groupe de mise à disposition peut nécessiter des profils itinérants Citrix stockés dans un autre emplacement avec plusieurs dossiers redirigés.

- Si d'autres administrateurs de votre organisation sont responsables des stratégies Citrix Virtual Apps and Desktops, travaillez avec eux pour vous assurer qu'ils définissent les stratégies liées aux profils sur vos groupes de mise à disposition.
- Les stratégies Profile Management peuvent également être définies dans la stratégie de groupe, dans le fichier .ini de Profile management et localement sur des machines virtuelles individuelles. Ces diverses méthodes permettant de définir le comportement de profil sont lues dans l'ordre suivant :

  1. Stratégie de groupe (fichiers .adm ou .admx)
  2. Stratégies Citrix Virtual Apps and Desktops dans le nœud Stratégie
  3. Stratégies locales sur la machine virtuelle à laquelle l'utilisateur se connecte
  4. Fichier .ini Profile Management

  Par exemple, si vous configurez la même stratégie dans le nœud Stratégie de groupe et le nœud Stratégie, le système lit le paramètre de stratégie dans la stratégie de groupe et ignore le paramètre de stratégie Citrix Virtual Apps and Desktops.

Quelle que soit la solution de gestion des profils que vous choisissez, les administrateurs Director peuvent accéder à des informations de diagnostic afin de résoudre les problèmes liés aux profils utilisateur. Pour de plus amples informations, consultez la documentation de Director.

### Configuration automatique

Le type de bureau est automatiquement détecté, basé sur l'installation de Virtual Delivery Agent et, en plus du choix de configuration que vous effectuez dans Studio, définit les valeurs par défaut de Profile Management en conséquence.

Les stratégies que Profile Management ajuste sont affichées dans le tableau suivant. Les paramètres de stratégie autres que les paramètres par défaut sont préservés et ne sont pas écrasés par cette fonctionnalité. Consultez la documentation Profile Management pour de plus amples informations sur chaque stratégie. Les types de machines qui créent des profils affectent les stratégies qui sont modifiées. Votre choix doit se baser sur les facteurs principaux suivants : les machines sont-elles persistantes ou provisionnées, sont-elles partagées par de multiples utilisateurs ou dédiées à un seul utilisateur ?

Les systèmes persistants disposent d'un stockage local dont le contenu est conservé lorsque le système est éteint. Les systèmes persistants peuvent utiliser des technologies de stockage telles que les réseaux SAN pour mettre en miroir le disque local. En revanche, les systèmes provisionnés sont créés « à la volée » à partir d'un disque de base et d'un type de disque d'identité. Le stockage local est généralement imité par un disque RAM ou un disque réseau, ce dernier étant fourni la plupart du temps par un SAN doté d'un lien à haute vitesse. La technologie de provisioning utilisée est générale-

ment Citrix Provisioning ou Machine Creation Services (ou une technologie tierce). Parfois, les systèmes provisionnés sont dotés d'un stockage local persistant. Ils sont classés comme persistants.

Ensemble, ces deux facteurs définissent les types de machines suivants :

- **Persistantes et dédiées**. Exemples : machines dotées d'un système d'exploitation monosession avec une attribution statique et un stockage local persistant créées avec Machine Creation Services, postes de travail physiques et ordinateurs portables.
- **Persistantes et partagées**. Exemples : machines dotées d'un système d'exploitation multisession créées avec Machine Creation Services et serveurs Citrix Virtual Apps.
- **Provisionnées et dédiées**. Exemples : machines dotées d'un système d'exploitation monosession avec une attribution statique mais sans stockage persistant créées avec Citrix Provisioning Service (dans Citrix Virtual Desktops).
- **Provisionnées et partagées**. Exemples : machines dotées d'un système d'exploitation monosession avec une attribution aléatoire créées avec Provisioning Service (dans Citrix Virtual Desktops) et serveurs Citrix Virtual Desktops.

Les paramètres de stratégie Profile Management suivants sont suggérés pour les types de machines différents. Ils sont adaptés à la plupart des cas, mais vous pouvez en choisir d'autres plus adaptés à votre déploiement.

> **Important :**
>
> **Supprimer les profils mis en cache localement à la fermeture de session**, **Streaming des profils** et **Toujours mettre en cache** sont appliqués par la fonctionnalité de configuration automatique. Ajustez les autres stratégies manuellement.

**Machines persistantes**

| Stratégie | Persistantes et dédiées | Persistantes et partagées |
|---|---|---|
| Supprimer les profils mis en cache localement à la fermeture de session | Désactivé | Activé |
| Streaming des profils | Désactivé | Activé |
| Toujours mettre en cache | Activée (remarque 1) | Désactivée (remarque 2) |
| Réécriture active | Désactivé | Désactivée (remarque 3) |
| Traiter les connexions des administrateurs locaux | Activé | Désactivée (remarque 4) |

**Machines provisionnées**

| Stratégie | Provisionnées et dédiées | Provisionnées et partagées |
|---|---|---|
| Supprimer les profils mis en cache localement à la fermeture de session | Désactivée (remarque 5) | Activé |
| Streaming des profils | Activé | Activé |
| Toujours mettre en cache | Désactivée (remarque 6) | Désactivé |
| Réécriture active | Activé | Activé |
| Traiter les connexions des administrateurs locaux | Activé | Activée (remarque 7) |

1. Étant donné que la stratégie **Streaming de profil** est désactivée pour ce type de machine, le paramètre **Toujours mettre en cache** est toujours ignoré.
2. Désactivez **Toujours mettre en cache**. Toutefois, vous pouvez vous assurer que les fichiers volumineux sont chargés dans les profils dès que possible après l'ouverture de session en activant cette stratégie et en l'utilisant pour définir une limite de taille de fichier (en Mo). Tout fichier de taille égale ou supérieure est placé en cache dès que possible.
3. Désactivez **Réécriture active** sauf pour enregistrer des modifications dans les profils des utilisateurs qui passent d'un serveur Citrix Virtual Apps à un autre. Dans ce cas, activez cette stratégie.
4. Désactivez **Traiter les ouvertures de session des administrateurs locaux** sauf pour les bureaux partagés hébergés. Dans ce cas, activez cette stratégie.
5. Désactivez **Supprimer les profils mis en cache localement à la fermeture de session**. Ce paramètre conserve les profils mis en cache localement. Étant donné que les machines sont réinitialisées à la fermeture de session mais attribuées à des utilisateurs individuels, les ouvertures de session sont plus rapides si leurs profils sont mis en cache.
6. Désactivez **Toujours mettre en cache**. Toutefois, vous pouvez vous assurer que les fichiers volumineux sont chargés dans les profils dès que possible après l'ouverture de session en activant cette stratégie et en l'utilisant pour définir une limite de taille de fichier (en Mo). Tout fichier de taille égale ou supérieure est placé en cache dès que possible.
7. Activez **Traiter les ouvertures de session des administrateurs locaux** sauf pour les profils des utilisateurs qui itinèrent entre serveurs Citrix Virtual Apps and Desktops. Dans ce cas, désactivez cette stratégie.

## Redirection de dossiers

La redirection de dossiers vous permet de stocker les données utilisateur sur des partages réseau autres que l'emplacement dans lequel les profils sont stockés. La redirection de dossiers permet de

réduire la taille du profil et de la durée de chargement, mais peut avoir un impact sur la bande passante réseau. La redirection de dossiers ne nécessite pas que les profils utilisateur Citrix soient utilisés. Vous pouvez gérer les profils utilisateur vous-mêmes, et toujours rediriger les dossiers.

Configurez la redirection de dossiers à l'aide de stratégies Citrix dans Studio.

- Assurez-vous que les emplacements réseau utilisés pour stocker le contenu de ces dossiers redirigés sont disponibles et que vous avez les permissions appropriées. Les propriétés d'emplacement sont validées.
- Les dossiers redirigés sont configurés sur le réseau et leur contenu rempli depuis les bureaux virtuels des utilisateurs à l'ouverture de session.

Configurez la redirection de dossiers à l'aide des stratégies Citrix ou des objets de stratégie de groupe Active Directory, mais pas les deux. La configuration de la redirection de dossiers à l'aide des deux moteurs de stratégie peut résulter en un comportement imprévisible.

### Redirection vers les dossiers spéciaux avancée

Dans les déploiements comportant plusieurs systèmes d'exploitation (OS), il se peut que vous souhaitiez partager un profil utilisateur avec chaque système d'exploitation. Le reste du profil n'est pas partagé et est uniquement utilisé par un seul système d'exploitation. Pour assurer une expérience utilisateur cohérente sur les systèmes d'exploitation, vous devez disposer d'une autre configuration pour chaque système d'exploitation, en d'autres termes, la redirection de dossiers avancée. Par exemple, les différentes versions d'une application s'exécutant sur deux systèmes d'exploitation peuvent être nécessaires pour lire ou modifier un fichier partagé, vous décidez ainsi de le rediriger vers un emplacement réseau sur lequel les deux versions peuvent y accéder. Éventuellement, car le contenu du dossier **Menu Démarrer** est conçu différemment dans les deux systèmes d'exploitation, si vous décidez de rediriger uniquement un dossier, mais pas les deux. Cette approche sépare le dossier **Menu Démarrer** et son contenu sur chaque système d'exploitation, en assurant aux utilisateurs une expérience cohérente.

Si votre déploiement requiert la redirection de dossiers avancée, vous devez comprendre la structure des données de profil de vos utilisateurs et déterminer quelles parties peuvent être partagées entre systèmes d'exploitation. Un comportement imprévisible peut se produire à moins que la redirection de dossier ne soit utilisée correctement.

Pour rediriger les dossiers dans les déploiements avancés :

- Utilisez un groupe de mise à disposition distinct pour chaque système d'exploitation.
- Comprenez l'emplacement où vos applications virtuelles, y compris celles se trouvant sur des bureaux virtuels, stockent des données et des paramètres utilisateur, et la façon dont les données sont structurées.

- Pour partager les données de profil qui peuvent itinérer en toute sécurité (car elles sont conçues de manière identique dans chaque système d'exploitation), redirigez les dossiers contenant dans chaque groupe de mise à disposition.
- Pour les données de profil non partagées qui ne peuvent pas itinérer, redirigez le dossier contenant uniquement dans l'un des groupes de bureaux, généralement celui avec le système d'exploitation le plus utilisé ou celui dans lequel les données sont plus pertinentes. Éventuellement, pour les données non partagées qui ne peuvent pas itinérer entre systèmes d'exploitation, redirigez les dossiers contenant sur les deux systèmes pour séparer les emplacements réseau.

#### Exemple de déploiement avancé

Le déploiement possède des applications, y compris des versions de Microsoft Outlook et Internet Explorer, en cours d'exécution sur des bureaux et des applications Windows 10, y compris d'autres versions d'Outlook et Internet Explorer, mises à disposition par Windows Server 2019. Vous avez déjà configuré deux groupes de mise à disposition pour les deux systèmes d'exploitation. Les utilisateurs souhaitent accéder à la même série de **contacts** et de **favoris** dans les deux versions des deux applications.

**Important :** les décisions et les conseils suivants sont valides pour les systèmes d'exploitation et le déploiement décrits. Dans votre organisation, les dossiers que vous choisissez de rediriger et si vous décidez de les partager dépend d'un certain nombre de facteurs qui sont uniques à votre déploiement spécifique.

- À l'aide des stratégies appliquées aux groupes de mise à disposition, vous choisissez les dossiers suivants à rediriger.

| Folder | Redirigé dans Windows 10 ? | Redirigé dans Windows Server 2019 ? |
|---|---|---|
| Mes documents | Oui | Oui |
| Données d'application | Non | Non |
| Contacts | Oui | Oui |
| Bureau | Oui | Non |
| Téléchargements | Non | Non |
| Favoris | Oui | Oui |
| Liens | Oui | Non |
| Ma musique | Oui | Oui |

| Folder | Redirigé dans Windows 10 ? | Redirigé dans Windows Server 2019 ? |
|---|---|---|
| Mes images | Oui | Oui |
| Mes vidéos | Oui | Oui |
| Recherches | Oui | Non |
| Parties enregistrées | Non | Non |
| Menu Démarrer | Oui | Non |

- Pour les dossiers partagés et redirigés :
  - Une fois l'analyse de la structure des données enregistrées par les différentes versions d'Outlook et Internet Explorer, vous décidez qu'il est préférable de partager les dossiers **Contacts** et **Favoris**.
  - Vous savez que la structure des dossiers **Documents**, **Musique**, **Images** et **Vidéos** est standard sur tous les systèmes d'exploitation. Il est donc sûr de stocker ces dossiers dans le même emplacement réseau pour chaque groupe de mise à disposition.
- Pour les dossiers non partagés et redirigés :
  - Vous ne redirigez pas les dossiers Bureau, Liens, Recherches ou **Menu Démarrer** dans le groupe de mise à disposition Windows Server, car les données de ces dossiers sont organisées différemment dans les deux systèmes d'exploitation. Il ne peut donc pas être partagé.
  - Pour assurer un comportement prévisible de ces données non partagées, vous redirigez uniquement vers le groupe de mise à disposition de Windows 10. Windows 10 est utilisé plus souvent par les utilisateurs dans leur travail quotidien. Les utilisateurs n'accèdent qu'occasionnellement aux applications fournies par Windows Server. Par ailleurs, dans ce cas, les données non partagées sont plus pertinentes dans un environnement de bureau plutôt qu'un environnement d'application. Par exemple, des raccourcis Bureau sont stockés dans le dossier **Bureau** et peuvent être utiles s'ils proviennent d'une machine Windows 10, mais pas depuis une machine Windows Server.
- Pour les dossiers non redirigés :
  - Vous ne souhaitez pas embarrasser vos serveurs avec les fichiers téléchargés de l'utilisateur, de sorte que vous choisissez de ne pas rediriger le dossier Téléchargements.
  - Les données d'applications individuelles peuvent entraîner des problèmes de compatibilité et de performances, vous décidez ainsi de ne pas rediriger le dossier Données d'application.

Pour de plus amples informations sur la redirection de dossiers, consultez les rubriques Présentation de la redirection de dossiers, des fichiers hors connexion et des profils utilisateur itinérants.

### Redirection de dossiers et exclusions

Dans Citrix Profile Management (mais pas dans Studio), une amélioration des performances vous permet d'éviter que les dossiers soient traités à l'aide d'exclusions. Si vous utilisez cette fonctionnalité, n'excluez pas les dossiers redirigés. Les fonctionnalités de redirection et d'exclusion de dossiers fonctionnent conjointement. Ceci garantit qu'aucun dossier redirigé n'est exclu et permet à Profile Management de les replacer dans la structure de dossiers du profil et de conserver l'intégrité des données, si vous décidez de ne pas de les rediriger ultérieurement. Pour plus d'informations sur les exclusions, veuillez consulter la section Inclure et exclure des éléments.

## Enregistrement de VDA

June 27, 2024

### Introduction

> **Remarque :**
>
> Dans un environnement local, les VDA sont enregistrés auprès d'un Delivery Controller. Dans un environnement de service Citrix Cloud, les VDA sont enregistrés auprès d'un Cloud Connector. Dans un environnement hybride, certains VDA sont enregistrés auprès d'un Delivery Controller tandis que d'autres sont enregistrés auprès d'un Cloud Connector.

Avant qu'un VDA puisse être utilisé, il doit s'enregistrer (établir la communication) auprès d'un ou de plusieurs Controller ou Cloud Connector sur le site. Le VDA trouve un Controller ou un Connector en vérifiant une liste appelée `ListofDDCs`. La liste `ListOfDDCs` sur un VDA se compose d'une ou plusieurs entrées DNS qui pointent le VDA vers des Controller ou Cloud Connector sur le site. Pour assurer l'équilibrage de charge, le VDA répartit automatiquement les connexions de manière équitable entre les Controller ou Cloud Connector dans la liste.

Pourquoi l'enregistrement de VDA est-il si important ?

- Du point de vue de la sécurité, l'enregistrement est une opération sensible. Vous établissez une connexion entre le Controller ou Cloud Connector et le VDA. Pour une telle opération délicate, le comportement attendu est le rejet de la connexion si toutes les conditions requises ne sont pas remplies. Vous établissez en fait deux canaux de communication distincts : VDA vers Controller

ou Cloud Connector et Controller ou Cloud Connector vers VDA. La connexion utilise Kerberos, donc les problèmes de synchronisation de l'heure et d'appartenance de domaine bloqueront le processus. Kerberos utilise les noms principaux de service (SPN), donc vous ne pouvez pas utiliser d'adresse IP ou de nom d'hôte avec équilibrage de charge.

- Si un VDA ne dispose pas d'informations précises et à jour sur le Controller ou Cloud Connector lorsque vous ajoutez et supprimez des Controller ou Cloud Connector, le VDA peut rejeter les lancements de session qui sont négociés par un Controller ou Cloud Connector non répertorié. La présence d'entrées non valides peut retarder le démarrage du logiciel système du bureau virtuel. Un VDA n'accepte pas de connexion à partir d'un Controller ou Cloud Connector inconnu et non fiable.

En plus de la `ListofDDCs`, la `ListOfSIDs` (ID de sécurité) indique les machines de `ListofDDCs` qui sont fiables. La liste `ListofSIDs` peut être utilisée pour réduire la charge sur Active Directory ou pour éviter des menaces de sécurité provenant d'un serveur DNS non fiable. Pour plus d'informations, consultez la section ListOfSIDs ci-dessous.

Si une liste `ListofDDCs` spécifie plusieurs Controller ou Cloud Connector, le VDA tente de s'y connecter aléatoirement. Dans un déploiement sur site, la liste `ListofDDCs` peut également contenir des groupes de Controller. Le VDA tente de se connecter à chaque Controller dans un groupe avant de passer à d'autres entrées dans la liste `ListofDDCs`.

Citrix Virtual Apps and Desktops teste automatiquement la connectivité avec les Controller ou Cloud Connector configurés lors de l'installation de VDA. Les erreurs sont affichées si un Controller ou Cloud Connector n'est pas accessible. Si vous ignorez un message d'avertissement indiquant qu'un Controller ou Cloud Connector ne peut pas être contacté (ou lorsque vous ne spécifiez pas d'adresses de Controller ou Cloud Connector au cours de l'installation de VDA), des messages de rappel sont envoyés.

### Méthodes de configuration des adresses de Controller ou Cloud Connector

L'administrateur décide de la méthode de configuration à utiliser lorsque le VDA s'enregistre pour la première fois (enregistrement initial). Lors de l'enregistrement initial, un cache permanent est créé sur le VDA. Lors des enregistrements ultérieurs, le VDA récupère la liste de Controller ou Cloud Connector à partir de ce cache local, sauf si une modification de configuration est détectée.

La meilleure façon de récupérer cette liste lors des enregistrements ultérieurs consiste à utiliser la fonction de mise à jour automatique. Par défaut, la mise à jour automatique est activée. Pour plus d'informations, consultez Mise à jour automatique.

Il existe plusieurs méthodes de configuration des adresses de Controller ou Cloud Connector sur un VDA.

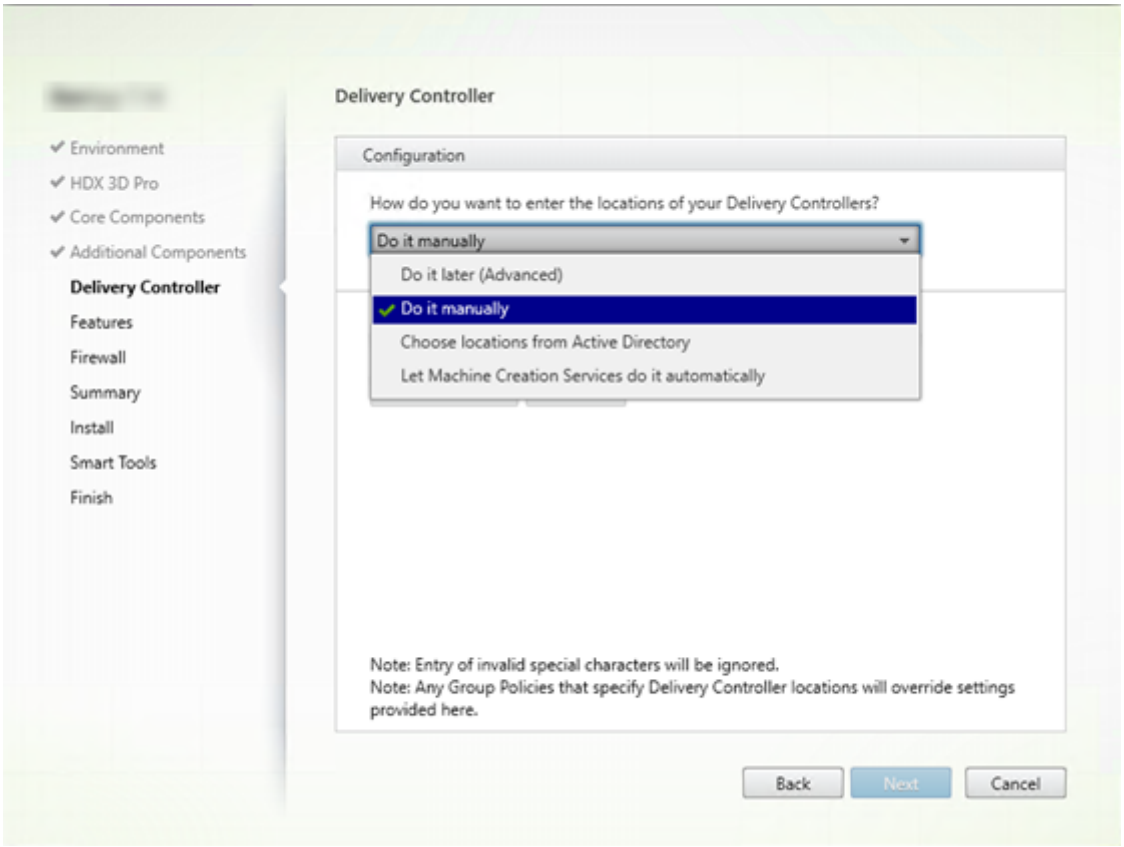
- Basée une stratégie (LGPO ou GPO)

- Basée sur le Registre (manuelle, préférences de stratégie de groupe ou GPP, spécifiée lors de l'installation de VDA)
- Basée sur l'unité d'organisation Active Directory (découverte d'unité d'organisation ancienne génération)
- Basée sur MCS (personality.ini)

Vous spécifiez la méthode d'enregistrement initial lorsque vous installez un VDA. (Si vous désactivez la mise à jour automatique, la méthode que vous sélectionnez lors de l'installation d'un VDA est également utilisée pour les enregistrements ultérieurs.)

Le graphique suivant montre la page **Delivery Controller** de l'Assistant d'installation de VDA.




**Basée sur une stratégie (LGPO/GPO)**

Citrix vous recommande d'utiliser un objet de stratégie de groupe (GPO) pour l'enregistrement initial de VDA. Cette méthode a la priorité la plus élevée. (Bien que la mise à jour automatique soit répertoriée comme priorité la plus élevée, la mise à jour automatique est utilisée uniquement après l'enregistrement initial). L'enregistrement basé sur une stratégie offre les avantages que représente l'utilisation de la stratégie de groupe pour la configuration en termes de centralisation.

Pour spécifier cette méthode, effectuez les deux étapes suivantes :

- Sur la page **Delivery Controller** dans l'assistant d'installation VDA, sélectionnez **Le faire plus tard (avancé)**. L'assistant vous rappelle plusieurs fois de spécifier les adresses de Controller, même si vous ne les spécifiez pas lors de l'installation de VDA. (L'enregistrement VDA est particulièrement important.)
- Activez ou désactivez l'enregistrement de VDA basé sur une stratégie par le biais de la stratégie Citrix avec le paramètre `Virtual Delivery Agent Settings > Controllers`. (Si la sécurité est votre priorité principale, utilisez le paramètre `Virtual Delivery Agent Settings > Controller SIDs`.)

Ce paramètre est stocké sous `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`.

#### Basé sur registre

Pour spécifier cette méthode, effectuez une des étapes suivantes :

- Sur la page **Delivery Controller** dans l'assistant d'installation VDA, sélectionnez **Effectuer manuellement**. Ensuite, entrez le nom de domaine complet d'un Controller installé, puis cliquez sur **Ajouter**. Si vous avez installé des Controller supplémentaires, ajoutez leurs adresses.
- Pour une installation de VDA par ligne de commande, utilisez l'option /controllers et spécifiez les noms de domaine complets des Controller ou Cloud Connector installés.

Ces informations sont stockées dans la valeur de Registre `ListOfDDCs` sous la clé de Registre `HKLM\Software\Citrix\VirtualDesktopAgent` ou `HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`.

Vous pouvez également configurer cette clé de Registre manuellement ou utiliser les préférences de stratégie de groupe (GPP). Cette méthode peut être préférable à la méthode basée sur la stratégie (par exemple, si vous souhaitez un traitement conditionnel de différents Controller ou Cloud Connector, tel que : utiliser XDC-001 pour les noms d'ordinateur qui commencent par XDW-001-).

Mettez à jour la clé de registre `ListOfDDCs`, qui répertorie les noms de domaine complets de tous les Controller ou Cloud Connector du site. (Cette clé est l'équivalent de l'unité d'organisation du site Active Directory.)

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

Si l'emplacement de Registre `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent` contient les clés `ListOfDDCs` et `FarmGUID`, `ListOfDDCs` est utilisé pour la découverte du Controller ou du Cloud Connector. `FarmGUID` est présent si une unité d'organisation du site a été spécifiée lors de l'installation du VDA. (Elle peut être utilisée dans les déploiements d'ancienne génération).

Si vous le souhaitez, mettez à jour la clé de Registre `ListOfSIDs` (pour plus d'informations, consultez la section ListOfSIDs) :

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs` (`REG_SZ`)

Rappel : si vous activez également l'enregistrement de VDA via une stratégie Citrix, cette configuration remplace les paramètres que vous spécifiez lors de l'installation de VDA, car il s'agit d'une méthode à priorité plus élevée.

#### Basée sur l'unité d'organisation Active Directory (ancienne génération)

Cette méthode est prise en charge principalement pour la rétrocompatibilité et n'est pas recommandée. Si vous l'utilisez toujours, Citrix suggère de changer de méthode.

Pour spécifier cette méthode, effectuez les deux étapes suivantes :

- Sur la page **Delivery Controller** dans l'assistant d'installation VDA, sélectionnez **Choisir les emplacements d'Active Directory**.
- Utilisez le script `Set-ADControllerDiscovery.ps1` (disponible sur chaque Controller). Configurez également l'entrée de Registre `FarmGuid` sur chaque VDA de manière à pointer vers l'unité d'organisation correcte. Ce paramètre peut être configuré à l'aide de la stratégie de groupe.

#### Basée sur MCS

Si vous utilisez MCS pour provisionner des machines virtuelles, MCS configure la liste des Controller ou Cloud Connector. Cette fonctionnalité fonctionne avec la mise à jour automatique. Lors de la création du catalogue, MCS injecte la liste des Controller ou Cloud Connector dans le fichier `Personality.ini` lors du provisioning initial. La mise à jour automatique permet de conserver la liste à jour.

Pour spécifier cette méthode, sur la page **Delivery Controller** dans l'assistant d'installation VDA, sélectionnez **Laisser Machine Creation Services effectuer ceci automatiquement**.

#### Recommandations

Recommandations :

- Utilisez la méthode de stratégie de groupe pour l'enregistrement initial.
- Utilisez la mise à jour automatique (activée par défaut) pour garder votre liste de Controller à jour.

- Dans un déploiement multi-zone, utilisez la stratégie de groupe pour la configuration initiale (avec au moins deux Controller ou Cloud Connector). Pointez les VDA vers des Controller ou Cloud Connector locaux, dans leur zone. Utilisez la mise à jour automatique pour assurer leur mise à jour. La mise à jour automatique optimise automatiquement la liste `ListofDDCs` pour les VDA dans des zones satellite.
- Répertoriez plusieurs Delivery Controller sur la clé de registre `ListOfDDCs`, séparés par un espace ou une virgule, pour éviter les problèmes d'enregistrement si un Controller n'est pas disponible. Par exemple :

```
DDC7x.xd.local DDC7xHA.xd.local

32-bit: HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
    ListOfDDCs

HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
    ListOfDDCs (REG_SZ)
<!--NeedCopy-->
```

- Assurez-vous que toutes les valeurs répertoriées sous `ListofDDCs` correspondent à un nom de domaine complet valide afin d'éviter les retards d'enregistrement au démarrage.

### Mise à jour automatique

La mise à jour automatique (introduite dans XenApp et XenDesktop 7.6) est activée par défaut. Il s'agit de la méthode la plus efficace pour assurer la mise à jour de vos enregistrements de VDA. Bien que la mise à jour automatique ne soit pas utilisée pour l'enregistrement initial, le logiciel de mise à jour automatique télécharge et stocke la liste `ListofDDCs` dans un cache permanent sur le VDA lors de l'enregistrement initial. Ce processus est effectué pour chaque VDA. Le cache contient également des informations sur la stratégie de la machine, ce qui garantit que les paramètres de stratégie sont conservés après les redémarrages.

La mise à jour automatique est prise en charge lors de l'utilisation de MCS ou Citrix Provisioning pour provisionner des machines, sauf pour le cache côté serveur Citrix Provisioning. Le cache côté serveur n'est pas un scénario courant car il n'existe pas de stockage permanent pour le cache de mise à jour automatique.

Pour spécifier cette méthode :

- Activez ou désactivez la mise à jour automatique via une stratégie Citrix contenant le paramètre `Virtual Delivery Agent Settings` > `Enable auto update of Controllers`. Ce paramètre est activé par défaut.

Fonctionnement

- Chaque fois qu'un VDA se réenregistre (par exemple, après un redémarrage de machine), le cache est mis à jour. Chaque Controller ou Cloud Connector vérifie également la base de données du site toutes les 90 minutes. Si un Controller ou Cloud Connector a été ajouté ou supprimé depuis la dernière vérification, ou si une modification de stratégie s'est produite qui affecte l'enregistrement du VDA, le Controller ou Cloud Connector envoie une liste actualisée vers les VDA enregistrés et le cache est mis à jour. Le VDA accepte les connexions provenant de tous les Controller ou Cloud Connector figurant dans la liste mise en cache le plus récemment.
- Si un VDA reçoit une liste qui ne comprend pas le Controller ou Cloud Connector auprès duquel il est enregistré (en d'autres termes, ce Controller ou Cloud Connector a été supprimé du site), le VDA s'enregistre de nouveau, en choisissant parmi les Controller ou Cloud Connector dans la liste `ListofDDCs`.

Exemple :

- Un déploiement dispose de trois Controller : A B et C. Un VDA s'enregistre auprès du Controller B (qui a été spécifié lors de l'installation du VDA).
- Deux Controller (D et E) sont ajoutés au site plus tard. Dans les 90 minutes qui suivent, le VDA reçoit les listes mises à jour et accepte les connexions provenant des Controller A, B, C, D et E. (La charge ne sera pas répartie de manière égale sur tous les Controller tant que les VDA ne sont pas redémarrés.)
- Plus tard, le Controller B est déplacé vers un autre site. Dans les 90 minutes qui suivent, le VDA sur le site d'origine reçoit les listes mises à jour car un Controller a été modifié depuis la dernière vérification. Le VDA qui s'est enregistré initialement auprès du Controller B (qui ne figure plus sur la liste) se réenregistre en choisissant parmi les Controller disponibles dans la liste actuelle (A, C, D et E).

Dans un déploiement multi-zone, la mise à jour automatique dans une zone satellite commence par mettre automatiquement en cache tous les Controller locaux. Tous les Controller de la zone principale sont mis en cache dans un groupe de secours. Si aucun Controller local de la zone satellite n'est disponible, une tentative d'enregistrement avec les Controller de la zone principale est effectuée.

Comme illustré dans l'exemple suivant, le fichier de cache contient des noms d'hôte et une liste d'ID de sécurité (`ListofSIDs`). Le VDA n'interroge pas les SID, ce qui réduit la charge d'Active Directory.


Vous pouvez récupérer le fichier cache avec un appel WMI. Toutefois, il est stocké dans un emplacement lisible uniquement par le compte système.

> **Important :**
>
> Cette information est fournie uniquement à titre indicatif. NE MODIFIEZ PAS CE FICHIER. Toute modification de ce fichier ou dossier entraîne une configuration non prise en charge.

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation"-Class "
Citrix_VirtualDesktopInfo"-Property "PersistentDataLocation"
```

Si vous avez besoin de configurer manuellement la `ListofSIDs` pour des raisons de sécurité (et non à des fins de réduction de la charge d'Active Directory), vous ne pouvez pas utiliser la fonctionnalité de mise à jour automatique. Pour plus amples informations, consultez la section ListOfSIDs.

#### Exception à la priorité de mise à jour automatique

Bien que la mise à jour automatique ait généralement la priorité la plus élevée de toutes les méthodes d'enregistrement de VDA et remplace les paramètres des autres méthodes, il existe une exception. Les éléments `NonAutoListOfDDCs` dans le cache spécifient la méthode de configuration initiale de VDA. La mise à jour automatique contrôle ces informations. Si la méthode d'enregistrement initial est modifiée, le processus d'enregistrement ignore la mise à jour automatique et utilise parmi les méthodes configurées celle dont la priorité est la plus proche. Ce processus peut s'avérer utile lorsque vous déplacez un VDA vers un autre site (par exemple, lors d'une récupération d'urgence).

### Considérations liées à la configuration

Regardez une configuration d'enregistrement VDA courante.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Regardez les étapes d'un enregistrement VDA.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Tenez compte des éléments suivants lors de la configuration d'éléments pouvant affecter l'enregistrement de VDA.

#### Adresses de Controller ou Cloud Connector

Quelle que soit la méthode que vous utilisez pour spécifier des Controller ou Cloud Connector, Citrix recommande d'utiliser une adresse de nom de domaine complet. Une adresse IP n'est pas considérée comme une configuration de confiance, car il est plus facile de compromettre une adresse IP qu'un enregistrement DNS. Si vous remplissez la liste `ListofSIDs` manuellement, vous pouvez utiliser une adresse IP dans une liste `ListofDDCs`. Cependant, un nom de domaine complet est toujours recommandé.

#### Équilibrage de charge

Comme indiqué précédemment, le VDA répartit automatiquement les connexions de manière équitable entre les Controller ou Cloud Connector dans la liste `ListofDDCs`. La fonctionnalité d'équilibrage de charge et de basculement est intégrée au protocole CBP (Citrix Brokering Protocol). Si vous spécifiez plusieurs Controller ou Cloud Connector dans votre configuration, l'enregistrement bascule automatiquement de l'un à l'autre, si nécessaire. Avec la mise à jour automatique, le basculement automatique se produit automatiquement pour tous les VDA.

Pour des raisons de sécurité, vous ne pouvez pas utiliser un équilibreur de charge réseau, tel que Citrix ADC. L'enregistrement de VDA utilise l'authentification mutuelle Kerberos, où le client (VDA) doit prouver son identité au service (Controller). Toutefois, le Controller ou Cloud Connector doit prouver son identité au VDA. Cela signifie que le VDA et le Controller ou Cloud Connector agissent en tant que serveur et client en même temps. Comme indiqué au début de cet article, il existe deux canaux de communications : VDA vers Controller/Cloud Connector et Controller/Cloud Connector vers VDA.

Un composant de ce processus est appelé Nom de service principal (SPN) ; il est stocké en tant que propriété dans un objet ordinateur Active Directory. Lorsque votre VDA se connecte à un Controller ou Cloud Connector, il doit spécifier avec « qui » il souhaite communiquer. Cette adresse est un SPN. Si vous utilisez une adresse IP d'équilibrage de charge, l'authentification Kerberos mutuelle reconnaît correctement que l'adresse IP n'appartient pas au Controller ou Cloud Connector attendu.

Pour plus d'informations, consultez :

- Introduction à Kerberos
- Authentification mutuelle à l'aide de Kerberos

#### La mise à jour automatique remplace CNAME

La fonctionnalité de mise à jour automatique remplace la fonction CNAME (alias DNS) des versions XenApp et XenDesktop antérieures à 7.x. La fonctionnalité CNAME est désactivée, à compter de XenApp et XenDesktop 7. Utilisez la mise à jour automatique au lieu de CNAME. (Si vous devez utiliser CNAME, consultez la section CTX137960. Pour que l'alias DNS fonctionne de manière cohérente, n'utilisez pas la mise à jour automatique et CNAME en même temps.)

#### Groupes de Controller/Cloud Connector

Dans certains scénarios, vous pouvez gérer les Controller ou Cloud Connector sous forme de groupes, avec un groupe préféré et l'autre groupe utilisé pour le basculement si tous les Controller/Cloud Connector échouent. N'oubliez pas que les Controller ou Cloud Connector sont sélectionnés de manière aléatoire dans la liste, par conséquent le regroupement peut vous aider à imposer l'utilisation de certains Controller.

Ces groupes sont destinés à être utilisés dans un seul site (et non dans plusieurs sites).

Pour spécifier des groupes de Controller/Cloud Connector, utilisez des parenthèses. Par exemple, avec quatre Controller (deux principaux et deux de sauvegarde), un regroupement peut être :

```
(XDC-001.cdz.lan XDC-002.cdz.lan)(XDC-003.cdz.lan XDC-004.cdz.lan)
```

Dans cet exemple, les Controller du premier groupe (001 et 002) sont traités en premier. S'ils échouent, les Controller du deuxième groupe (003 et 004) sont traités.

Pour XenDesktop 7.0 ou version ultérieure, vous devez effectuer une étape supplémentaire pour utiliser la fonctionnalité **Groupes d'inscription** (Registration Groups). Vous devez **interdire** la stratégie **Activer la mise à jour automatique des Controller** dans Studio.

### ListOfSIDs

La liste de Controller qu'un VDA peut contacter pour l'enregistrement est la liste `ListofDDCs`. Un VDA doit également connaître les Controller à approuver ; les VDA ne font pas automatiquement confiance aux Controller de la liste `ListofDDCs`. La liste `ListofSIDs` (ID de sécurité) identifie les Controller de confiance. Les VDA tentent de s'enregistrer uniquement avec les Controller de confiance.

Dans la plupart des environnements, la liste `ListofSIDs` est générée automatiquement à partir de la liste `ListofDDCs`. Vous pouvez utiliser une trace CDF pour lire la `ListofSIDs`.

En général, il n'est pas nécessaire de modifier manuellement la `ListofSIDs`. Il existe toutefois des exceptions. Les deux premières exceptions ne sont plus valides, car des technologies plus récentes sont disponibles.

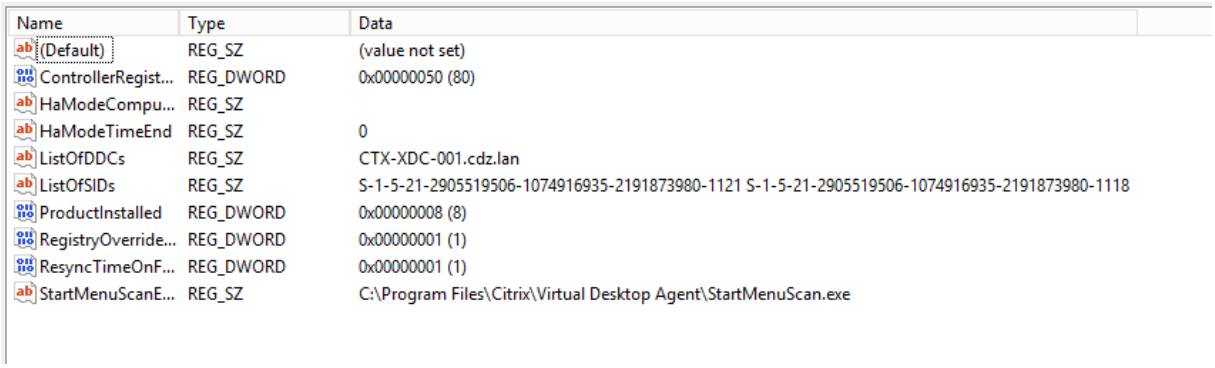
 

- **Séparer les rôles pour les Controller :** avant que les zones soient introduites dans XenApp et XenDesktop 7.7, la `ListofSIDs` était configurée manuellement lorsqu'un sous-ensemble de Controller était utilisé pour l'enregistrement. Par exemple, si vous utilisiez XDC-001 et XDC-002 en tant que brokers XML, et XDC-003 et XDC-004 pour l'enregistrement de VDA, vous deviez spécifier tous les Controller dans la liste `ListofSIDs` et XDC-003 et XDC-004 dans la liste `ListofDDCs`. Il ne s'agit pas d'une configuration typique ou recommandée. Ne l'utilisez pas dans des environnements plus récents. Utilisez plutôt les zones.
- **Réduction de la charge d'Active Directory :** avant que la fonctionnalité de mise à jour automatique ait été introduite dans XenApp et XenDesktop 7.6, la `ListofSIDs` était utilisée pour réduire la charge sur les contrôleurs de domaine. La résolution de noms DNS vers des SID pouvait être ignorée en prédéfinissant la liste `ListofSIDs`. Toutefois, la fonctionnalité de mise à jour automatique supprime le besoin d'effectuer cette opération, car ce cache permanent contient les SID. Citrix recommande de toujours activer la fonctionnalité de mise à jour automatique.
- **Sécurité :** dans certains environnements hautement sécurisés, les SID de Controller de confiance étaient configurés manuellement pour éviter les menaces de sécurité depuis un serveur DNS non fiable. Toutefois, si vous procédez ainsi, vous devez également désactiver la fonctionnalité de mise à jour automatique. Sinon, la configuration du cache permanent est utilisée.

Donc, à moins que vous ayez une bonne raison, ne modifiez pas la `ListofSIDs`.

Si vous devez modifier la liste `ListofSIDs`, créez une clé de Registre nommée `ListOfSIDs` (`REG_SZ`) sous `HKLM\Software\Citrix\VirtualDesktopAgent`. La valeur est une liste de SID de confiance, séparée par des espaces, s'il y en a plusieurs.

Dans l'exemple suivant, un Controller est utilisé pour l'enregistrement de VDA (`ListofDDCs`), mais deux Controller sont utilisés pour la négociation des connexions (liste OfSIDs).




### Recherche de contrôleur lors de l'enregistrement du VDA

Lorsqu'un VDA tente de s'enregistrer, l'agent Broker effectue d'abord une recherche DNS dans le domaine local pour s'assurer que le contrôleur spécifié peut être atteint.

Si cette recherche initiale ne trouve pas le contrôleur, l'agent Broker peut lancer une requête de secours descendante dans AD. Cette requête recherche tous les domaines et se répète fréquemment. Si l'adresse du contrôleur n'est pas valide (par exemple, l'administrateur a entré un nom de domaine complet incorrect lors de l'installation du VDA), l'activité de cette requête peut potentiellement conduire à une condition de déni de service distribué (DDoS) sur le contrôleur de domaine.

La clé de registre suivante contrôle si l'agent Broker utilise la requête de secours descendante lorsqu'il ne peut pas localiser un contrôleur pendant la recherche initiale.

`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`

- Nom :`DisableDdcWildcardNameLookup`
- Type : `DWORD`
- Valeur : `1` (par défaut) ou `0`

Lorsque la valeur est définie sur `1`, la recherche de secours est désactivée. Si la recherche initiale du contrôleur échoue, la recherche de l'agent Broker cesse. C'est le réglage par défaut.
Lorsque la valeur est définie sur `0`, la recherche de secours est activée. Si la recherche initiale du contrôleur échoue, la recherche de secours descendante est lancée.

### Séquençage des liaisons LDAP lors de l'enregistrement d'un VDA à l'aide d'un contrôleur de domaine en lecture seule

Lorsqu'un VDA s'enregistre auprès d'un contrôleur de domaine en lecture seule (RODC), le Broker Agent doit sélectionner la ou les liaisons LDAP (Light Directory Access Protocol) à ignorer. Pour effectuer cette sélection, le Broker Agent a besoin d'une clé de registre appropriée.

Si aucune clé de registre n'est fournie ou si le champ de clé de registre est vide, l'enregistrement du VDA auprès du RODC prend plus de temps car il est nécessaire de suivre la séquence de liaisons LDAP d'origine.

Pour modifier la séquence de liaisons LDAP, la clé de registre `ListofIgnoredBindings` a été ajoutée à `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`. L'utilisation de `ListofIgnoredBindings` vous permet de modifier la séquence de liaisons LDAP si nécessaire, et ainsi d'accélérer l'enregistrement du VDA auprès d'un RODC.

- Nom :`ListofIgnoredBindings`
- Type : `REG_SZ`
- Valeurs : `DefaultPath`, `DomainPath`, `PDCPath`

La valeur est une liste d'options de chemin des liaisons, chacune étant séparée par une virgule. La clé de registre ignorera toutes les valeurs qu'elle ne reconnaît pas comme valides.

### Résoudre les problèmes d'enregistrement de VDA

Comme indiqué précédemment, un VDA doit être enregistré auprès d'un Delivery Controller ou d'un Cloud Connector pour être pris en compte lors du lancement de sessions négociées. Des VDA non enregistrés peuvent entraîner une sous-utilisation des ressources disponibles. Il existe un certain nombre de raisons pour lesquelles un VDA peut ne pas être enregistré, un grand nombre d'entre elles pouvant être résolues par un administrateur. Studio offre des informations de dépannage dans l'Assistant de création de catalogue de machines, et après la création d'un groupe de mise à disposition.

- **Identification de problèmes lors de la création de catalogue de machines :** dans l'assistant Créer un catalogue de machines, lorsque vous ajoutez des machines existantes, la liste des noms de compte d'ordinateur indique si chaque machine peut être ajoutée au catalogue. Placez le pointeur de la souris sur l'icône située en regard de chaque machine pour afficher un message informatif sur cette machine.

  Si le message identifie une machine problématique, vous pouvez supprimer cette machine (à l'aide du bouton **Supprimer**) ou ajouter la machine. Par exemple, si un message indique qu'il est impossible d'obtenir des informations sur une machine (peut-être parce qu'elle n'a jamais été enregistrée), vous pouvez quand même choisir d'ajouter la machine.

  Le niveau fonctionnel d'un catalogue détermine les fonctionnalités du produit qui sont disponibles pour les machines du catalogue. L'utilisation de fonctionnalités introduites dans les nouvelles versions de produit peut nécessiter un nouveau VDA. Définir un niveau fonctionnel met toutes les fonctionnalités introduites dans cette version (et les versions ultérieures, si le niveau fonctionnel ne change pas) à disposition des machines du catalogue. Toutefois, les machines de ce catalogue avec une version antérieure de VDA ne pourront pas s'enregistrer.

- **Identification de problèmes après la création de groupes de mise à disposition :** une fois que vous avez créé un groupe de mise à disposition, Studio affiche davantage de détails sur les machines associées à ce groupe.

  Le panneau de détails pour un groupe de mise à disposition indique le nombre de machines qui devraient être enregistrées, mais ne le sont pas. En d'autres termes, une ou plusieurs machines peuvent être sous tension et pas en mode de maintenance, mais pas enregistrées auprès d'un Controller. Lors de l'affichage d'une machine « non enregistrée », mais qui devrait l'être, l'onglet **Dépannage** dans le panneau Détails fournit des causes possibles et les actions correctives recommandées.

#### Plus d'informations sur le dépannage de l'enregistrement de VDA

- Pour de plus amples informations sur les niveaux fonctionnels, consultez la section Versions VDA et niveaux fonctionnels.

- Pour plus d'informations sur le dépannage de l'enregistrement de VDA, voir l'article CTX136668.
- Vous pouvez également utiliser les analyses de l'état de santé Citrix pour résoudre les problèmes d'enregistrement de VDA et de lancement de session. Pour de plus amples informations, consultez la section À propos des contrôles d'intégrité.

## IP virtuelle et boucle virtuelle

June 27, 2024

> **Important :**
>
> - Windows 10 Enterprise multi-sessions ne prend pas en charge Remote Desktop IP Virtualization (Virtual IP) et nous ne prenons pas en charge Remote Desktop IP Virtualization ni Virtual Loopback sur Windows 10 Enterprise multi-sessions.
> - Remote Desktop IP Virtualization (Virtual IP) n'est pas pris en charge sur les machines hébergées dans le cloud.
>
>  Pour de plus amples informations, consultez la documentation de Microsoft.

Les fonctionnalités de Remote Desktop IP Virtualization et Virtual Loopback sont prises en charge sur les machines Windows Server 2016, Windows Server 2019 et Windows Server 2022. Elles ne sont pas prises en charge par les machines avec système d'exploitation de bureau Windows.

La fonctionnalité d'adresse Remote Desktop IP Virtualization de Microsoft propose une application publiée avec une adresse IP unique attribuée dynamiquement à chaque session. La fonction Virtual Loopback de Citrix vous permet de configurer des applications qui dépendent des communications avec localhost (127.0.0.1 par défaut) pour utiliser une adresse de bouclage virtuelle unique dans la plage localhost (127.*).

Certaines applications, telles que les applications de type CRM ou CTI (Computer Telephony Integration), utilisent une adresse IP pour l'adressage, l'identification, les licences, ou à d'autres fins. Elles nécessitent par conséquent une adresse IP unique ou adresse de bouclage. D'autres applications peuvent se lier à un port statique, c'est pourquoi les tentatives de démarrage des instances d'une application dans un environnement multi-utilisateur échouent car le port est utilisé. Pour assurer un fonctionnement correct de ces applications dans l'environnement Citrix Virtual Apps, chaque machine nécessite une adresse IP unique.

Remote Desktop IP Virtualization et Virtual Loopback sont des fonctionnalités indépendantes l'une de l'autre. Vous pouvez sélectionnez ces deux options ou l'une ou l'autre.

Résumé des actions de l'administrateur :

- Pour utiliser la fonction Remote Desktop IP Virtualization de Microsoft, activez-la et configurez-la sur le serveur Windows. (Les paramètres de stratégie Citrix ne sont pas nécessaires.)
- Pour utiliser le bouclage virtuel Citrix, configurez deux paramètres dans une stratégie Citrix.

### Remote Desktop IP Virtualization (Virtual IP)

Lorsque la fonction Remote Desktop IP Virtualization est activée et configurée sur le serveur Windows, chaque application configurée en cours d'exécution dans une session dispose d'une adresse unique. Les utilisateurs peuvent accéder à ces applications sur un serveur Citrix Virtual Apps comme ils accèdent à toute autre application publiée. Un processus nécessite Remote Desktop IP Virtualization dans l'un des cas suivants :

- Le processus utilise un numéro de port TCP fixe
- Le processus utilise des sockets Windows et nécessite une adresse IP unique ou un numéro de port TCP spécifié

Pour déterminer si une application doit utiliser des adresses Remote Desktop IP Virtualization, procédez comme suit :

1. Obtenez l'outil **TCPView** auprès de Microsoft. Cet outil répertorie toutes les applications liées à des adresses IP et ports spécifiques. Pour en savoir plus sur TCPView, consultez la documentation de Microsoft.
2. Désactivez la fonction **Résoudre les adresses IP** afin d'afficher les adresses au lieu des noms d'hôtes.
3. Lancez l'application et utilisez **TCPView** pour voir quelles adresses IP et ports sont ouverts par celle-ci ainsi que les noms des processus qui ouvrent ces ports.
4. Configurez tous les processus qui ouvrent l'adresse IP du serveur, 0.0.0.0 ou 127.0.0.1.
5. Lancez une autre instance de l'application afin de vous assurer qu'elle n'ouvre pas la même adresse IP sur un port différent.

#### Fonctionnement de la virtualisation IP Microsoft Remote Desktop (RD)

- L'adressage IP virtuel doit être activé sur le serveur Microsoft.

  Par exemple, dans un environnement Windows Server 2016, à partir du Gestionnaire de serveur, développez **Services Bureau à distance > Connexions hôtes de session Bureau à distance** pour activer la fonctionnalité de virtualisation IP des services Bureau à distance et configurer les paramètres pour attribuer dynamiquement des adresses IP à l'aide du serveur DHCP (Dynamic Host Configuration Protocol) par session ou par programme. Pour en savoir plus sur la configuration Remote Desktop IP Virtualization, consultez la documentation de Microsoft.

- Lorsque cette fonctionnalité est activée, le serveur demande des adresses IP attribuées dynamiquement auprès du serveur DHCP au démarrage de la session.
- La fonction **RD IP Virtualization** attribue les adresses IP aux connexions de bureau à distance par session ou par programme. Si vous attribuez des adresses IP à de multiples programmes, ces derniers partagent une adresse IP par session.
- Une fois qu'une adresse est attribuée à une session, la session utilise l'adresse virtuelle plutôt que l'adresse IP principale pour le système chaque fois que les appels suivants sont effectués : `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

Lors de l'utilisation de la fonctionnalité de virtualisation d'adresses IP de Microsoft dans la configuration d'hôte de session Bureau à distance, les applications sont liées à des adresses IP spécifiques par l'insertion d'un composant « filtre » entre l'application et les appels de fonction Winsock. L'application ne voit alors que l'adresse IP correcte à utiliser. Toute tentative d'écoute de communications TCP ou UDP par l'application est liée à l'adresse IP virtuelle (ou adresse de bouclage) qui lui est attribuée automatiquement. Toutes les connexions ouvertes par l'application sont établies au départ par l'adresse IP liée à l'application.

Pour les fonctions qui renvoient une adresse, telle que `GetAddrInfo()` (contrôlée par une stratégie Windows), si l'adresse IP de l'hôte local est requise, Remote Desktop IP Virtualization examine l'adresse IP renvoyée et la remplace par l'adresse Remote Desktop IP Virtualization de la session. Les applications qui tentent d'obtenir l'adresse IP du serveur local à travers ce type de noms de fonctions n'obtiennent que l'adresse Remote Desktop IP Virtualization unique attribuée à la session. Cette adresse IP est souvent utilisée dans les appels de socket suivants, tels que bind ou connect. Pour plus d'informations sur les stratégies Windows, consultez l'article RDS IP Virtualization in Windows Server.

Une application demande souvent à se lier à un port pour procéder à une écoute de l'adresse « 0.0.0.0 ». Lorsque c'est le cas et qu'une application utilise un port statique, vous ne pouvez pas ouvrir plus d'une instance de celle-ci. La fonction d'adresse Remote Desktop IP Virtualization recherche également 0.0.0.0 dans ces types d'appels. Il modifie l'appel pour écouter sur l'adresse Remote Desktop IP Virtualization spécifique, ce qui permet à plusieurs applications d'écouter sur le même port sur le même ordinateur, car elles écoutent toutes sur des adresses différentes. L'appel est modifié uniquement s'il se trouve dans une session ICA et que la fonction d'adresse Remote Desktop IP Virtualization est activée. Par exemple, si deux instances d'une application exécutées dans des sessions différentes tentent toutes deux de se lier à toutes les interfaces (0.0.0.0) et à un port spécifique (par exemple, 9000), elles sont liées à VIPAddress1:9000 et VIPAddress2:9000, sans aucun conflit.

### Bouclage virtuel

L'activation des paramètres de **stratégie de bouclage Remote Desktop IP Virtualization de Citrix** permettent à chaque session de disposer de sa propre adresse de bouclage pour les communications. Lorsqu'une application utilise l'adresse localhost (valeur par défaut = 127.0.0.1) dans un appel Winsock, la fonctionnalité de bouclage virtuel remplace simplement 127.0.0.1 par 127.X.X.X, où X.X.X représente l'ID de session + 1. Par exemple, 127.0.0.8. pour un ID session de 7. Dans le cas peu probable où l'ID session dépasse le quatrième octet (plus de 255), l'adresse passe à l'octet suivant (127.0.1.0), jusqu'à 127.255.255.255 maximum.

Un processus nécessite le bouclage virtuel dans l'un des cas suivants :

- Le processus utilise l'adresse de bouclage de socket Windows 127.0.0.1 (localhost)
- Le processus utilise un numéro de port TCP fixe

Utilisez les paramètres de stratégie de bouclage virtuel pour les applications qui utilisent une adresse de bouclage pour la communication entre les processus. Aucune configuration supplémentaire n'est requise. Le bouclage virtuel n'a pas de dépendance à l'égard des adresses IP virtuelles, de sorte que vous n'avez pas à configurer le serveur Microsoft.

- Prise en charge du bouclage d'adresse IP virtuelle. Lorsqu'il est activé, ce paramètre de stratégie permet à chaque session de disposer de sa propre adresse de bouclage virtuel. Cette option est désactivée par défaut. Cette fonctionnalité ne s'applique qu'aux applications spécifiées avec le paramètre de stratégie Liste de programmes de bouclage virtuel d'adresse IP virtuelle.
- Liste de programmes de bouclage virtuel d'adresse IP virtuelle. Ce paramètre de stratégie spécifie les applications qui utilisent la fonctionnalité de bouclage d'adresse IP virtuelle. Ce paramètre ne s'applique que lorsque le paramètre de stratégie de prise en charge du bouclage d'adresse IP virtuelle est activé.

#### Fonction connexe

Vous pouvez utiliser les paramètres de registre suivants pour vous assurer que le bouclage virtuel est préféré aux adresses IP virtuelles. Cette fonctionnalité s'appelle un bouclage par défaut. Soyez, toutefois, prudent :

- Utilisez le bouclage par défaut uniquement si les adresses IP virtuelles et le bouclage virtuel sont activés. Sinon, vous risquez d'obtenir des résultats inattendus.
- Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir que les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre peuvent être résolus. Vous

utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Exécutez regedit sur les serveurs sur lesquels les applications résident.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- Nom : PreferLoopback, Type : REG_DWORD, Données : 1
- Nom : PreferLoopbackProcesses, Type : REG_MULTI_SZ, Données :<liste des processus>

## Zones

June 27, 2024

> **Remarque :**
>
> Vous pouvez gérer votre déploiement de Citrix Virtual Apps and Desktops à l'aide de deux consoles de gestion : Web Studio (console basée sur le Web) et Citrix Studio (console basée sur Windows). Cet article ne concerne que Web Studio. Pour plus d'informations sur Citrix Studio, consultez l'article équivalent dans Citrix Virtual Apps and Desktops 7 2212 ou version antérieure.

Les déploiements répartis sur différents emplacements géographiques et connectés à un réseau étendu peuvent rencontrer des problèmes de latence réseau et de fiabilité. Il existe deux options pour pallier ces problèmes :

- Déployer plusieurs sites, chacun avec sa propre base de données de site SQL Server.

  Cette option est recommandée pour les déploiements de grande taille. Plusieurs sites sont gérés séparément et chacun requiert sa propre base de données de site SQL Server. Chaque site est un déploiement Citrix Virtual Apps distinct.

- Configurer plusieurs zones au sein d'un seul site.

  La configuration de zones peut aider les utilisateurs situés dans des régions éloignées à se connecter à des ressources sans que leurs connexions soient obligées de traverser des segments importants de réseau étendu. L'utilisation de zones permet une gestion efficace de site à partir d'une seule console Web Studio, de Citrix Director et de la base de données du site. Vous économisez ainsi les coûts liés au déploiement, au personnel, aux licences et à l'exploitation de sites contenant des bases de données distinctes dans des emplacements distants.

  Les zones peuvent s'avérer utiles dans les déploiements de toutes tailles. Vous pouvez utiliser des zones pour que les applications et les bureaux se trouvent à proximité des utilisateurs finaux, ce qui améliore les performances. Une zone peut disposer d'un ou de plusieurs Controller

installés localement pour assurer la redondance et la résilience, mais cette configuration n'est pas obligatoire.

Le nombre de Controller configurés sur le site peut affecter les performances de certaines opérations, telles que l'ajout de nouveaux Controller au site lui-même. Pour éviter ce problème, nous vous recommandons de limiter le nombre de zones de votre site Citrix Virtual Apps ou Citrix Virtual Desktops Site à un maximum de 50.

Lorsque la latence du réseau de vos zones est supérieure à 250 ms (RTT), nous vous recommandons de déployer plusieurs sites plutôt que des zones.

Dans cet article, le terme « local » fait référence à la zone dont il est question. Par exemple, « Un VDA s'enregistre auprès d'un Controller local » signifie qu'un VDA s'enregistre auprès d'un Controller dans la zone dans laquelle le VDA est situé.

Les zones de cette version sont semblables, mais pas identiques aux zones de XenApp 6.5 et versions antérieures. Par exemple, dans cette implémentation de zones, il n'existe aucun collecteur de données. Tous les Controller du site communiquent avec une seule base de données du site dans la zone principale. En outre, les zones de basculement et les zones préférées fonctionnent différemment dans cette version.

## Types de zone

Un site dispose toujours d'une zone principale. Il peut également disposer d'une ou de plusieurs zones satellite. Les zones satellite peuvent être utilisées pour la récupération d'urgence, des centres de données distants, des succursales, un cloud ou une zone de disponibilité dans un cloud.

**Zone principale :**

Le nom par défaut de la zone principale est « Primary » (Principal). Cette zone contient la base de données du site SQL Server (et des serveurs SQL haute disponibilité, le cas échéant), Web Studio, Director, StoreFront, le serveur de licences Citrix et Citrix Gateway. Gardez toujours la base de données du site dans la zone principale.

La zone principale doit avoir au moins deux Controller pour assurer la redondance. La zone principale peut disposer de VDA avec des applications étroitement liées à la base de données et à l'infrastructure.

**Zone satellite :**

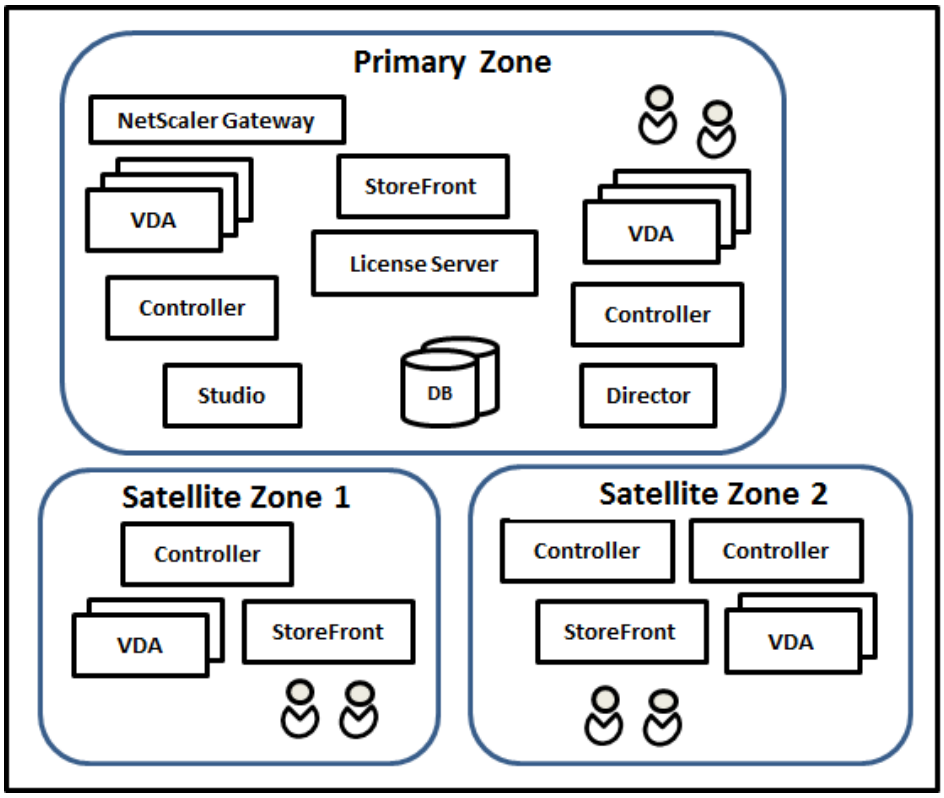
Une zone satellite contient un ou plusieurs VDA, Controller, serveurs StoreFront et serveurs Citrix Gateway. Dans des conditions de fonctionnement normales, les Controller d'une zone satellite communiquent directement avec la base de données située dans la zone principale.

Une zone satellite, en particulier une zone de grande taille, peut également contenir un hyperviseur qui est utilisé pour provisionner et stocker des machines pour cette zone. Lorsque vous configurez

une zone satellite, vous pouvez lui associer une connexion à un hyperviseur ou à un autre service (Assurez-vous que les catalogues qui utilisent cette connexion se trouvent dans la même zone).

Un site peut contenir différentes configurations de zones satellite, en fonction de vos besoins et de votre environnement. La figure suivante illustre une zone principale et des exemples de zones satellite.




Dans l'illustration :

- **Zone principale :** contient deux Controller, Web Studio, Director, StoreFront, le serveur de licences et la base de données du site (plus des déploiements SQL Server haute disponibilité). La zone principale contient également plusieurs VDA et un boîtier Citrix Gateway.
- **Zone satellite 1 - VDA avec Controller :** la zone satellite 1 contient un Controller, des VDA et un serveur StoreFront. Les VDA de cette zone satellite s'enregistrent auprès du Controller local. Le Controller local communique avec la base de données du site et le serveur de licences de la zone principale.

  Si le réseau étendu échoue, la fonctionnalité de cache d'hôte local permet au Controller de la zone satellite de continuer la négociation des connexions avec les VDA de cette zone. Un tel déploiement peut être efficace dans un bureau où les utilisateurs utilisent un site StoreFront local et le Controller local pour accéder à leurs ressources locales.
- **Zone satellite 2 - VDA avec Controller redondants :** la zone satellite 2 contient deux Controller, des VDA et un serveur StoreFront. Il s'agit du type de zone le plus robuste, offrant une protection

contre un échec simultané du réseau étendu et de l'un des Controller locaux.

### Enregistrement des VDA et basculement des Controller

Dans un site contenant des zones principale et satellite, avec des VDA à la version 7.7 au minimum :

- Un VDA de la zone principale s'enregistre auprès d'un Controller de la zone principale. Un VDA de la zone principale ne tente jamais de s'enregistrer auprès d'un Controller situé dans une zone satellite.
- Un VDA situé dans une zone satellite s'enregistre auprès d'un Controller local, si possible (Il est considéré comme Controller préféré). Si aucun Controller local n'est disponible (par exemple, lorsque les Controller locaux ne peuvent pas accepter d'enregistrements VDA supplémentaires ou si les Controller locaux ont échoué), le VDA tente de s'enregistrer auprès d'un Controller de la zone principale. Dans ce cas, le VDA reste dans la zone principale sans être enregistré, même si un Controller de la zone satellite devient de nouveau disponible. Un VDA situé dans une zone satellite ne tente jamais de s'enregistrer auprès d'un Controller situé dans une autre zone satellite.
- Lorsque la mise à jour automatique est activée pour la découverte VDA de Controller, et que vous spécifiez une liste d'adresses de Controller lors de l'installation du VDA, un Controller est sélectionné de façon aléatoire à partir de cette liste pour l'enregistrement initial (quelle que soit la zone dans laquelle le Controller réside). Une fois que la machine avec ce VDA est redémarrée, le VDA s'enregistre de préférence auprès d'un Controller de sa zone locale.
- Si un Controller d'une zone satellite échoue, il bascule vers un autre Controller local, si possible. Si aucun Controller local n'est disponible, il bascule vers un Controller de la zone principale.
- Si vous déplacez un Controller dans ou hors d'une zone, et que la mise à jour automatique est activée, les VDA des deux zones reçoivent des listes mises à jour qui indiquent quels Controller sont locaux et lesquels se trouvent dans la zone principale, de façon à ce qu'ils sachent avec lesquels ils peuvent s'enregistrer et accepter des connexions.
- Si vous déplacez un catalogue vers une autre zone, les VDA de ce catalogue s'enregistrent auprès des Controller situés dans la zone dans laquelle vous avez déplacé le catalogue (Lorsque vous déplacez un catalogue vers une autre zone, assurez-vous que cette zone et la zone avec la connexion hôte associée sont bien connectées. Si la bande passante est limitée ou si la latence est élevée, déplacez la connexion hôte vers la même zone contenant le catalogue de machines associé.)

Si tous les Controller de la zone principale échouent :

- Web Studio ne peut pas se connecter au site.
- Impossible de se connecter aux VDA de la zone principale.
- Les performances du site se dégradent jusqu'à ce que les Controller de la zone principale deviennent disponibles.

Pour les sites contenant des VDA de versions antérieures à la version 7.7 :

- Un VDA situé dans une zone satellite accepte les requêtes de Controller situés dans sa zone locale et la zone principale (Les VDA à partir de la version 7.7 peuvent accepter les demandes de Controller d'autres zones satellite).
- Un VDA situé dans une zone satellite s'enregistre auprès d'un Controller situé dans la zone principale ou la zone locale de façon aléatoire. (Les VDA à partir de la version 7.7 préfèrent la zone locale).

## Préférence de zone

Pour utiliser la fonctionnalité de préférence de zone, vous devez utiliser StoreFront 3.7 et Citrix Gateway 11.0-65.x au minimum

Dans un site multi-zone, la fonctionnalité de préférence de zone permet à l'administrateur de mieux contrôler les VDA utilisés pour lancer une application ou un bureau.

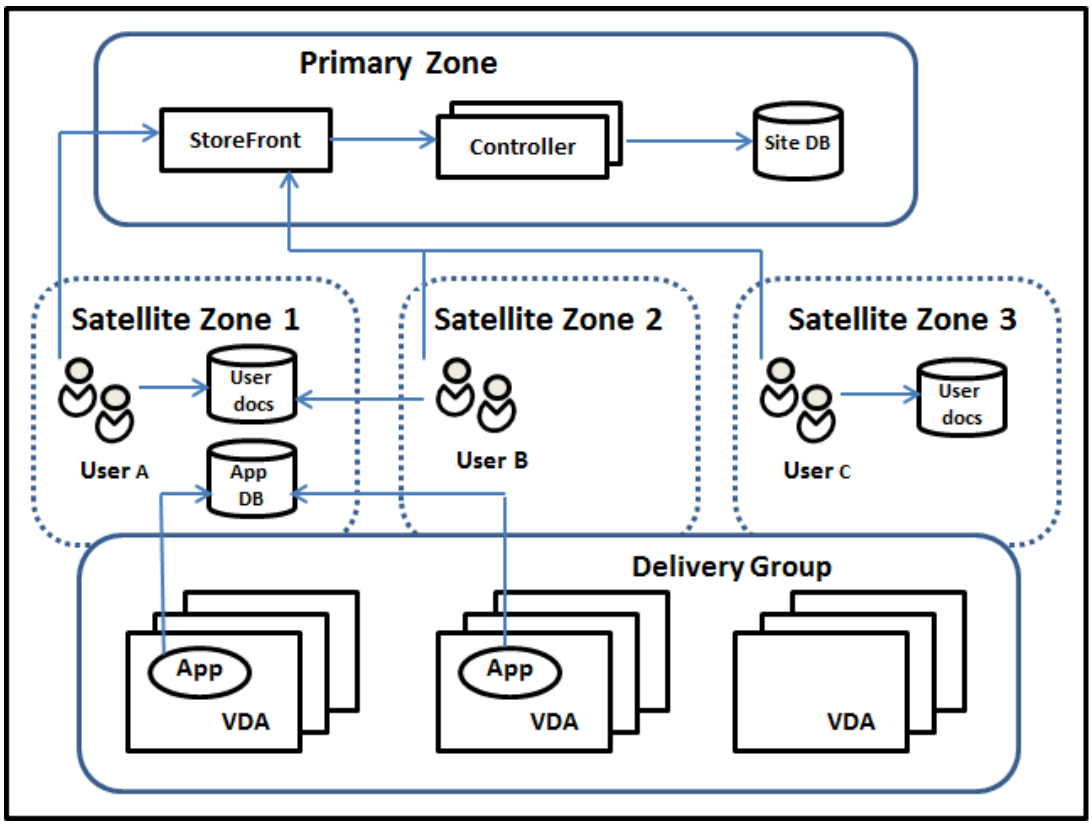
### Comment fonctionne la préférence de zone

Il existe trois formes de préférence de zone. Il est possible d'utiliser un VDA situé dans une zone spécifique, en fonction des éléments suivants :

- Emplacement où les données de l'application sont stockées. Il s'agit de la zone d'accueil de l'application.
- Emplacement de base des données de l'utilisateur, comme un profil ou un partage. Il s'agit de la zone d'accueil de l'utilisateur.
- Emplacement actuel de l'utilisateur (où l'application Citrix Workspace est exécutée). Il s'agit de l'emplacement de l'utilisateur.

Le graphique suivant illustre un exemple de configuration multi-zone.




Dans cet exemple, les VDA sont répartis entre trois zones satellite, mais ils sont tous dans le même groupe de mise à disposition. Par conséquent, le broker peut choisir le VDA à utiliser pour une demande de lancement d'un utilisateur. Cet exemple indique qu'il existe plusieurs emplacements où les utilisateurs peuvent exécuter leurs points de terminaison d'application Citrix Workspace :

- L'utilisateur A utilise un périphérique avec l'application Citrix Workspace dans la zone satellite 1.
- L'utilisateur B utilise un périphérique dans la zone satellite 2.
- Les documents d'un utilisateur peuvent être stockés à différents endroits.
  - Les utilisateurs A et B utilisent un partage basé dans la zone satellite 1.
  - L'utilisateur C utilise un partage de la zone satellite C.
  - L'une des applications publiées utilise une base de données qui se trouve dans la zone satellite 1.

Vous pouvez associer un utilisateur ou une application avec une zone en configurant une zone d'accueil pour l'utilisateur ou l'application. Le broker du Delivery Controller utilise ces associations pour sélectionner la zone dans laquelle une session est lancée, si les ressources sont disponibles. Vous pouvez :

- Configurer la zone d'accueil d'un utilisateur en ajoutant un utilisateur à une zone.

- Configurer la zone d'accueil d'une application en modifiant les propriétés de l'application.

Un utilisateur ou une application ne peut avoir qu'une seule zone d'accueil à la fois (Il peut exister une exception pour les utilisateurs qui peuvent être associés à plusieurs zones s'ils sont membres de plusieurs groupes d'utilisateurs ; veuillez consulter la section « Autres considérations ». Toutefois, même dans ce cas, le broker utilise une seule zone d'accueil).

Bien que les préférences de zone pour les utilisateurs et les applications puissent être configurées, le broker sélectionne une seule zone préférée pour le lancement. L'ordre de priorité par défaut pour sélectionner la zone préférée est : accueil application > accueil utilisateur > emplacement utilisateur. Vous pouvez restreindre la séquence ; voir Préférence de zone de personnalisation. Lorsqu'un utilisateur lance une application :

- Si l'application est associée à une zone (accueil application), la zone préférée est la zone d'accueil de cette application.
- Si l'application n'est pas associée à une zone, mais si l'utilisateur est associé à une zone (accueil utilisateur), la zone préférée est la zone d'accueil de cet utilisateur.
- Si ni l'application ni l'utilisateur n'est associé à une zone, la zone préférée est la zone dans laquelle l'utilisateur exécute une instance de l'application Citrix Workspace (emplacement utilisateur). Si cette zone n'est pas définie, le VDA et la zone sont sélectionnés de façon aléatoire. L'équilibrage de charge est appliqué à tous les VDA dans la zone préférée. S'il n'existe aucune zone préférée, l'équilibrage de charge est appliqué à tous les VDA du groupe de mise à disposition.

#### Configuration de la préférence de zone

Lorsque vous configurez (ou supprimez) une zone d'accueil pour un utilisateur ou une application, vous pouvez restreindre la façon dont la préférence de zone est utilisée.

- **Utilisation obligatoire de la zone d'accueil utilisateur :** dans un groupe de mise à disposition, vous pouvez spécifier qu'une session se lance dans la zone d'accueil de l'utilisateur (si elle est configurée), sans basculement vers une autre zone si la zone d'accueil ne dispose pas de ressources disponibles. Cette restriction est utile lorsque vous souhaitez éviter les risques de copie de profils ou de fichiers de données importants entre les zones. En d'autres termes, vous souhaitez plutôt interdire le lancement d'une session plutôt que de lancer une session dans une zone différente.
- **Utilisation obligatoire de la zone d'accueil de l'application :** de même, lorsque vous configurez une zone d'accueil pour une application, vous pouvez indiquer que l'application doit être lancée uniquement dans cette zone, sans basculement vers une autre zone si les ressources ne sont pas disponibles dans la zone d'accueil de l'application.
- **Aucune zone d'accueil de l'application et ignorer la zone d'accueil utilisateur configurée :** si vous ne spécifiez pas de zone d'accueil pour une application, vous pouvez également spé-

cifier qu'aucune des zones utilisateur ne devrait être considérée lors du lancement de cette application. Par exemple, vous pouvez préférer que les utilisateurs exécutent une application sur un VDA proche de la machine, en utilisant la préférence de zone d'emplacement utilisateur, même si certains utilisateurs peuvent disposer d'une zone d'accueil différente.

#### Comment les zones préférées affectent les sessions

Lorsqu'un utilisateur lance une application ou un bureau, le broker préfère utiliser la zone préférée, plutôt que d'utiliser une session existante.

Si l'utilisateur qui démarre une application ou un bureau est déjà dans une session qui est appropriée pour la ressource en cours de démarrage (par exemple, qui peut utiliser le partage de session pour une application, ou une session qui exécute déjà la ressource en cours de démarrage), mais que la session s'exécute sur un VDA situé dans une zone différente de la zone préférée pour l'utilisateur/application, le système peut créer une nouvelle session. Cela permet de démarrer dans la zone appropriée (si elle dispose d'une capacité disponible), plutôt que de se reconnecter à une session dans une zone moins adaptée aux besoins de cette session.

Pour éviter une session orpheline ne pouvant plus être contactée, la reconnexion est autorisée à des sessions déconnectées existantes, même si elles ne se trouvent pas dans une zone préférée.

L'ordre de préférence pour un démarrage réussi des sessions est le suivant :

1. Se reconnecter à une session existante dans la zone préférée.
2. Se reconnecter à une session déconnectée existante dans une zone différente de la zone préférée.
3. Démarrer une nouvelle session dans la zone préférée.
4. Se reconnecter à une session connectée existante dans une zone différente de la zone préférée.
5. Démarrer une nouvelle session dans une zone différente de la zone préférée.

#### Autres considérations pour les préférences de zone

- Si vous configurez une zone d'accueil pour un groupe d'utilisateurs (par exemple, un groupe de sécurité), les utilisateurs de ce groupe (via une appartenance directe ou indirecte) sont associés à la zone spécifiée. Toutefois, un utilisateur peut appartenir à plusieurs groupes de sécurité, et, par conséquent, être associé à une autre zone d'accueil configurée via d'autres appartenances à un groupe. Dans de tels cas, déterminer la zone d'accueil de l'utilisateur peut être aléatoire.

Si un utilisateur est associé à une zone d'accueil qui n'a pas été acquise par l'appartenance à un groupe, cette zone est utilisée pour la préférence de zone. Toute association de zone acquise par l'appartenance à un groupe est ignorée.

Si l'utilisateur est associé à plusieurs zones acquises uniquement via l'appartenance à un groupe, le broker choisit entre les zones de manière aléatoire. Une fois que le broker a effectué ce choix, cette zone est utilisée pour chaque démarrage de session suivant, jusqu'à ce que l'appartenance de l'utilisateur à ce groupe change.

- Si la préférence de zone est l'emplacement utilisateur, l'application Citrix Workspace sur la machine de point de terminaison doit être détectée par le boîtier Citrix Gateway par le biais duquel la machine est connectée. Citrix Gateway doit être configuré pour associer des plages d'adresses IP avec certaines zones et l'identité de la zone découverte doit être transmise via StoreFront au Controller.

Pour plus d'informations sur les préférences de zone, consultez la section Fonctionnement des préférences de zone.

### Considérations, configurations requises et recommandations

- Vous pouvez placer les éléments suivants dans une zone : Controller, catalogues de machines, connexions hôtes, utilisateurs et applications. Si un catalogue utilise une connexion hôte, assurez-vous que le catalogue et la connexion doivent se trouver dans la même zone. (Cependant, si une connexion à bande passante élevée et à faible latence est disponible, ils peuvent être dans des zones différentes.)
- Lorsque vous placez des éléments dans une zone satellite, cette opération affecte la façon dont le site interagit avec eux et avec d'autres objets qui leur sont liés.
  - Lorsque des Controller sont placés dans une zone satellite, il est supposé que ces machines disposent d'une bonne connectivité (locale) aux hyperviseurs et aux VDA dans la même zone. Les Controller dans cette zone satellite sont ensuite préférés aux Controller de la zone principale pour gérer ces hyperviseurs et machines VDA.
  - Lorsqu'une connexion d'hyperviseur est placée dans une zone satellite, il est supposé que tous les hyperviseurs gérés via cette connexion d'hyperviseur résident également dans cette zone satellite. Les Controller dans cette zone satellite sont alors préférés aux Controller de la zone principale lors de la communication avec cette connexion d'hyperviseur.
  - Lorsqu'un catalogue de machines est placé dans une zone satellite, il est supposé que toutes les machines VDA de ce catalogue se trouvent dans la zone satellite. Les Controller locaux sont préférés aux Controller de la zone principale lors de la tentative d'enregistrement auprès du site, une fois que le mécanisme de mise à jour automatique de liste des Controller a été activé après le premier enregistrement de chaque VDA.
  - Des instances de Citrix Gateway peuvent également être associées à des zones. Cela se fait dans le cadre de la configuration du routage HDX optimal de StoreFront plutôt que, comme pour les autres éléments décrits ici, dans le cadre de la configuration du site. Lorsqu'une

passerelle Citrix Gateway est associée à une zone, elle est utilisée de préférence lorsque des connexions HDX à des machines VDA dans cette zone sont utilisées.

- Lorsque vous créez un site de production, puis créez le premier catalogue et le premier groupe de mise à disposition, tous les éléments se trouvent dans la zone principale ; vous ne pouvez pas créer de zones satellite tant que cette configuration initiale n'a pas été effectuée (Si vous créez un site vide, la zone principale ne contiendra initialement qu'un Controller. Vous pouvez créer des zones satellites avant ou après la création d'un catalogue et d'un groupe de mise à disposition.
- Lorsque vous créez la première zone satellite contenant un ou plusieurs éléments, tous les autres éléments de votre site restent dans la zone principale.
- La zone principale est appelée « Principale » par défaut ; vous pouvez changer ce nom. Bien que Web Studio indique quelle zone est la zone principale, il est recommandé d'utiliser un nom facile à identifier pour la zone principale. Vous pouvez réaffecter la zone principale (c'est-à-dire définir une autre zone comme zone principale), mais elle doit toujours contenir la base de données du site et les serveurs haute disponibilité.
- Gardez toujours la base de données du site dans la zone principale.
- Après avoir créé une zone, vous pouvez déplacer les éléments d'une zone à une autre. Cette flexibilité vous permet de séparer potentiellement les éléments qui fonctionnent mieux à proximité. Par exemple, le déplacement d'un catalogue vers une zone différente de la connexion (hôte) qui crée les machines dans le catalogue peut affecter les performances. Prenez en compte les effets potentiels du déplacement d'éléments entre les zones. Gardez un catalogue et la connexion hôte qu'il utilise dans la même zone ou dans des zones bien connectées (par exemple, via un réseau à faible latence et à bande passante élevée).
- Pour des performances optimales, installez Web Studio et Director uniquement dans la zone principale. Vous pouvez accéder à Web Studio et à Director depuis une zone satellite (par exemple, si une zone satellite contenant des Controller à utiliser pour le basculement au cas où la zone principale serait inaccessible) car il s'agit d'applications Web.
- Dans l'idéal, Citrix Gateway situé dans une zone satellite est utilisé pour les connexions utilisateur entrant dans cette zone depuis d'autres zones ou des emplacements externes, mais vous pouvez l'utiliser pour les connexions à l'intérieur de la zone.
- Rappel : pour utiliser la fonctionnalité de préférence de zone, vous devez utiliser StoreFront 3.7 et Citrix Gateway 11.0-65.x au minimum

#### Limites de la qualité des connexions

Les Controller de la zone satellite effectuent les interactions SQL directement avec la base de données du site. Cela impose certaines limites sur la qualité de la liaison entre la zone satellite et la zone princi-

pale qui contient la base de données du site. Les limites spécifiques sont relatives au nombre de VDA et de sessions utilisateur sur ces VDA qui sont déployés dans la zone satellite. Ainsi, des zones satellite avec uniquement quelques VDA et sessions peuvent fonctionner avec une connexion à la base de données de qualité plus faible que des zones satellite avec un grand nombre de sessions et de VDA.

Pour plus d'informations, consultez la section Latency and SQL Blocking Query Improvements.

#### Impact de la latence sur les performances de négociation

Bien que les zones permettent aux utilisateurs de se trouver sur des liaisons à latence plus élevée, à condition qu'il y ait un broker local, la latence supplémentaire a un impact inévitable sur l'utilisateur final. La plupart du temps, les utilisateurs observeront une certaine lenteur causée par l'aller-retour entre les Controller de la zone satellite et la base de données du site.

Avec le lancement d'applications, il est possible de rencontrer des délais supplémentaires pendant que le processus de négociation de session identifie les VDA appropriés auxquels envoyer des demandes de lancement de session.

### Créer et gérer des zones

Un administrateur complet peut effectuer toutes les tâches de création et de gestion de zone. Toutefois, vous pouvez également créer un rôle personnalisé qui vous permet de créer, modifier ou supprimer une zone. Le déplacement d'éléments entre les zones ne nécessite pas d'autorisations liées à la zone (à l'exception des autorisations en lecture) ; cependant, vous devez disposer d'une autorisation de modification pour les éléments que vous déplacez. Par exemple, pour déplacer un catalogue d'une zone vers une autre, vous devez disposer d'une autorisation de modification pour ce catalogue. Pour plus d'informations, consultez Administration déléguée.

**Si vous utilisez Citrix Provisioning :** étant donné que la console Citrix Provisioning ne sait pas identifier les zones, nous vous recommandons d'utiliser Web Studio pour créer des catalogues pour des zones satellite. Créez le catalogue dans Web Studio, en spécifiant la zone satellite correcte. Puis, utilisez la console Citrix Provisioning pour provisionner des machines dans ce catalogue (si vous créez le catalogue à l'aide de l'assistant Citrix Provisioning, le catalogue est placé dans la zone principale. Vous devez utiliser Web Studio pour le déplacer ultérieurement vers la zone satellite.)

#### Créer une zone

1. Connectez-vous à Web Studio.
2. Sélectionnez **Zones** dans le volet de gauche.
3. Sélectionnez **Créer une zone** dans la barre d'actions.
4. Entrez un nom pour la zone et une description (facultatif). Le nom doit être unique dans le site.

5. Sélectionnez les éléments à placer dans la nouvelle zone. Vous pouvez filtrer ou effectuer une recherche dans la liste des éléments à partir de laquelle vous sélectionnez. Vous pouvez également créer une zone vide ; dans ce cas, ne sélectionnez pas d'éléments.
6. Cliquez sur **Enregistrer**.

Au lieu de cette méthode, vous pouvez sélectionner un ou plusieurs éléments dans Web Studio, puis sélectionner **Créer une zone** dans la barre d'actions.

#### Modifier le nom ou la description d'une zone

1. Connectez-vous à Web Studio.
2. Sélectionnez **Zones** dans le volet de gauche.
3. Sélectionnez une zone dans le volet central, puis sélectionnez **Modifier la zone** dans la barre d'actions.
4. Modifiez le nom de la zone, la description ou les deux. Si vous modifiez le nom de la zone principale, assurez-vous que la zone reste facile à identifier comme zone principale.
5. Cliquez sur **Enregistrer** ou sur **Appliquer**.

#### Déplacer des éléments d'une zone à une autre

1. Connectez-vous à Web Studio.
2. Sélectionnez **Zones** dans le volet de gauche.
3. Sélectionnez une zone dans le volet central, puis sélectionnez un ou plusieurs éléments.
4. Faites glisser les éléments vers la zone de destination ou sélectionnez **Déplacer des éléments** dans la barre d'actions et spécifiez la zone vers laquelle les déplacer.

Un message de confirmation dresse la liste des éléments que vous avez sélectionnés et demande si vous êtes sûr de vouloir déplacer tous ces éléments.

**Rappel :** si un catalogue utilise une connexion hôte vers un hyperviseur ou un autre service, placez le catalogue et la connexion dans la même zone. Sinon, les performances peuvent être affectées. Si vous déplacez un élément, déplacez l'autre.

#### Supprimer une zone

Une zone doit être vide pour pouvoir être supprimée. Vous ne pouvez pas supprimer la zone principale.

1. Connectez-vous à Web Studio.
2. Sélectionnez **Zones** dans le volet de gauche.
3. Sélectionnez une zone dans le volet central.

4. Sélectionnez **Supprimer la zone** dans la barre d'actions. Si la zone n'est pas vide (elle contient des éléments), vous êtes invité à choisir la zone vers laquelle ces éléments seront déplacés.
5. Confirmez la suppression.

#### Ajouter une zone d'accueil pour un utilisateur

La configuration d'une zone d'accueil pour un utilisateur consiste à *ajouter un utilisateur à une zone*.

1. Connectez-vous à Web Studio.
2. Sélectionnez **Zones** dans le volet de gauche, puis sélectionnez une zone dans le volet central.
3. Sélectionnez **Ajouter des utilisateurs à la zone** dans la barre d'actions.
4. Dans la boîte de dialogue **Ajouter des utilisateurs à la zone**, cliquez sur **Ajouter**, puis sélectionnez les utilisateurs et les groupes d'utilisateurs à ajouter à la zone. Si vous spécifiez des utilisateurs qui disposent déjà d'une zone d'accueil, un message offre deux options : **Oui** = ajouter uniquement les utilisateurs que vous avez spécifiés qui ne disposent pas d'une zone d'accueil ; **Non** = retourner à la boîte de dialogue de sélection des utilisateurs.
5. Cliquez sur **OK**.

Pour les utilisateurs associés à une zone d'accueil, vous pouvez demander à ce que les sessions démarrent uniquement à partir de leur zone d'accueil :

1. Créez ou modifiez un groupe de mise à disposition.
2. Sur la page **Utilisateurs**, sélectionnez la case **Les sessions doivent être lancées dans la zone d'accueil d'un utilisateur, si une zone a été configurée**.

Toutes les sessions lancées par un utilisateur dans ce groupe de mise à disposition doivent être lancées à partir de machines se trouvant dans la zone d'accueil de l'utilisateur. Si un utilisateur du groupe de mise à disposition n'est pas associé à une zone d'accueil, ce paramètre n'a aucun effet.

#### Supprimer une zone d'accueil pour un utilisateur

Cette procédure consiste à supprimer un utilisateur d'une zone.

1. Connectez-vous à Web Studio.
2. Sélectionnez **Zones** dans le volet de gauche, puis sélectionnez une zone dans le volet central.
3. Sélectionnez **Supprimer des utilisateurs de la zone** dans la barre d'actions.
4. Dans la boîte de dialogue **Supprimer des utilisateurs de la zone**, cliquez sur **Supprimer**, puis sélectionnez les utilisateurs et les groupes d'utilisateurs à supprimer de la zone. Cette action supprime les utilisateurs de la zone uniquement ; ces utilisateurs restent dans les groupes de mise à disposition et les groupes d'applications auxquels ils appartiennent.
5. Confirmez la suppression lorsque vous y êtes invité.

#### Gérer les zones d'accueil pour les applications

La configuration d'une zone d'accueil pour une application consiste à ajouter une application à une zone. Par défaut, dans un environnement multi-zone, une application ne dispose pas de zone d'accueil.

La zone d'accueil d'une application est spécifiée dans les propriétés de l'application. Vous pouvez configurer les propriétés de l'application lorsque vous ajoutez l'application à un groupe ou ultérieurement.

- Lors de la création d'un groupe de mise à disposition, la création d'un groupe d'applications ou l'ajout d'applications à des groupes existants, sélectionnez **Propriétés** sur la page **Applications** de l'assistant.
- Pour modifier les propriétés d'une application après l'ajout de l'application, sélectionnez **Applications** dans le volet de gauche. Sélectionnez une application, puis sélectionnez **Modifier les propriétés d'application** dans la barre d'actions.

Sur la page **Zones** des propriétés/paramètres de l'application :

- Si vous souhaitez que l'application soit associée à une zone d'accueil :
  - Sélectionnez le bouton radio **Utiliser la zone sélectionnée pour déterminer**, puis sélectionnez la zone.
  - Si vous souhaitez que l'application démarre uniquement depuis la zone sélectionnée (et non pas à partir d'une autre zone), sélectionnez la case à cocher sous la sélection de zone.
- Si vous ne souhaitez pas que l'application soit associée à une zone d'accueil :
  - Sélectionnez le bouton radio **Ne pas configurer de zone d'accueil**.
  - Si vous ne souhaitez pas que le broker prenne en compte les zones utilisateur configurées lors du lancement de cette application, sélectionnez la case à cocher sous le bouton radio. Dans ce cas, ni la zone d'accueil de l'application ni la zone d'accueil de l'utilisateur n'est utilisée pour déterminer l'emplacement du lancement de cette application.

### Autres actions impliquant la spécification de zones

Après avoir créé au moins une zone satellite, vous pouvez spécifier une zone lorsque vous ajoutez une connexion hôte ou créez un catalogue.

Dans la plupart des cas, la zone principale est la valeur par défaut. Lors de l'utilisation de Machine Creation Services pour créer un catalogue, la zone qui est configurée pour la connexion hôte est sélectionnée automatiquement.

Si le site ne contient aucune zone satellite, il est supposé que la zone principale sera utilisée et la sélection de zone ne s'affiche pas.

# Surveiller

June 27, 2024

Les administrateurs et le personnel d'assistance technique peuvent surveiller les sites Citrix Virtual Apps and Desktops à l'aide d'un grand nombre de fonctionnalités et d'outils. À l'aide de ces outils, vous pouvez surveiller :

- les sessions utilisateur et l'utilisation des sessions ;
- les performances d'ouverture de session ;
- les connexions et les machines, y compris les échecs ;
- le calcul de charge ;
- Tendances historiques
- Infrastructure

## Citrix Director

Director est un outil Web en temps réel que vous pouvez utiliser pour effectuer la surveillance et la résolution des problèmes, et réaliser des tâches d'assistance pour les utilisateurs finaux.

Pour de plus amples informations, veuillez consulter les articles Director.

## Journalisation de la configuration

La journalisation de la configuration permet aux administrateurs de garder un suivi des modifications administratives apportées à un site. La journalisation de la configuration peut aider les administrateurs à identifier et résoudre les problèmes lorsque des modifications sont apportées à la configuration, à la gestion des modifications et au suivi des modifications, et à la création d'un rapport d'activité d'administration.

Vous pouvez afficher et générer des rapports sur les informations de journalisation à partir de Studio. Vous pouvez également afficher les éléments journalisés dans Director avec Trend View pour fournir des notifications des modifications apportées à la configuration. Cette fonctionnalité est utile pour les administrateurs qui n'ont pas accès à Studio.

La vue Trend View fournit des données d'historique des modifications apportées à la configuration sur une période de temps afin que les administrateurs puissent évaluer les modifications qui ont été apportées au site, lorsqu'ils ont été générés et qui les a effectuées pour trouver la cause d'un problème. Cette vue trie les informations de configuration en trois catégories :

- Échecs de connexion

- Machines mono-session défectueuses
- Machines multi-session défectueuses

Pour de plus amples informations sur la marche à suivre pour activer et configurer la journalisation de la configuration, consultez Journalisation de la configuration. Les articles Director décrivent comment afficher les informations de session à partir de cet outil.

### Journaux d'événements

Les services dans Citrix Virtual Apps and Desktops consignent les événements qui se produisent. Les journaux d'événements sont utilisés pour les opérations de surveillance et de dépannage.

Pour de plus amples informations, consultez Journaux d'événements. Les articles sur chaque fonctionnalité peuvent également contenir des informations sur les événements.

## Journalisation de la configuration

June 27, 2024

La journalisation de la configuration est une fonctionnalité qui capture les modifications apportées à la configuration du site et les activités administratives effectuées sur la base de données. Par défaut, cette fonction est activée. Vous pouvez utiliser le contenu consigné pour :

- Diagnostiquer et résoudre les problèmes après que des modifications sont apportées à la configuration. Le journal fournit une arborescence hiérarchique.
- Assister la gestion des modifications et suivre les configurations.
- Signaler les activités administratives.

Vous définissez les préférences de journalisation de la configuration, afficher les journaux de configuration et générer des rapports HTML et CSV à partir de Citrix Studio. Vous pouvez filtrer les affichages des journaux de configuration par plages de dates et selon les résultats de recherche en texte intégral. La journalisation obligatoire, lorsqu'elle est activée, empêche les modifications de la configuration à moins qu'elles puissent être journalisées. Avec des autorisations appropriées, vous pouvez supprimer des entrées dans le journal de configuration. Vous ne pouvez pas utiliser la fonction de journalisation de la configuration pour modifier le contenu du journal.

La journalisation de la configuration utilise un SDK PowerShell et le service de journalisation de la configuration. Le service de journalisation de la configuration s'exécute sur chaque Controller du site. Si un Controller échoue, le service sur un autre Controller traite automatiquement les demandes de journalisation.

Par défaut, la fonction de journalisation de la configuration est activée, et utilise la base de données qui est créée lorsque vous créez le site (la base de données de configuration de site). Vous pouvez spécifier un emplacement différent pour la base de données. La base de données de journalisation de la configuration prend en charge les mêmes fonctions haute disponibilité que la base de données de configuration de site.

L'accès à la journalisation de la configuration est contrôlé via l'administration déléguée, avec les autorisations Modifier les préférences de journalisation et Afficher les journaux de configuration.

Les journaux de configuration sont localisés lorsqu'ils sont créés. Par exemple, un journal créé en anglais est lu en anglais, quels que soient les paramètres régionaux du lecteur.

### Qu'est-ce qui est journalisé

Les modifications de configuration et les activités administratives initiées depuis Studio, Director et des scripts PowerShell sont journalisées. Les exemples de modifications apportées à la configuration journalisées comprennent l'utilisation de (création, modification, suppression des attributions) :

- Catalogues de machines
- Groupes de mise à disposition (y compris la modification des paramètres de gestion de la puissance)
- Rôles et étendues de l'administrateur
- Ressources et connexions de l'hôte
- Stratégies Citrix au travers de Studio

Exemples de modifications administratives journalisées :

- Gestion de la puissance d'une machine virtuelle ou d'un bureau utilisateur
- Envoi d'un message à un utilisateur par Studio ou Director

Les opérations suivantes ne sont pas enregistrées :

- Opérations autonomes telles que la mise sous tension de la gestion du pool de machines virtuelles.
- Actions de stratégie implémentées au travers de la console de gestion des stratégies de groupe (GPMC) ; utilisez les outils Microsoft pour afficher des journaux de ces actions.
- Les modifications effectuées via le Registre, accès direct à la base de données, ou à partir de sources autres que Studio, Director ou PowerShell.
- Lorsque le déploiement est initialisé, la journalisation de la configuration est disponible lorsque la première instance du service de journalisation de la configuration s'enregistre auprès du service de configuration. Par conséquent, les premières étapes de configuration ne sont pas journalisées (par exemple, lorsque le schéma de base de données est obtenu et appliqué, lors de l'initialisation d'un hyperviseur).

### Gérer la journalisation de la configuration

Par défaut, la journalisation de la configuration utilise la base de données qui est créée lorsque vous créez un site (également connu sous le nom de base de données de configuration de site). Citrix vous recommande d'utiliser un autre emplacement pour la base de données de journalisation de configuration (et la base de données de surveillance) pour les raisons suivantes :

- La stratégie de sauvegarde de la base de données de journalisation de la configuration est susceptible d'être différente de celle de la stratégie de sauvegarde de la base de données de configuration de site.
- Le volume de données collectées pour la journalisation de la configuration (et le service de surveillance) peut avoir un impact négatif sur l'espace disponible pour la base de données de configuration de site.
- Elle partage le point de défaillance unique pour les trois des bases de données.

Les éditions de produit qui ne prennent pas en charge la journalisation de la configuration ne disposent pas d'un nœud Journalisation dans Studio.

### Activer/désactiver la journalisation de la configuration et la journalisation obligatoire

Par défaut, la journalisation de la configuration est activée et la journalisation obligatoire est désactivée.

1. Connectez-vous à Web Studio et sélectionnez **Journalisation** dans le volet de gauche.
2. Sélectionnez **Préférences** dans la barre d'actions. La boîte de dialogue Journalisation de la configuration contient des informations de base de données et indique si la journalisation de la configuration et la journalisation obligatoire sont activées ou désactivées.
3. Sélectionnez l'action souhaitée :

   Pour activer la journalisation de la configuration, sélectionnez **Activer**. C'est le réglage par défaut. S'il est impossible d'écrire sur la base de données, les informations de journalisation sont ignorées, mais l'opération se poursuit.

   Pour désactiver la journalisation de la configuration, sélectionnez **Désactiver**. Si la journalisation était préalablement activée, les journaux existants restent lisibles avec le SDK PowerShell.

   Pour activer la journalisation obligatoire, sélectionnez **Empêche les modifications à la configuration du site lorsque la BDD n'est pas disponible**. Aucune modification de la configuration ou activité administrative ne sera enregistrée (contrairement à la normale) à moins qu'elle puisse être écrite dans la base de données de journalisation de la configuration. Vous pouvez activer la journalisation obligatoire uniquement lorsque la journalisation de la configuration est activée (c'est-à-dire lorsque **Activer** est sélectionné). Si le service de journalisation de la

configuration échoue, et que la haute disponibilité n'est pas utilisée, la journalisation obligatoire est utilisée. Dans de tels cas, les opérations qui seraient normalement enregistrées ne le sont pas.

Pour désactiver la journalisation obligatoire, sélectionnez **Autoriser modifications de la configuration du site lorsque la BDD n'est pas disponible**. Les modifications de configuration et les activités administratives sont autorisées, même si la base de données utilisée pour la journalisation de la configuration est inaccessible. C'est le réglage par défaut.

### Pour modifier l'emplacement de la base de données de journalisation de la configuration

Vous ne pouvez pas modifier l'emplacement de la base de données lorsque la journalisation obligatoire est activée, car la modification de l'emplacement inclut un bref intervalle qui ne peut pas être enregistré.

1. Créez un serveur de base de données, à l'aide d'une version SQL Server prise en charge.
2. Connectez-vous à Web Studio et sélectionnez **Journalisation** dans le volet de gauche.
3. Sélectionnez **Préférences** dans la barre d'actions.
4. Dans la boîte de dialogue Préférences de journalisation, sélectionnez **Modifier la base de données de journalisation**.
5. Dans la boîte de dialogue Changer la base de données de journalisation, spécifiez l'emplacement du serveur contenant le nouveau serveur de base de données. Voir Formats d'adresse de base de données pour les formats valides.
6. Pour autoriser Studio pour créer la base de données, cliquez sur **OK**. Lorsque vous y êtes invité, cliquez sur **OK** et la base de données sera créée automatiquement. Studio tente d'accéder à la base de données à l'aide des informations d'identification de l'utilisateur de Studio. Si la tentative échoue, vous êtes invité à entrer les informations d'identification de l'utilisateur de la base de données. Studio télécharge ensuite le schéma de base de données vers la base de données. (Les informations d'identification ne sont conservées que lors de la création de la base de données.)
7. Pour créer la base de données manuellement, cliquez sur **Générer script de base de données**. Le script généré comprend des instructions pour la création manuelle de la base de données. Assurez-vous que la base de données est vide et qu'au moins un utilisateur est autorisé à accéder et modifier la base de données avant le chargement du schéma.

Les données journalisation de la configuration ne sont pas importées vers la nouvelle base de données. Les journaux ne peuvent pas être regroupés pour les deux bases de données lors de la récupération des journaux. La première entrée du journal dans la nouvelle base de données de journalisation de la configuration indique qu'une modification a été apportée dans une base de données, mais elle n'identifie pas la base de données précédente.

### Afficher le contenu du journal de configuration

Lorsque vous effectuez des modifications de configuration et des activités administratives, les opérations de haut niveau créées par Studio et Director sont affichées dans la partie supérieure du panneau central dans Studio. Une opération de haut niveau se traduit par un ou plusieurs appels de service et de SDK, qui sont des opérations de bas niveau. Lorsque vous sélectionnez une opération de haut niveau dans le panneau supérieur, le panneau inférieur affiche les opérations de bas niveau.

Si une opération échoue avant la fin de l'opération, l'opération de journalisation peut ne pas être effectuée dans la base de données. Par exemple, un enregistrement de début n'aura pas d'enregistrement de fin correspondant. Dans de tels cas, le journal indique qu'il manque des informations. Lorsque vous affichez les journaux basés en fonction de plages de temps, les journaux incomplets sont affichés si les données dans les journaux correspondent aux critères. Par exemple, si tous les journaux des cinq derniers jours sont demandés et qu'un journal existe avec une heure de début dans les cinq derniers jours, mais sans date de fin, il est inclus.

Lors de l'utilisation d'un script pour appeler des applets de commande PowerShell, si vous créez une opération de bas niveau sans spécifier une opération de haut niveau parente, la journalisation de la configuration crée une opération de haut niveau de substitution.

Pour afficher le contenu du journal de configuration, sélectionnez **Journalisation** dans le panneau de navigation de Studio. Par défaut, le panneau central affiche le contenu du journal par ordre chronologique (la plus récente des entrées en premier), en les séparant par date. Vous pouvez :

- Trier l'affichage par en-tête de colonne.
- Filtrer l'affichage en spécifiant un intervalle de jours ou en entrant du texte dans la zone **Rechercher**. Pour revenir à l'affichage standard après la recherche, désactivez le texte dans la zone **Rechercher**.

### Générer des rapports

Vous pouvez générer des rapports au format CSV et HTML contenant les données du journal de la configuration.

- Le rapport CSV contient toutes les données de journalisation à partir d'un intervalle de temps spécifié. La hiérarchie des données dans la base de données est aplatie dans un seul tableau CSV. Aucun aspect des données n'a la priorité dans le fichier. Aucune mise en forme n'est utilisée, les données sont donc inintelligibles. Le fichier (appelé sur MyReport) contient les données dans un format lisible. Les fichiers CSV sont souvent utilisés pour l'archivage des données ou en tant que source de données pour un outil de création de rapports ou de manipulation de données tel que Microsoft Excel.

- Le rapport HTML fournit un formulaire lisible des données de journalisation pour un intervalle de temps spécifié. Il fournit une vue structurée et navigable pour la vérification des modifications. Un rapport HTML se compose de deux fichiers appelés Résumé et Détails. Le fichier Résumé répertorie les opérations de haut niveau : moment auquel chaque opération se produit, personne qui réalise l'opération et le résultat. Si vous cliquez sur un lien **Détails** en regard de chaque opération, vous êtes amené aux opérations de bas niveau dans le fichier Détails, qui fournit des informations supplémentaires.

Pour générer un rapport du journal de configuration, sélectionnez **Journalisation** dans le panneau de navigation de Studio, puis sélectionnez **Créer un rapport personnalisé** dans la barre d'actions.

- Sélectionnez la plage de dates pour le rapport.
- Sélectionnez le format du rapport : CSV, HTML ou les deux.
- Accédez à l'emplacement où vous souhaitez enregistrer le rapport.

### Supprimer le contenu du journal de configuration

Pour supprimer le journal de configuration, vous devez posséder certaines permissions d'administration déléguée et de base de données SQL Server.

- **Administration déléguée :** vous devez disposer d'un rôle Administration déléguée qui permet la lecture de la configuration du déploiement. Le rôle d'administrateur complet dispose de cette autorisation. Les options En lecture seule ou Gérer doivent être sélectionnées dans la catégorie Autres permissions pour un rôle personnalisé.

  Pour créer une copie de sauvegarde des données de journalisation de la configuration avant de les supprimer, les options En lecture seule ou Gérer doivent également être sélectionnées dans la catégorie Permissions de journalisation pour le rôle personnalisé.

- **Base de données SQL Server :** vous devez disposer d'une connexion au serveur SQL avec la permission de supprimer des enregistrements de la base de données. Il existe deux façons de procéder :

  - Utiliser une connexion à une base de données SQL Server avec un rôle de serveur sysadmin, ce qui vous permet d'effectuer toute activité sur le serveur de base de données. Les rôles de serveur `serveradmin` ou `setupadmin` vous permettent d'effectuer des opérations de suppression.
  - Si votre déploiement requiert une sécurité supplémentaire, utilisez une connexion de base de données non-sysadmin mappée sur un utilisateur de base de données qui est autorisé à supprimer des enregistrements de la base de données.

    1. Dans SQL Server Management Studio, créez une connexion SQL Server avec un rôle de serveur autre que « sysadmin ».

2. Mappez la connexion à un utilisateur dans la base de données. SQL Server crée automatiquement un utilisateur dans la base de données avec le même nom que la connexion.
3. Dans l'appartenance au rôle de base de données, spécifiez au moins un des membres de rôle pour la base de données utilisateur : `ConfigurationLoggingSchema_ROLE` ou `dbowner`.

Pour de plus amples informations, consultez la documentation de SQL Server Management Studio.

Pour supprimer les journaux de configuration :

1. Connectez-vous à Web Studio et sélectionnez **Journalisation** dans le volet de gauche.
2. Sélectionnez **Supprimer les journaux** dans la barre d'actions.
3. Vous êtes invité à indiquer si vous voulez créer une sauvegarde des journaux avant de les supprimer. Si vous choisissez de créer une copie de sauvegarde, naviguez jusqu'à l'emplacement où l'archive de sauvegarde est enregistrée. La sauvegarde va être créée en tant que fichier CSV.

Une fois les journaux de configuration effacés, la suppression du journal est la première activité consignée dans le journal vide. Cette entrée fournit des informations sur la personne qui a supprimé les journaux et la date à laquelle ils ont été supprimés.

### Afficher les journaux de l'API et de PowerShell

Pour surveiller les requêtes d'API effectuées au cours de votre session en cours, cliquez sur l'onglet **API**. Les journaux d'API sont effacés lorsque vous vous déconnectez de Web Studio.

Pour afficher les commandes PowerShell correspondant aux actions de l'interface utilisateur que vous avez effectuées au cours de la journée, cliquez sur l'onglet **PowerShell**.

### Associer des métadonnées aux journaux de configuration

Vous pouvez joindre des métadonnées aux journaux de configuration en associant une paire `name-value` appelée `MetadataMap` aux enregistrements des journaux.

> **Remarque :**
>
> - Vous ne pouvez associer des métadonnées qu'à des objets d'opération de haut niveau.
> - Les métadonnées sont associées aux enregistrements existants au moment de l'exécution.

### Définir les métadonnées

Exécutez la commande PowerShell `Set-LogHighLevelOperationMetadata` pour associer un enregistrement de journal à `MetadataMap`.
`Set-LogHighLevelOperationMetadata` accepte les paramètres suivants :

- **ID** : ID de l'opération de haut niveau.
- **InputObject** : opérations de haut niveau auxquelles vous ajoutez les métadonnées. Il s'agit d'une alternative au paramètre `Id` dans lequel un objet d'opération de haut niveau ou une liste d'objets est transmis à la commande PowerShell.

---

**Name** : nom de propriété des métadonnées à ajouter. La propriété doit être unique pour l'opération de haut niveau spécifiée. La propriété ne peut contenir aucun des caractères suivants : ()/;:#.*?=<> []'".

---

- 
- **Value** : valeur de la propriété.
- **Map** : dictionnaire des paires (name, value) pour les propriétés. Il s'agit d'une alternative à la définition des métadonnées utilisant les paramètres `-Name` et `-Value`.

Par exemple, pour associer les métadonnées à tous les enregistrements de journal de haut niveau portant l'ID 40, exécutez la commande PowerShell suivante :

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata
 -Name A -Value B
```

Pour associer les métadonnées à l'enregistrement de haut niveau avec l'utilisateur `abc@example.com`, exécutez la commande PowerShell suivante :

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperation
 -Name C -Value D
```

### Récupérer les enregistrements à l'aide des métadonnées

Exécutez les commandes PowerShell suivantes pour utiliser les métadonnées associées afin de récupérer les enregistrements de journal :

- Recherche par clé et par valeur :

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Recherche par valeur et n'importe quelle clé :

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- Recherche par clé et par n'importe quelle valeur :

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

#### Supprimer les métadonnées

Exécutez la commande PowerShell `Remove-LogHighLevelOperationMetadata` pour supprimer les métadonnées associées.
`Remove-LogHighLevelOperationMetadata` utilise les paramètres suivants :

- **ID** : ID de l'opération de haut niveau.
- **InputObject** : opérations de haut niveau auxquelles vous ajoutez les métadonnées. Il s'agit d'une alternative au paramètre `Id`‘ dans lequel un objet d'opération de haut niveau ou une liste d'objets est transmis à la commande PowerShell.
- **Name** : nom de propriété des métadonnées à supprimer. Définissez cette valeur sur $null pour supprimer toutes les métadonnées de l'objet spécifié.
- **Map** : dictionnaire des paires (name, value) pour les propriétés. Il peut s'agir d'une table de hachage (créée avec @{“name1”= “val1”; “name2”= “val2”}) ou d'un dictionnaire de chaînes (créé avec new-object “System.Collections.Generic.Dictionary[String, String]”). Les propriétés dont les noms correspondent aux clés du dictionnaire sont supprimées.

## Journaux d'événements

June 27, 2024

Les articles suivants contiennent des listes et des descriptions des événements qui peuvent être consignés par les services dans Citrix Virtual Apps and Desktops.

Ces informations ne sont pas complètes. Consultez les articles de chaque fonctionnalité pour plus d'informations sur les événements.

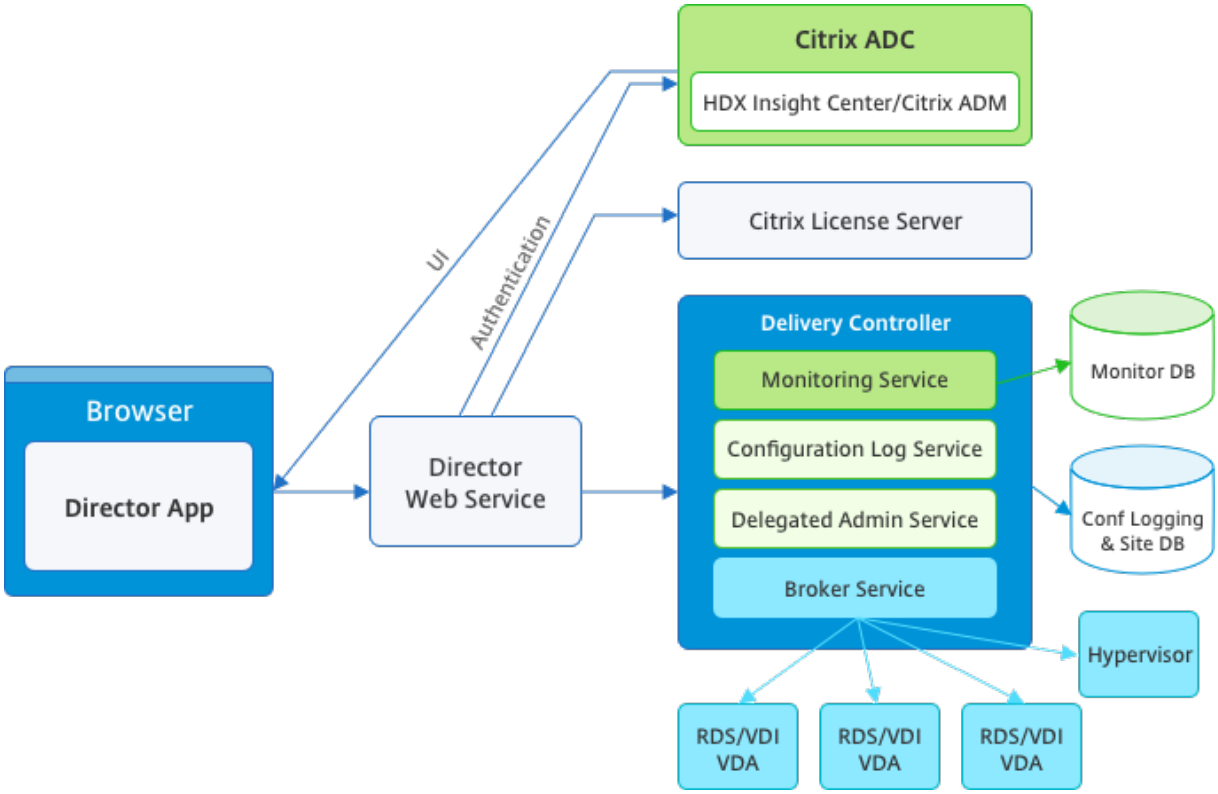
- Événements Citrix Broker Service
- Événements SDK Citrix FMA Service
- Événements Citrix Configuration Service
- Événements Citrix Delegated Administration Service

# Director

June 27, 2024

Director est une console de surveillance et de résolution des problèmes pour Citrix Virtual Apps and Desktops.




Director peut accéder :

- Aux données en temps réel à partir de l'agent Broker à l'aide d'une console unifiée, intégrée à Analytics, Performance Manager et Network Inspector. Les analyses suivantes sont optimisées par Citrix ADM pour identifier les goulots d'étranglement causés par le réseau dans votre environnement Citrix Virtual Apps ou Desktops :
  - Gestion du rendement pour assurer l'intégrité et les capacités
  - Tendances historiques et analyse du réseau
- Accès aux données d'historiques stockées dans la base de données Monitor pour accéder à la base de données de journalisation de la configuration.
- Aux données ICA provenant de Citrix Gateway à l'aide de Citrix ADM.
  - À la visibilité du gain dans l'expérience des utilisateurs pour les applications et les bureaux virtuels, et les utilisateurs pour Citrix Virtual Apps ou Desktops.

- Effectuez une corrélation des données réseau avec les données d'application et les mesures en temps réel pour une résolution des problèmes effective.
- Intégration à l'outil d'analyse Citrix Virtual Desktop 7 Director.

Director utilise un tableau de bord de résolution des problèmes qui offre un contrôle d'intégrité en temps réel et historique du site Citrix Virtual Apps ou Desktops. Cette fonctionnalité vous permet d'afficher les défaillances en temps réel, ce qui permet de vous faire une meilleure idée des problèmes rencontrés par les utilisateurs.

Pour plus d'informations sur la compatibilité des fonctionnalités de Director avec les Delivery Controller (DC), les VDA et tout autre composant dépendant, consultez la section Tableau de compatibilité des fonctionnalités.

> **Remarque :**
>
> Étant donné la découverte de Meltdown et Spectre, des vulnérabilités de canal auxiliaire de l'exécution spéculative, Citrix vous recommande d'installer les correctifs appropriés. Ces correctifs peuvent affecter les performances de SQL Server. Pour plus d'informations, consultez l'article Microsoft, Protéger SQL Server contre les attaques liées aux vulnérabilités de canal auxiliaire Spectre et Meltdown. Citrix vous recommande de tester et de planifier vos charges de travail avant de déployer les correctifs dans vos environnements de production.

Director est installé par défaut en tant que site Web sur le Delivery Controller. Pour les composants prérequis et d'autres détails, consultez la documentation relative à la configuration système requise pour cette version. Pour plus d'informations sur l'installation et la configuration de Director, voir Installer et configurer Director.

### Ouvrir une session sur Director

Le site Web Director se trouve à l'adresse https ou `http://<Server FQDN>/Director`.

Si l'un des sites d'un déploiement multisite est arrêté, l'ouverture de session nécessite un peu plus de temps lorsqu'il tente de se connecter au site qui est arrêté.

### Utiliser Director avec l'authentification par carte à puce PIV

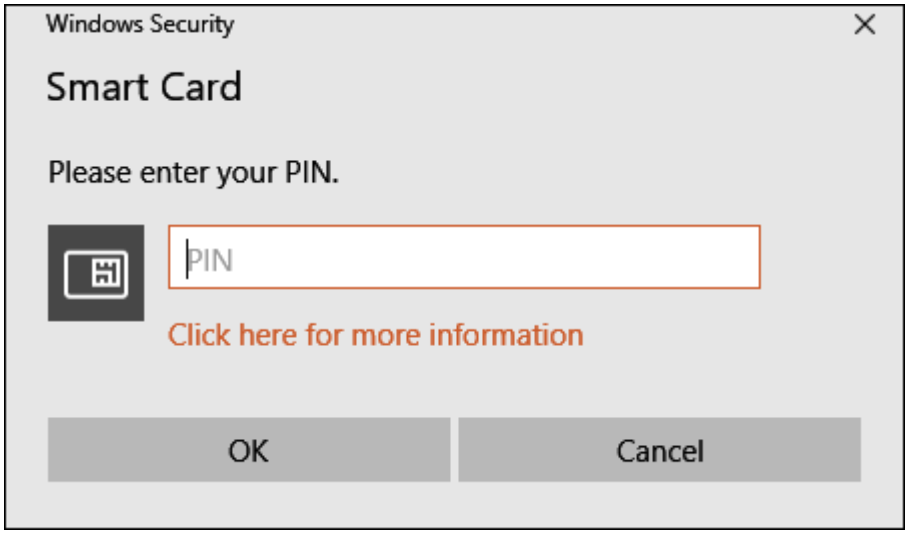
Director prend désormais en charge l'authentification par carte à puce basée sur Personal Identity Verification (PIV) pour se connecter. Cette fonctionnalité est utile pour les organisations et les organismes gouvernementaux qui utilisent l'authentification par carte à puce pour le contrôle d'accès. L'authentification par carte à puce requiert une configuration spécifique sur le serveur Director et dans Active Directory. Les étapes de configuration sont détaillées dans Configurer l'authentification par carte à puce PIV.

> **Remarque :**
>
> L'authentification par carte à puce est prise en charge uniquement pour les utilisateurs du même domaine Active Directory.

Après avoir effectué la configuration requise, vous pouvez vous connecter à Director à l'aide d'une carte à puce :

1. Insérez votre carte à puce dans le lecteur de carte à puce.
2. Ouvrez un navigateur et accédez à l'URL de Director, `https://<directorfqdn>/Director`.
3. Sélectionnez un certificat utilisateur valide dans la liste affichée.
4. Entrez votre jeton de carte à puce.




5. Une fois authentifié, vous pouvez accéder à Director sans fournir d'informations d'identification supplémentaires sur la page d'ouverture de session de Director.

### Utiliser Director avec l'authentification Windows intégrée

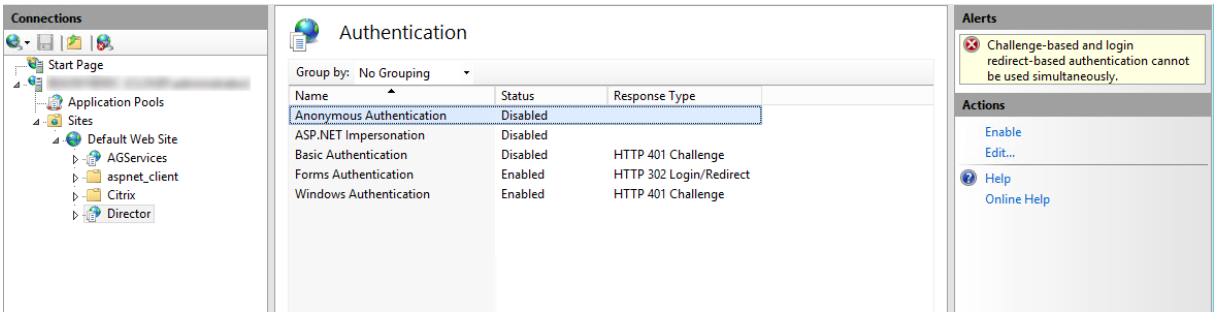
Avec l'authentification Windows intégrée (IWA), les utilisateurs appartenant à un domaine disposent d'un accès direct à Director sans avoir à saisir de nouveau leurs informations d'identification dans la page d'ouverture de session Director. Configuration requise pour l'utilisation de l'authentification Windows intégrée et de Director :

- Activez l'authentification Windows intégrée sur le site Web IIS qui héberge Director. Lorsque vous installez Director, l'authentification anonyme et l'authentification par formulaire sont activées. Pour utiliser l'authentification Windows intégrée et Director, désactivez l'authentifi-

cation anonyme et activez l'authentification Windows. L'authentification par formulaire doit rester activée pour l'authentification des utilisateurs sans domaine.

1. Démarrez le gestionnaire IIS.
2. Accédez à **Sites** > **Site Web par défaut** > **Director**.
3. Sélectionnez **Authentification**.
4. Cliquez avec le bouton droit sur **Authentification Anonyme** et sélectionnez **Désactiver**.
5. Cliquez avec le bouton droit sur **Authentification Windows** et sélectionnez **Activer**.




- Configurez l'autorisation de délégation Active Directory pour la machine Director. La configuration est requise uniquement si Director et le Delivery Controller sont installés sur des machines distinctes.

  1. Sur la machine Active Directory, ouvrez la console de gestion Active Directory.
  2. Dans la console de gestion Active Directory, accédez à **Nom de domaine** > **Ordinateurs**. Sélectionnez la machine Director.
  3. Cliquez avec le bouton droit et sélectionnez **Propriétés**.
  4. Dans Propriétés, sélectionnez l'onglet **Délégation**.
  5. Sélectionnez l'option **Approuver cet ordinateur pour la délégation à tous les services (Kerberos uniquement)**.

- Le navigateur qui est utilisé pour accéder à Director doit prendre en charge l'authentification Windows intégrée. Des étapes de configuration supplémentaires peuvent être requises dans Firefox et Chrome. Pour plus d'informations, reportez-vous à la documentation relative au navigateur.
- Le service de surveillance Monitoring Service doit exécuter Microsoft .NET Framework 4.5.1 ou une version ultérieure prise en charge répertoriée dans la section Configuration système requise pour Director. Pour plus d'informations, veuillez consulter la section Configuration système requise.

Lorsqu'un utilisateur ferme sa session sur Director ou à l'expiration de la session, la page d'ouverture de session s'affiche. À partir de la page de connexion, l'utilisateur peut définir le type d'authentification sur **Ouverture de session automatique** ou **Informations d'identification utilisateur**.

### Vues de l'interface

Director offre différentes vues de l'interface adaptées aux administrateurs particuliers. Les permissions du produit déterminent ce qui est affiché et les commandes disponibles.

Par exemple, les administrateurs du bureau d'assistance voient une interface adaptée aux tâches du personnel d'assistance technique. Director permet aux administrateurs du bureau d'assistance de rechercher l'utilisateur signalant un problème et afficher les activités associées à cet utilisateur. Par exemple, l'état des applications et des processus de l'utilisateur. Ils peuvent résoudre des problèmes rapidement en effectuant des actions telles que la fermeture d'une application ou d'un processus qui ne répond pas, l'observation d'opérations sur la machine de l'utilisateur, le redémarrage de la machine ou la réinitialisation du profil utilisateur.

Inversement, les administrateurs complets peuvent voir et gérer l'ensemble du site et peuvent réaliser des commandes pour plusieurs utilisateurs et machines. Le tableau de bord fournit une vue d'ensemble des aspects clés d'un déploiement, tel que l'état des sessions, les ouvertures de session des utilisateurs et l'infrastructure d'un site. Les informations sont mises à jour toutes les minutes. Si des problèmes surviennent, des détails apparaissent automatiquement sur le nombre et le type d'échec.

Pour plus d'informations sur les différents rôles et leurs autorisations dans Director, voir Administration déléguée et Director.

### Collecte de données d'utilisation par Google Analytics

Director Service commence à utiliser Google Analytics pour collecter des données d'utilisation après l'installation de Director. Des statistiques sur l'utilisation des pages Tendances et des analyses des appels d'API OData sont collectées. La collecte de données d'analyse est conforme à la politique de confidentialité de Citrix. La collecte des données est activée par défaut lors de l'installation Director.

Pour désactiver la collecte de données Google Analytics, modifiez la clé de registre sur la machine sur laquelle Director est installé. Si la clé de registre n'existe pas, créez-la et définissez-la sur la valeur souhaitée. Actualisez l'instance de Director après avoir modifié la valeur de la clé de registre.

**Attention :** une utilisation incorrecte de l'Éditeur du Registre peut occasionner de sérieux problèmes qui pourraient nécessiter la réinstallation du système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Citrix vous recommande d'effectuer une copie de sauvegarde du Registre Windows avant de le modifier.

Emplacement : HKEY_LOCAL_MACHINE\Software\Citrix\Director

Nom : DisableGoogleAnalytics

Valeur : 0 = activé (valeur par défaut), 1 = désactivé

Vous pouvez utiliser l'applet de commande PowerShell suivante pour désactiver la collecte de données par Google Analytics :

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
    DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

### Guide des nouvelles fonctionnalités

Director dispose d'un guide intégré qui utilise Pendo pour donner un aperçu des nouvelles fonctionnalités publiées dans la version actuelle de Director. Cette présentation rapide, associée aux messages appropriés dans le produit, vous aide à comprendre les nouveautés du produit.

Pour désactiver cette fonctionnalité, modifiez la clé de registre, comme indiqué ci-dessous sur la machine sur laquelle Director est installé. Si la clé de registre n'existe pas, créez-la et définissez-la sur la valeur souhaitée. Actualisez l'instance de Director après avoir modifié la valeur de la clé de registre.

> **Attention :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Citrix vous recommande d'effectuer une copie de sauvegarde du Registre Windows avant de le modifier.

Emplacement : HKEY_LOCAL_MACHINE\Software\Citrix\Director

Nom : DisableGuidedHelp

Valeur : 0 = activé (valeur par défaut), 1 = désactivé

Vous pouvez utiliser l'applet de commande PowerShell suivante pour désactiver le guide intégré :

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
    -PropertyType DWORD -Value 1
```

## Installer et configurer

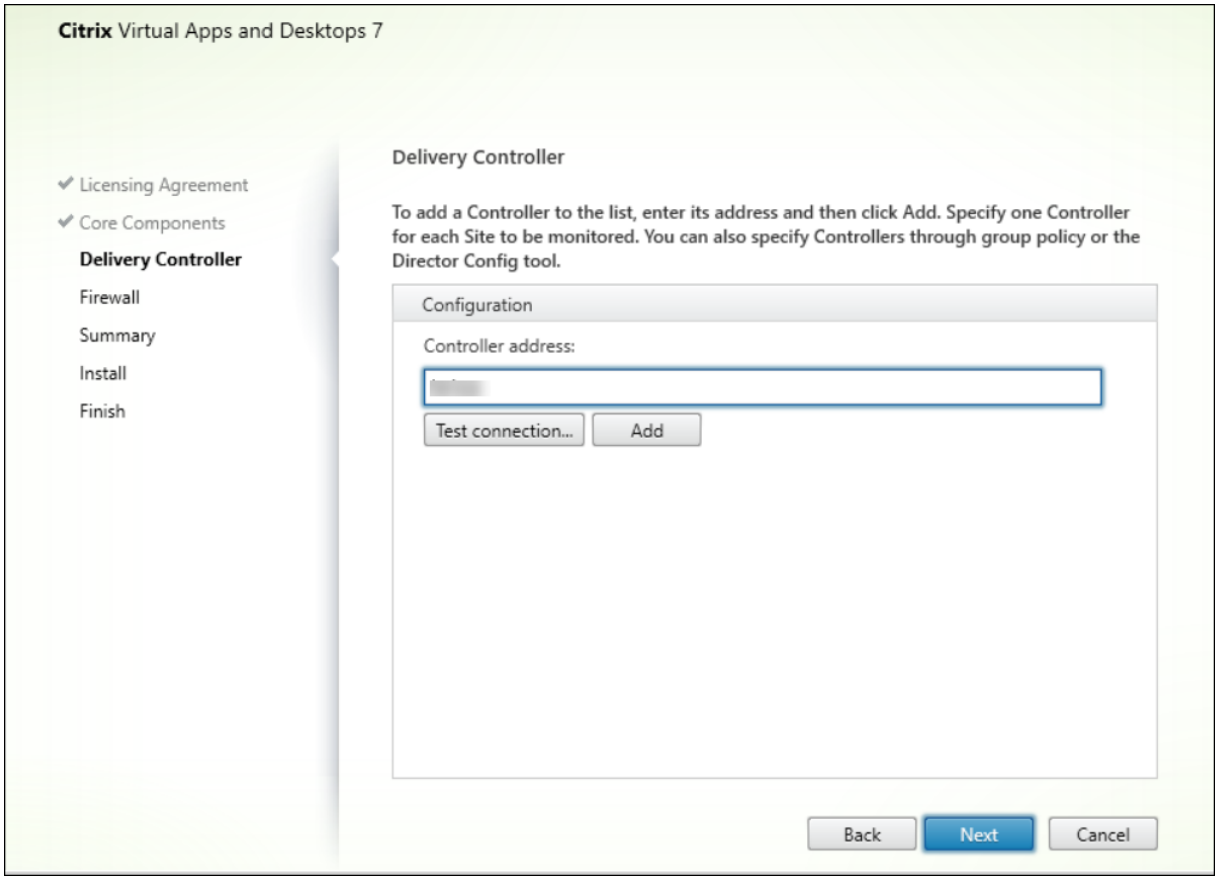
June 27, 2024

### Installer Director

Installez Director à l'aide du programme d'installation ISO du produit complet pour Citrix Virtual Apps and Desktops, qui vérifie la présence de composants pré-requis, installe les composants manquants, configure le site Web Director et effectue la configuration de base. Pour les composants pré-requis et d'autres détails, consultez la documentation relative à la configuration système requise pour cette version. Cette version de Director n'est pas compatible avec les déploiements Virtual Apps antérieurs à la version 6.5 ou les déploiements Virtual Desktops antérieurs à la version 7.
La configuration par défaut fournie par le programme d'installation ISO convient aux déploiements classiques. Si Director n'a pas été inclus au cours de l'installation, utilisez le programme d'installation ISO pour ajouter Director. Pour ajouter des composants supplémentaires, réexécutez le programme d'installation ISO et sélectionnez les composants à installer. Pour plus d'informations sur l'utilisation du programme d'installation ISO, consultez Installer les composants principaux dans la documentation relative à l'installation. Citrix vous recommande d'effectuer l'installation à l'aide du programme d'installation ISO du produit uniquement, et non pas le fichier MSI.

Lorsque Director est installé sur le Controller, il est automatiquement configuré avec localhost comme adresse de serveur, et Director communique avec le Controller local par défaut. Pour installer Director sur un serveur dédié qui est distant par rapport à un Controller, vous êtes invité à entrer l'adresse FQDN ou IP d'un Controller.



> **Remarque :**
>
> Cliquez sur **Ajouter** pour ajouter le Controller à surveiller.

Par défaut, Director communique avec ce Controller spécifié. Spécifiez une seule adresse de Controller pour chaque site que vous surveillez. Director découvre automatiquement tous les autres Controller du même site et retourne vers ces Controller en cas d'échec du Controller spécifié.

> **Remarque :**
>
> Director n'équilibre pas les charges entre les Controller.

Pour sécuriser les communications entre le navigateur et le serveur Web, Citrix recommande de mettre en œuvre TLS sur le site Web IIS qui héberge Director. Pour plus d'informations, reportez-vous à la documentation de Microsoft IIS. La configuration Director n'est pas requise pour activer TLS.

## Déployer et configurer Director

Lorsque Director est utilisé dans un environnement contenant plus d'un site, assurez-vous de synchroniser les horloges du système sur tous les serveurs sur lesquels les Controller, Director et autres composants principaux sont installés. Sinon, il se peut que les sites ne s'affichent pas correctement dans Director.

> **Important :**
>
> Pour protéger la sécurité des noms d'utilisateur et des mots de passe envoyés en texte brut via le réseau, autorisez les connexions Director utilisant uniquement HTTPS, et non pas HTTP. Certains outils peuvent lire le texte brut des noms d'utilisateur et des mots de passe dans des paquets réseau HTTP (non cryptés), ce qui peut créer un risque de sécurité pour les utilisateurs.

### Configurer des autorisations

Pour ouvrir une session sur Director, les administrateurs disposant de permissions pour Director doivent être des utilisateurs de domaine Active Directory et disposer des droits suivants :

- Droits de lecture dans toutes les forêts Active Directory à parcourir (voir Configuration avancée).
- Rôles d'administrateur délégué configurés (voir Administration déléguée et Director).
- Pour observer les utilisateurs, les administrateurs doivent être configurés à l'aide d'une stratégie de groupe Microsoft pour l'Assistance à distance Windows. De plus :
  - Lors de l'installation de VDA, assurez-vous que la fonction Assistance à distance de Windows est activée sur toutes les machines utilisateur (sélectionnée par défaut).

- Lorsque vous installez Director sur un serveur, assurez-vous que l'Assistance à distance Windows est installée (sélectionnée par défaut). Toutefois, elle est désactivée sur le serveur par défaut. La fonction ne doit pas être activée pour Director pour obtenir de l'aide auprès des utilisateurs. Citrix vous recommande de laisser la fonctionnalité désactivée pour améliorer la sécurité sur le serveur.
- Pour permettre aux administrateurs d'initier l'assistance à distance Windows, vous devez leur attribuer les permissions nécessaires à l'aide des paramètres de stratégie de groupe Microsoft correspondants pour l'assistance à distance. Pour plus d'informations, reportez-vous à l'article CTX127388 : How to Enable Remote Assistance for Desktop Director (Comment activer l'assistance à distance pour Desktop Director).

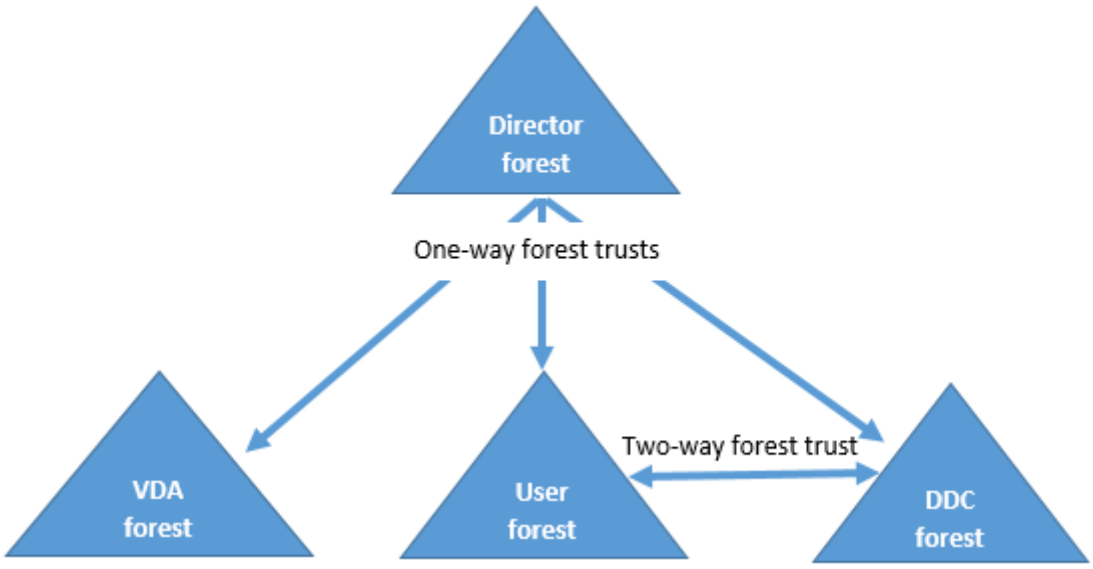
## Configuration avancée

June 27, 2024

Director peut prendre en charge les environnements multi-forêts multiples dans lesquels les utilisateurs, les Delivery Controller, les VDA et les Director se trouvent dans différentes forêts. Cela nécessite une configuration appropriée de relations d'approbation parmi les forêts et paramètres de configuration.

### Configuration recommandée dans un environnement multi-forêts

Il est recommandé de configurer des relations d'approbation de forêts bilatérales parmi les forêts avec authentification à l'échelle du domaine.



La relation d'approbation à partir de la console Director vous permet de résoudre les problèmes dans les sessions utilisateur, les VDA et les Delivery Controller situés dans des forêts différentes.

La configuration avancée requise pour Director pour la prise en charge de plusieurs forêts est contrôlée au travers de paramètres définis dans le Gestionnaire des services Internet (IIS).

> **Important :**
>
> Lorsque vous modifiez un paramètre dans les services IIS, Director Service redémarre automatiquement et ferme la session des utilisateurs.

Pour configurer les paramètres avancés à l'aide des services IIS :

1. Ouvrez la console du Gestionnaire des services Internet Information Services (IIS).
2. Accédez au site Web Director sous le site Web par défaut.
3. Cliquez deux fois sur **Paramètres d'application**.
4. Cliquez deux fois sur un paramètre pour le modifier.
5. Cliquez sur **Ajouter** pour ajouter un nouveau paramètre.

Director utilise Active Directory pour rechercher des utilisateurs et accéder à des informations supplémentaires sur ces utilisateurs ou leur machine. Par défaut, Director recherche le domaine ou la forêt dans lequel ou laquelle :

- le compte d'administrateur est membre ;
- le serveur Web Director est membre (si différent).

Director tente d'effectuer des recherches au niveau de la forêt à l'aide du catalogue global Active Directory. Si vous ne disposez pas de permissions vous permettant d'effectuer des recherches au niveau de la forêt, la recherche porte uniquement sur le domaine.

Pour rechercher des données dans un domaine ou une forêt Active Directory distincts, vous devez spécifier explicitement les domaines ou les forêts à parcourir. Configurez le paramètre Applications suivant sur le site Web Director dans le Gestionnaire des services Internet :

```
Connector.ActiveDirectory.Domains = (user),(server)
```

La valeur des attributs utilisateur et serveur représentent les domaines de l'utilisateur Director (l'administrateur) et du serveur Director respectivement.

Pour autoriser les recherches dans un autre domaine ou une autre forêt, ajoutez le nom du domaine à la liste comme indiqué dans l'exemple suivant :

```
Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

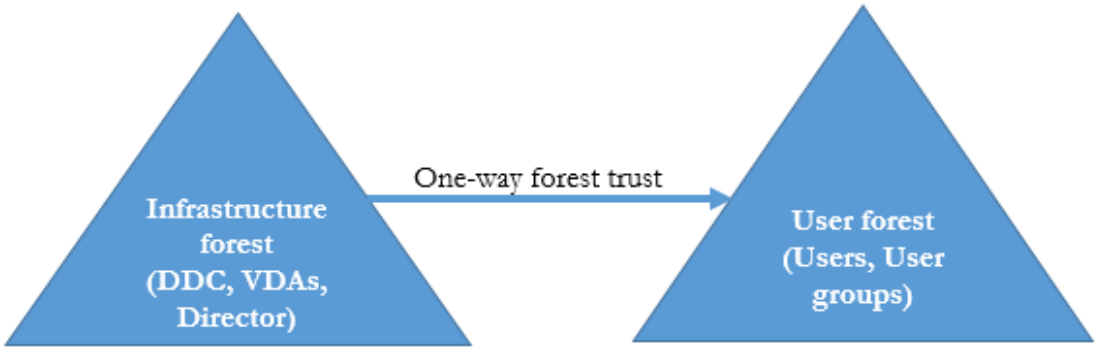
Pour chaque domaine de la liste, Director tente d'effectuer des recherches au niveau de la forêt. Si vous ne disposez pas de permissions vous permettant d'effectuer des recherches au niveau de la forêt, la recherche porte uniquement sur le domaine.

### Configuration du groupe local de domaine

La plupart des fournisseurs de services Citrix (CSP) ont des configurations d'environnement similaires, composées de VDA, Delivery Controller et Director dans la forêt Infrastructure. Les enregistrements des utilisateurs ou des groupes d'utilisateurs appartiennent à la forêt Client. Une approbation sortante unidirectionnelle existe depuis la forêt Infrastructure vers la forêt Client.

Les administrateurs CSP créent généralement un groupe local de domaine dans la forêt Infrastructure et ajoutent les utilisateurs ou les groupes d'utilisateurs de la forêt Client à ce groupe local de domaine.




Director peut prendre en charge une configuration multi-forêts de ce type et surveiller les sessions des utilisateurs configurés à l'aide de groupes locaux de domaine.

1. Ajoutez les paramètres Applications suivant sur le site Web Director dans le Gestionnaire des services Internet :

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true

   DomainLocalGroupSearchDomains= \<domain1\>,\<domain2\>
   ```

   <domaine1><domaine2> sont les noms des forêts dans lesquelles se trouve le groupe local de domaine.

2. Attribuez le groupe local de domaine aux groupes de mise à disposition dans Web Studio.
3. Redémarrez IIS et ouvrez une session sur Director pour que les modifications prennent effet. Maintenant, Director peut surveiller et afficher les sessions de ces utilisateurs.

### Ajouter des sites à Director

Si Director est déjà installé, configurez-le pour qu'il fonctionne avec plusieurs sites. Pour configurer, utilisez la console Gestionnaire des services Internet (IIS) sur chaque serveur Director pour mettre à jour la liste des adresses de serveurs dans les paramètres de l'application.

Ajoutez l'adresse d'un Controller pour chaque site au paramètre suivant :

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
<!--NeedCopy-->
```

SiteAController et SiteBController correspondent aux adresses Delivery Controllers de deux sites différents.

### Désactiver la visibilité des applications en cours d'exécution dans le Gestionnaire d'activités

Par défaut, le Gestionnaire d'activité de Director affiche une liste de toutes les applications en cours d'exécution pour la session d'un utilisateur. Ces informations peuvent être consultées par les administrateurs qui ont accès à la fonctionnalité Gestionnaire d'activité de Director. Pour les rôles d'administrateur délégué, ceci comprend l'administrateur complet, l'administrateur du groupe de mise à disposition et l'administrateur du bureau d'assistance.

Pour protéger la confidentialité des utilisateurs et les applications qu'ils ont en cours d'exécution, vous pouvez désactiver l'onglet **Applications** afin qu'il arrête de répertorier les applications en cours d'exécution.

> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne garantit pas la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

1. Sur le VDA, modifiez la clé de registre dans HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDa
   Par défaut, la clé est définie sur 1. Modifiez la valeur sur 0, ce qui signifie que les informations ne sont pas collectées depuis le VDA et par conséquent ne sont pas affichées dans le Gestionnaire d'activités.
2. Sur le serveur sur lequel Director est installé, modifiez le paramètre qui contrôle la visibilité des applications en cours d'exécution. Par défaut, la valeur est true, ce qui permet de voir les applications en cours d'exécution dans l'onglet Applications. Modifiez la valeur sur false, ce qui désactive cette visibilité. Cette option affecte uniquement le gestionnaire d'activité dans Director et non le VDA.
   Modifiez la valeur du paramètre suivant :
   UI.TaskManager.EnableApplications = false

> **Important :**
>
> Pour désactiver l'affichage des applications en cours d'exécution, effectuez ces modifications pour vous assurer que les données ne sont pas affichées dans le Gestionnaire d'activités.

## Configuration de l'authentification par carte à puce PIV

June 27, 2024

Cet article présente la configuration requise sur le serveur Director et dans Active Directory pour activer la fonctionnalité d'authentification par carte à puce.

> **Remarque :**
>
> L'authentification par carte à puce est prise en charge uniquement pour les utilisateurs du même domaine Active Directory.

### Configuration du serveur Director

Effectuez les étapes de configuration suivantes sur le serveur Director :

1. Installez et activez l'authentification par mappage de certificat client. Suivez les instructions sous **Client Certificate Mapping authentication using Active Directory** dans le document Microsoft Client Certificate Mapping Authentication.
2. Désactivez l'authentification par formulaires sur le site Director.

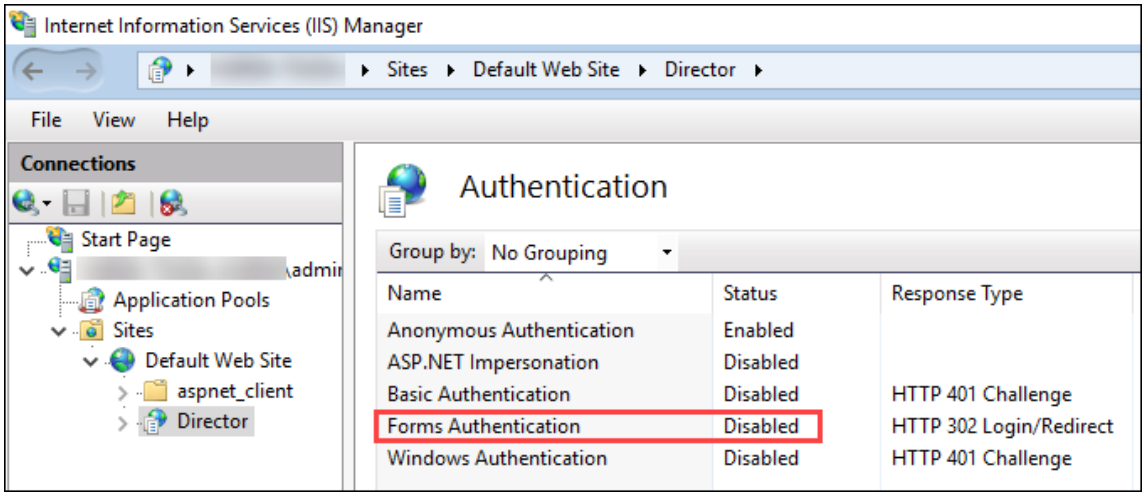
   Démarrez le gestionnaire des services Internet.

   Accédez à **Sites** > **Site Web par défaut** > **Director**.

   Sélectionnez **Authentification**.

   Cliquez avec le bouton droit sur **Authentification par formulaires** et sélectionnez **Désactiver**.



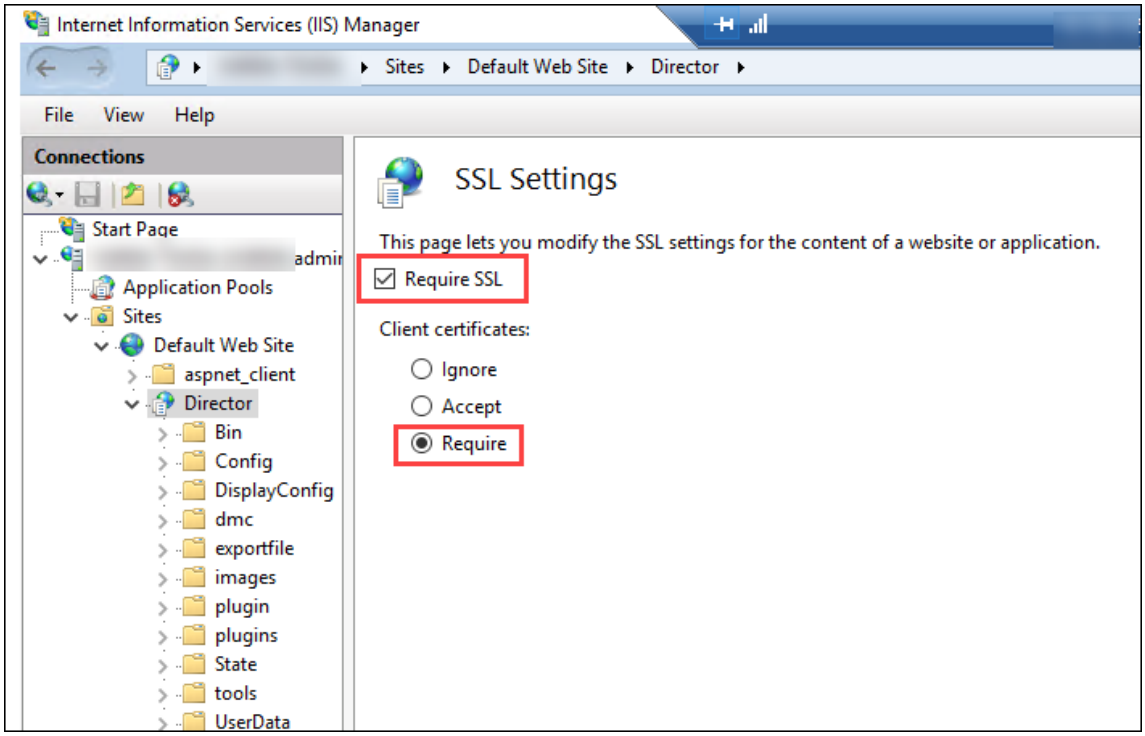

3. Configurez l'URL de Director pour le protocole https plus sécurisé (au lieu de HTTP) pour l'authentification par certificat client.

   a) Démarrez le gestionnaire des services Internet.

   b) Accédez à **Sites** > **Site Web par défaut** > **Director**.

   c) Sélectionnez **Paramètres SSL**.

   d) Sélectionnez **Exiger SSL** et **Certificats clients** > **Exiger**.




4. Mettez à jour web.config. Ouvrez le fichier web.config (disponible dans c:\inetpub\wwwroot\Director) à l'aide d'un éditeur de texte.

Sous l'élément parent <system.webServer>, ajoutez l'extrait suivant en tant que premier élément enfant :

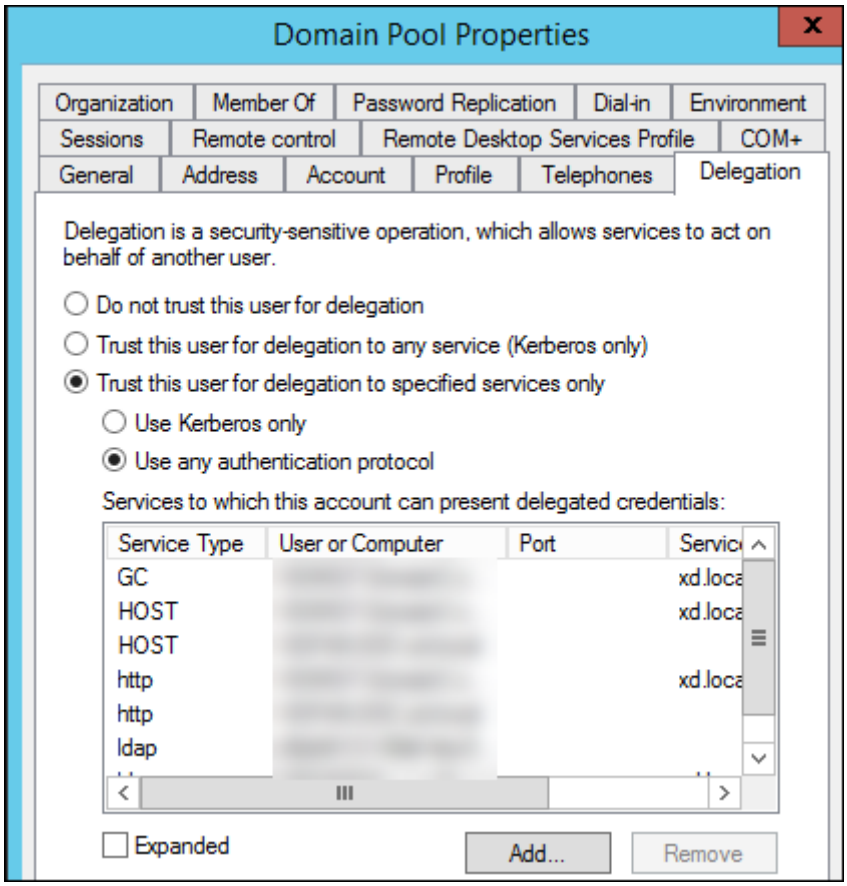
```
<defaultDocument>
   <files>
       <add value="LogOn.aspx"/>
   </files>
</defaultDocument>
```

### Configuration d'Active Directory

Par défaut, l'application Director s'exécute avec la propriété d'identité **Pool d'applications**. L'authentification par carte à puce requiert une délégation pour laquelle l'identité de l'application Director doit disposer des privilèges TCB (Trusted Computing Base) sur l'hôte de service.

Citrix vous recommande de créer un compte de service distinct pour l'identité Pool d'applications. Créez le compte de service et affectez les privilèges TCB conformément aux instructions de l'article MSDN de Microsoft, Protocol Transition with Constrained Delegation Technical Supplement.

Affectez le compte de service nouvellement créé au pool d'applications Director. La figure suivante montre la boîte de dialogue des propriétés d'un exemple de compte de service, Pool de domaines.



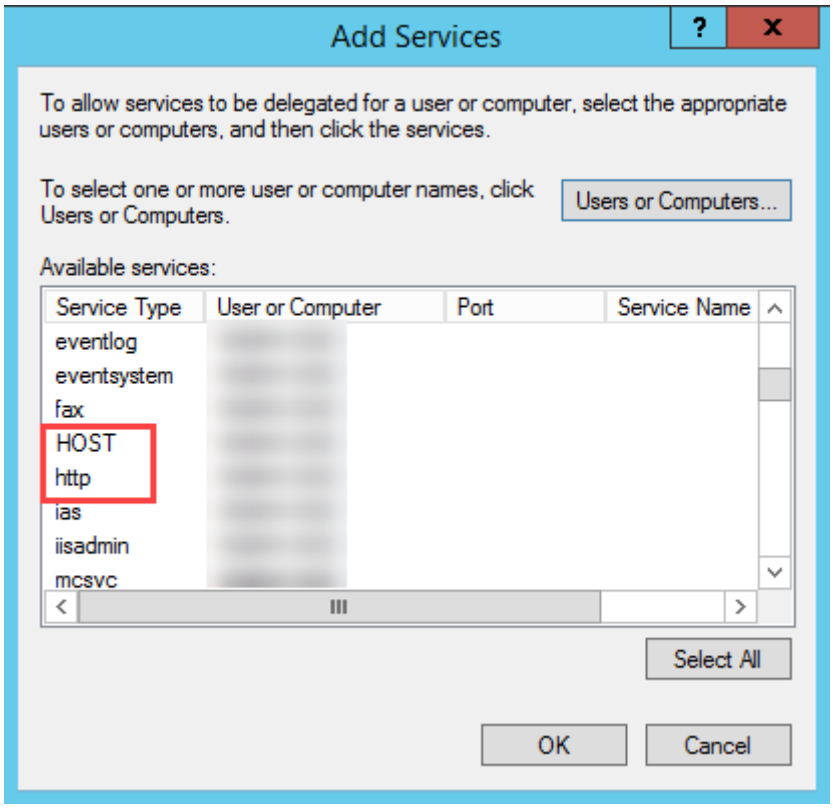

 

Configurez les services suivants pour ce compte :

- Delivery Controller : HOST, HTTP
- Director : HOST, HTTP
- Active Directory : GC, LDAP

Pour configurer,

1. Dans la boîte de dialogue Propriétés du compte utilisateur, cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Ajouter des services**, cliquez sur Utilisateurs ou ordinateurs.
3. Sélectionnez le nom d'hôte du Delivery Controller.
4. Dans la liste **Services disponibles**, sélectionnez HOST et HTTP pour **Service Type**.




De même, ajoutez des types de service pour les hôtes **Director** et **Active Directory**.

### Créer des enregistrements de nom de principal de service

Vous devez créer un compte de service pour chaque serveur Director et des adresses IP virtuelles (VIP) à charge équilibrée utilisées pour accéder à un pool de serveurs Director. Vous devez créer des enregistrements de nom principal de service (SPN) pour configurer une délégation vers le compte de service nouvellement créé.

- Utilisez la commande suivante pour créer un enregistrement SPN pour un serveur Director :

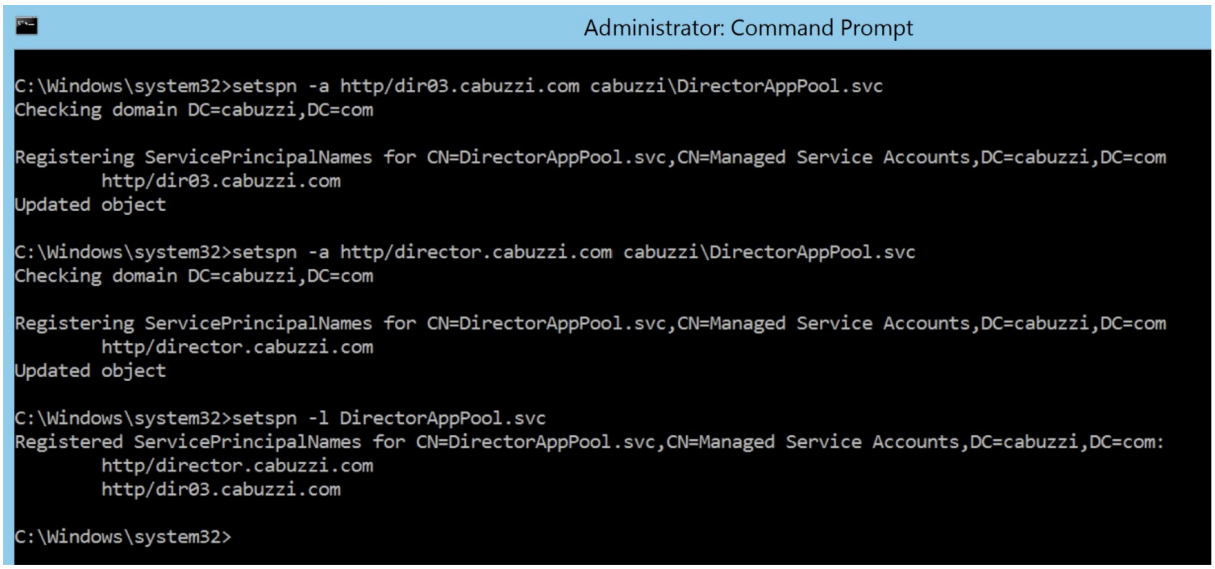
```
1   setspn -a http/<directorServer>.<domain_fqdn> <domain><
       DirectorAppPoolServiceAcct>
2
3  <!--NeedCopy-->
```

- Use the following command to create an SPN record for a load-balanced VIP:

```
1   setspn -S http/<DirectorFQDN> <domain>\<
       DirectorAppPoolServiceAcct>
2
3  <!--NeedCopy-->
```

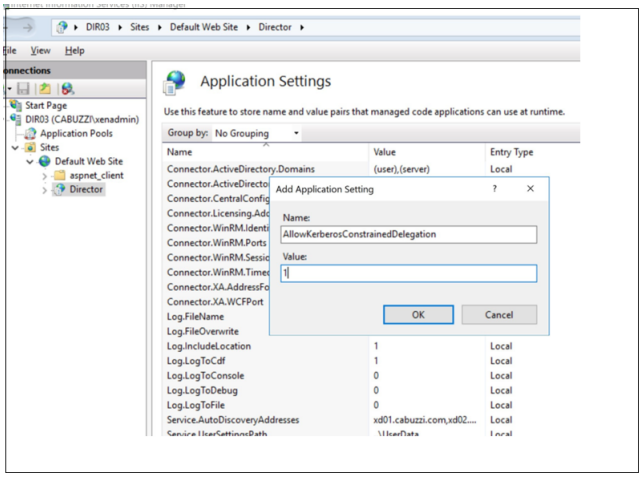
- Utilisez la commande suivante pour afficher ou tester les SPN créés :

```
1  setspn  – l <DirectorAppPoolServiceAcct>
2
3  <!--NeedCopy-->
```

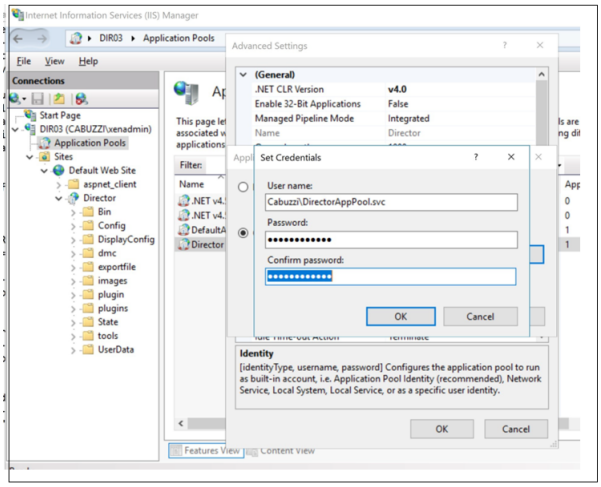



- Select the Director virtual directory in the left pane and double click **Application Settings**. Inside the Application Settings window, click **Add** and ensure **AllowKerberosConstrainedDelegation** is set to 1.




- Select **Application Pools** in the left-hand pane, then right-click the Director application pool and select **Advanced Settings**.
- Select **Identity**, click the ellipses ("…") to enter the service account domain\logon and password credentials. Close the IIS console.




- From an elevated command prompt, change the directory to C:\Windows\System32\inetsrv and enter the following commands:

```
1    appcmd.exe set config "Default Web Site" -section:system.webServer
       /security/authentication/clientCertificateMappingAuthentication /
       enabled:"True" /commit:apphost
2
3  <!--NeedCopy-->
```

```
1     appcmd.exe set config "Default Web Site" -section:system.
        webServer/security/access /sslFlags:"Ssl, SslNegotiateCert" /
        commit:apphost
2  \`\`\`
3
```

```
4 ![Invite de commandes](/en-us/citrix-virtual-apps-desktops/2402-ltsr/
     media/dir-smart-card-auth-5-scaled.png)
5
6 ## Configuration du navigateur Firefox
7
8 Pour utiliser le navigateur Firefox, installez le pilote PIV disponible
      sur [OpenSC 0.17.0](https://github.com/OpenSC/OpenSC/releases/tag
     /0.17.0). Pour obtenir des instructions sur l'installation et la
     configuration, reportez-vous à la page [Installing OpenSC PKCS#11
     Module in Firefox, Step by Step](https://github.com/OpenSC/OpenSC/
     wiki/Installing-OpenSC-PKCS%2311-Module-in-Firefox,-Step-by-Step).
9 Pour plus d'informations sur l'utilisation de l'authentification par
     carte à puce dans Director, consultez la section [Utiliser Director
     avec l'authentification par carte à puce PIV](/fr-fr/citrix-virtual-
     apps-desktops/2402-ltsr/director.html#use-director-with-piv-smart-
     card-authentication) dans l'article Director.<!--NeedCopy-->
```

## Configurer l'analyse réseau

June 27, 2024

> **Remarque :**
> La disponibilité de cette fonctionnalité dépend de la licence de votre organisation et de vos permissions d'administrateur.

Director s'intègre à Citrix ADM pour offrir une analyse de réseau et une gestion des performances :

- L'analyse de réseau utilise les rapports HDX Insight de Citrix ADM pour fournir une vue contextuelle des applications et des bureaux du réseau. Avec cette fonctionnalité, Director offre une analyse avancée du trafic ICA dans votre déploiement.
- La gestion des performances fournit un archivage des données d'historique ainsi que des rapports de tendance. Avec la conservation de l'historique des données par rapport à l'évaluation en temps réel, vous pouvez créer des rapports de tendance, y compris des tendances de capacité et d'intégrité.

Après avoir activé cette fonctionnalité dans Director, les rapports HDX Insight fournissent des informations supplémentaires à Director :

- L'onglet Réseau de la page Tendances affiche des effets de latence et de bande passante pour les applications, les bureaux et les utilisateurs sur l'ensemble du déploiement.
- La page Détails de l'utilisateur affiche des informations spécifiques à la latence et à la bande passante pour une session utilisateur particulière.

**Limitations :**

- Dans la vue Tendances, les données d'ouverture de session de connexion HDX ne sont pas collectées pour les VDA antérieurs à la version 7. Pour les VDA antérieurs, les données du graphique sont affichées en tant que 0.

Pour activer l'analyse de réseau, vous devez installer et configurer Citrix ADM dans Director. Director requiert Citrix ADM version 11.1 Build 49.16 ou une version ultérieure. Netscaler MAS est un boîtier virtuel exécuté sur XenServer. À l'aide de l'analyse de réseau, Director communique et rassemble les informations relatives à votre déploiement.

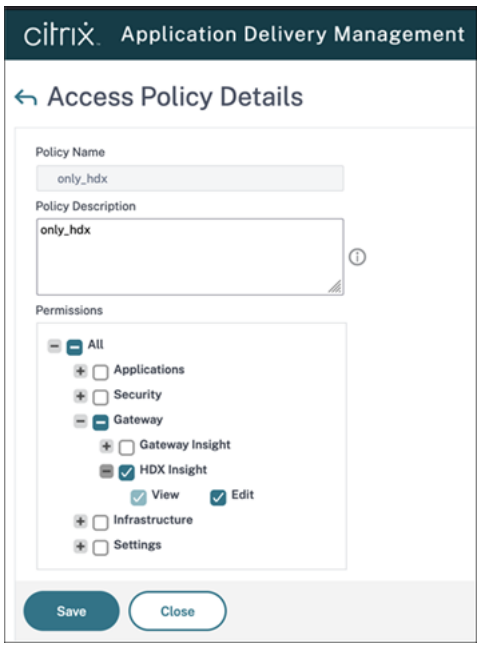
Pour de plus amples informations, veuillez consulter la documentation de Citrix ADM.

> **Remarque :**
>
> Citrix NetScaler Insight Center a atteint sa date de fin de maintenance le 15 mai 2018. Voir le Tableau des produits Citrix. Intégrez Director à Citrix ADM pour l'analyse du réseau. Pour migrer votre NetScaler Insight Center vers Citrix ADM, voir Migrer de NetScaler Insight Center vers Citrix ADM.

1. Sur le serveur sur lequel Director est installé, situez l'outil de ligne de commande DirectorConfig dans C:\inetpub\wwwroot\Director\tools, et exécutez-le avec le paramètre /confignetscaler dans une invite de commande.
2. Lorsque vous y êtes invité, entrez le nom de la machine (FQDN ou adresse IP) Citrix ADM, le nom d'utilisateur, le mot de passe, le type de connexion HTTPS (préférable à HTTP) et choisissez l'intégration à Citrix ADM.
3. Pour vérifier les modifications, fermez votre session et rouvrez-la.

> **Remarque :**
>
> Pour des raisons de sécurité, il est recommandé de créer un rôle personnalisé pour l'intégration d'ADM à Director avec des autorisations suffisantes pour accéder uniquement à HDX Insight.




Pour plus d'informations, consultez Configurer les stratégies d'accès.

## Administration déléguée et Director

June 27, 2024

L'administration déléguée utilise trois concepts : les administrateurs, les rôles et les étendues. Les permissions sont basées sur un rôle administrateur et l'étendue de ce rôle. Par exemple, un administrateur peut affecter un rôle d'administrateur du bureau d'assistance où l'étendue implique la responsabilité des utilisateurs à un site uniquement.

Pour de plus amples informations sur la création d'administrateurs délégués, veuillez consulter l'article Administration déléguée.

Les permissions d'administration déterminent l'interface Director présentée aux administrateurs et les tâches à effectuer. Les permissions déterminent :

- Les vues auxquelles l'administrateur peut accéder, collectivement nommées vue.
- Les bureaux, les machines et les sessions que l'administrateur peut afficher et interagir avec.
- Les commandes de l'administrateur peut effectuer, telles que l'observation d'une session de l'utilisateur ou l'activation du mode maintenance.

Les rôles et les permissions intégrés déterminent également la manière d'utilisation de Director par les administrateurs :

| Rôle d'administrateur | Permissions de Director |
| --- | --- |
| Administrateur complet | Possède un accès complet à toutes les vues et peut effectuer toutes les commandes, y compris l'observation d'une session utilisateur, l'activation du mode maintenance et l'exportation des données des tendances. |
| Administrateur de groupe de mise à disposition | Dispose d'un accès complet à toutes les vues et peut effectuer toutes les commandes, y compris l'observation d'une session utilisateur, la gestion de l'alimentation, la gestion des sessions, l'activation du mode de maintenance et l'exportation des données de tendances. |
| Administrateur en lecture seule | Peut accéder à toutes les vues et afficher tous les objets dans les étendues spécifiées et les informations globales. Peut télécharger des rapports à partir de canaux HDX et peut exporter les données de Tendances à l'aide de l'option Exporter dans la vue Tendances. Ne peut exécuter des commandes ou modifier quoi que ce soit dans les vues. |
| Administrateur du service d'assistance | Peut accéder uniquement aux vues Bureau d'assistance et Détails de l'utilisateur et peut afficher uniquement des objets que l'administrateur est autorisé à gérer. Peut observer une session utilisateur et exécuter des commandes pour cet utilisateur. Peut effectuer les opérations du mode maintenance. Peut utiliser les options de contrôle de l'alimentation pour les machines avec OS mono-session. Impossible d'accéder aux vues Tableau de bord, Tendances, Alertes ou Filtres. Ne peut utiliser les options de contrôle de l'alimentation pour les machines avec OS multi-session. |
| Administrateur du catalogue de machines | Peut accéder uniquement à la page Détails de machine (recherche machine). |
| Administrateur hôte | Aucun accès. Cet administrateur n'est pas pris en charge pour Director et ne peut pas afficher les données. |

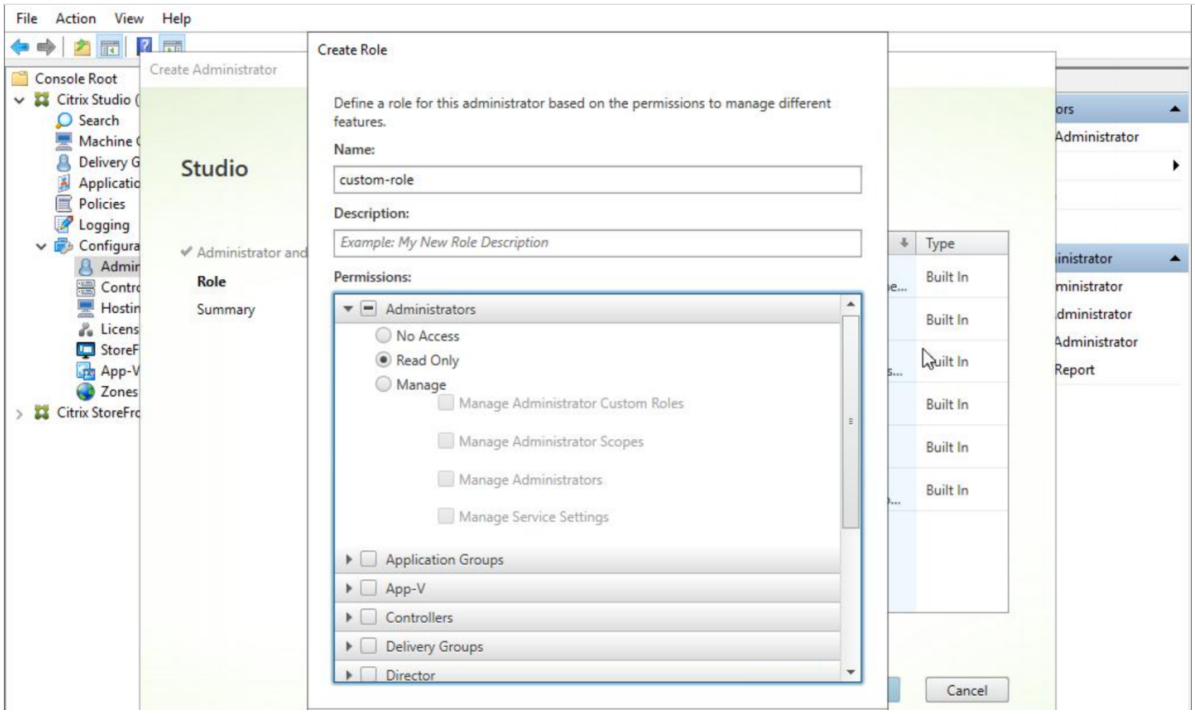
 

### Configurer les rôles personnalisés pour les administrateurs Director

Dans Studio, vous pouvez également configurer des rôles spécifiques à Director, personnalisés pour correspondre plus étroitement aux besoins de votre organisation et déléguer des permissions de manière plus flexible. Par exemple, vous pouvez limiter le rôle d'administrateur du Bureau d'assistance intégré afin que cet administrateur ne puisse pas fermer de sessions.

Si vous créez un rôle personnalisé avec les permissions Director, vous devez également donner à ce rôle d'autres permissions génériques :

- Permissions pour le Delivery Controller de se connecter à Director : au minimum un accès en lecture seule au nœud Administrateur
- Permissions pour les groupes de mise à disposition pour afficher les données liées à ces groupes de mise à disposition dans Director, un accès en lecture seule au minimum.




Éventuellement, vous pouvez créer un rôle personnalisé en copiant un rôle existant et inclure des permissions supplémentaires pour différentes vues. Par exemple, vous pouvez copier le rôle du Bureau d'assistance et inclure des permissions pour afficher les pages Tableau de bord ou Filtres.

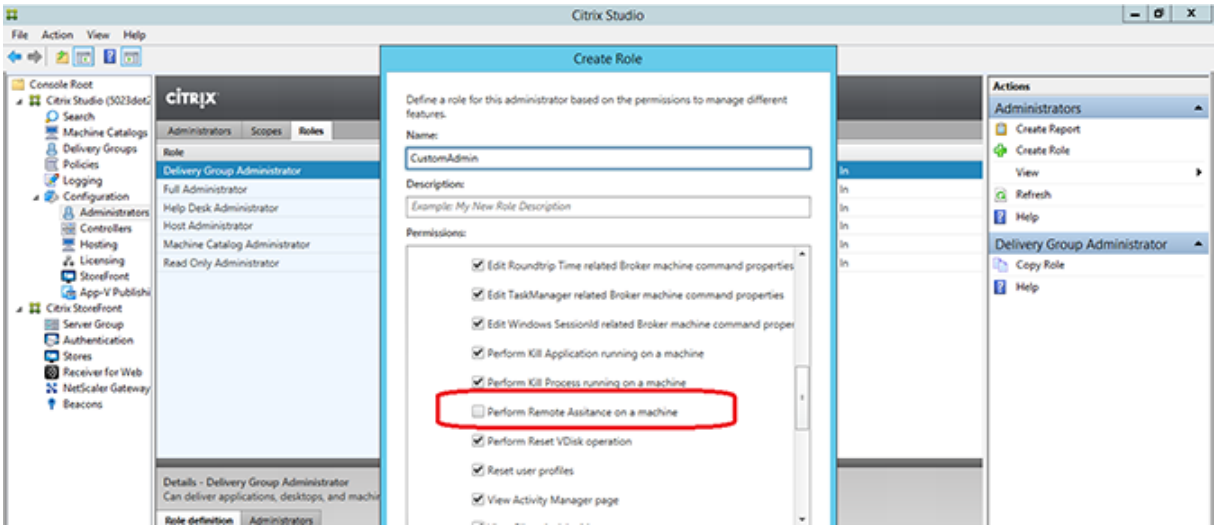
Sélectionnez les permissions de Director pour le rôle personnalisé, y compris :

- Arrêter l'application en cours d'exécution sur une machine
- Arrêter le processus en cours d'exécution sur une machine
- Intervenir à distance sur une machine
- Réinitialiser les profils utilisateur
- Afficher la page des détails du client

- Afficher la page du tableau de bord
- Afficher la page Filtres
- Afficher la page Détails de la machine
- Afficher la page des tendances
- Afficher la page des détails utilisateur

Dans cet exemple, l'observation (Effectuer une intervention à distance sur une machine) est désactivée.




Une permission peut dépendre d'autres permissions pour pouvoir s'appliquer sur l'interface utilisateur. Par exemple, la sélection de la permission **Arrêter l'application en cours d'exécution sur une machine** active la fonctionnalité **Arrêter l'application** uniquement dans les panneaux sur lesquels le rôle a la permission. Vous pouvez sélectionner les permissions de panneau suivantes :

- Afficher la page Filtres
- Afficher la page des détails utilisateur
- Afficher la page Détails de la machine
- Afficher la page des détails du client

En outre, depuis la liste des permissions pour d'autres composants, prenez en compte ces permissions des groupes de mise à disposition :

- Activer/désactiver le mode de maintenance d'une machine via l'appartenance à un groupe de mise à disposition
- Réaliser des opérations d'alimentation sur les machines de bureau Windows via l'appartenance à un groupe de mise à disposition
- Réaliser la gestion de session sur les machines via l'appartenance à un groupe de mise à disposition

# Sécuriser le déploiement de Director

June 27, 2024

Cet article dresse la liste des domaines susceptibles d'avoir un impact sur la sécurité du système lors du déploiement et de la configuration de Director.

## Configurer Microsoft Internet Information Services (IIS)

Vous pouvez configurer Director avec une configuration IIS limitée.

### Limites de recyclage du pool d'applications

Vous pouvez définir les limites de recyclage du pool d'applications suivantes :

- Limite de mémoire virtuelle : 4 294 967 295
- Limite de mémoire privée : taille de la mémoire physique du serveur StoreFront
- Nombre limite de demandes : 4 000 000 000

### Extensions de nom de fichier

Vous pouvez interdire les extensions de nom de fichier non répertoriées.

Director requiert ces extensions de nom de fichier dans le Filtrage des demandes :

- .aspx
- .css
- .html
- .js
- .png
- .svc
- .png
- .json
- .woff
- .woff2
- .ttf

Director requiert les verbes HTTP suivants dans le Filtrage des demandes : Vous pouvez interdire les verbes non répertoriés.

- GET

- POST
- HEAD

Director ne requiert pas ce qui suit :

- Filtres ISAPI
- Extensions ISAPI
- Programmes CGI
- Programmes FastCGI

> **Important :**
>
> - Director requiert l'approbation Confiance totale. Ne définissez pas le niveau de confiance .NET global sur Élevé ou Moyen.
> - Director gère un pool d'applications distinct. Pour modifier les paramètres de Director, sélectionnez le site Director et modifiez-le.

### Configurer les droits des utilisateurs

Lorsque Director est installé, ses pools d'applications se voient accorder les autorisations suivantes :

- Droit d'ouverture de session **Ouvrir une session en tant que service**
- Privilèges **Ajuster les quotas de mémoire pour un processus**, **Générer des audits de sécurité**et **Remplacer un jeton de niveau processus**

Les droits et privilèges mentionnés sont un comportement d'installation normal lors de la création de pools d'applications.

Vous n'avez pas besoin de changer ces droits d'utilisateur. Ces privilèges ne sont pas utilisés par Director et sont automatiquement désactivés.

### Communications Director

Dans un environnement de production, utilisez Internet Protocol Security (IPsec) ou le protocole HTTPS pour sécuriser le transfert des données entre Director et vos serveurs.

IPsec est un ensemble d'extensions standard du protocole Internet qui garantit des communications authentifiées et cryptées avec intégrité des données et protection contre la relecture. IPsec étant un ensemble de protocoles de couches réseau, les protocoles d'un niveau plus élevé peuvent l'utiliser sans modification. HTTPS utilise les protocoles Transport Layer Security (TLS) pour fournir un cryptage puissant des données.

> **Remarque :**
>
> - Citrix recommande fortement de restreindre l'accès à la console Director au sein du réseau intranet.
> - Citrix vous recommande de ne pas autoriser les connexions non sécurisées à Director dans un environnement de production.
> - Les communications sécurisées en provenance de Director requièrent une configuration séparée pour chaque connexion.
> - Le protocole SSL n'est pas recommandé. Utilisez plutôt le protocole TLS plus sécurisé.
> - Sécurisez les communications avec Citrix ADC à l'aide de TLS, et non IPsec.

Pour sécuriser les communications entre Director et les serveurs Citrix Virtual Apps and Desktops (pour le suivi et la création de rapports), reportez-vous à la section Sécurisation de l'accès aux données.

Pour sécuriser les communications entre Director et Citrix ADC (pour Citrix Insight), reportez-vous à la section Configurer l'analyse réseau.

Pour sécuriser les communications entre Director et le serveur de licences, reportez-vous à la section Sécuriser la console License Administration Console.

### Séparation de la sécurité de Director

Vous pouvez déployer n'importe quelle application Web dans le même domaine Web (nom de domaine et port) que Director. Toutefois, tout risque de sécurité dans ces applications Web peut potentiellement réduire la sécurité de votre déploiement Director. Lorsqu'un degré plus important de séparation de la sécurité est nécessaire, Citrix recommande de déployer Director dans un domaine Web distinct.

## Configuration de sites locaux avec Citrix Analytics for Performance

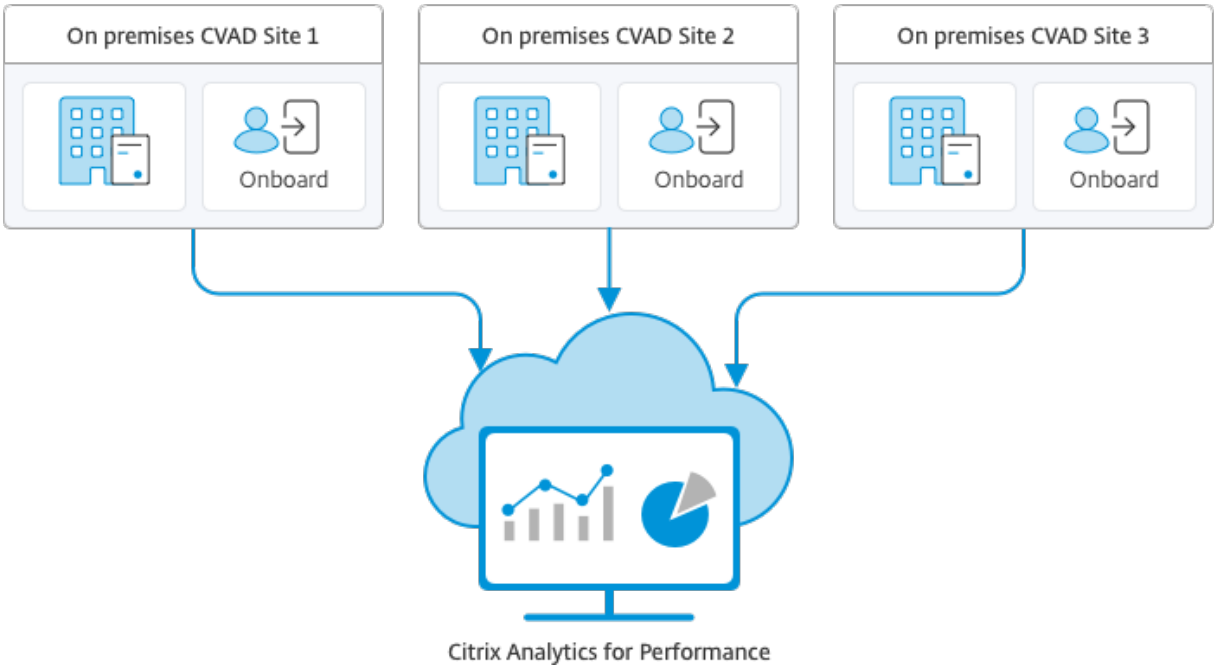
June 27, 2024

Citrix Analytics for Performance (Performance Analytics) est la solution complète de surveillance des performances du service cloud Citrix Analytics. Performance Analytics fournit des informations avancées et des analyses reposant sur des mesures de performance. Analyse des performances vous aide à surveiller et à afficher les mesures d'utilisation et de performances d'un ou de plusieurs sites Citrix Virtual Apps and Desktops de votre organisation.

Pour plus d'informations sur Performance Analytics, consultez l'article sur Performance Analytics.

Vous pouvez envoyer des données de performances depuis votre site à Citrix Analytics for Performance sur Citrix Cloud afin de tirer parti de ses fonctionnalités avancées d'analyse des performances. Pour afficher et utiliser Performance Analytics, vous devez d'abord configurer vos sites locaux avec Citrix Analytics for Performance à partir de l'onglet **Analytics** de **Director**.




Performance Analytics accède aux données de manière sécurisée et aucune donnée n'est transférée de Citrix Cloud vers l'environnement local.

## Logiciel requis

Pour configurer Citrix Analytics for Performance à partir de Director, aucun nouveau composant n'a besoin d'être installé. Assurez-vous que les conditions suivantes sont remplies :

- Votre Delivery Controller et Director sont à la version 1912 CU2 ou ultérieure. Pour de plus amples informations, consultez la section Tableau de compatibilité des fonctionnalités.

> **Remarque :**
>
> - La configuration de votre site local avec Citrix Analytics for Performance depuis Director peut échouer si le Delivery Controller exécute une version de Microsoft .NET Framework antérieure à 4.8. Pour contourner le problème, mettez à niveau .NET Framework dans votre Delivery Controller vers la version 4.8. LCM-9255.
> - Lorsque vous configurez votre site local exécutant Citrix Virtual Apps and Desktops version 2012 avec Citrix Analytics for Performance à partir de Director, la configuration peut échouer après quelques heures ou après un redémarrage du service Citrix Monitor dans

> le Delivery Controller. L'onglet Analytics affiche l'état Non connecté dans ce cas. Pour contourner ce problème, créez un dossier Encryption dans le registre du Delivery Controller, Emplacement : HKEY_LOCAL_MACHINE\Software\Citrix\XDServices\Monitor, Nom du dossier : Encryption. Assurez-vous que le compte CitrixMonitor dispose d'un accès en contrôle total sur le dossier Encryption. Redémarrez le service Citrix Monitor.DIR-14324.

- Seuls les administrateurs complets peuvent accéder à l'onglet **Analytics** pour effectuer cette configuration.
- Pour que Performance Analytics puisse accéder aux mesures de performances, un accès Internet sortant est disponible sur tous les Delivery Controller et sur les machines sur lesquelles Director est installé. Plus précisément, assurez-vous de l'accessibilité aux URL suivantes :
  - Enregistrement de la clé Citrix : `https://*.citrixnetworkapi.net/`
  - Citrix Cloud : `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics : `https://*.cloud.com/`
  - Microsoft Azure : `https://*.windows.net/`
    Dans le cas où les Delivery Controller et les machines Director se trouvent dans un intranet et l'accès Internet sortant se fait via un serveur proxy, assurez-vous de ce qui suit :
- Le serveur proxy doit autoriser la liste d'adresses URL précédente.
- Ajoutez la configuration suivante dans les fichiers web.config et citrix.monitor.exe.config de Director. Assurez-vous d'ajouter cette configuration dans les balises **configuration** :

```
<system.net>
    <defaultProxy>
        <proxy  usesystemdefault = "false"  proxyaddress = "http
            ://<your_proxyserver_address>:80" bypassonlocal = "
            true"  />
    </defaultProxy>
</system.net>
```

  - Le fichier web.config de Director se trouve sous `C:\inetpub\wwwroot\Director\web.config` sur la machine sur laquelle Director est installé.
  - Le fichier citrix.monitor.exe.config se trouve sous `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` sur la machine sur laquelle le Delivery Controller est installé.

  Ce paramètre est fourni par Microsoft sur IIS. Pour plus d'informations, consultez `https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration`.
  Le champ **defaultproxy** du fichier de configuration contrôle l'accès sortant de Director et de Monitor Service. La configuration et la communication avec Performance Analytics nécessitent que le champ **defaultproxy** soit défini sur **true**. Il est possible que les stratégies en vigueur

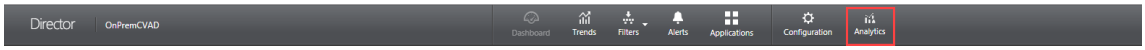
définissent ce champ sur false. Dans ce cas, vous devez définir manuellement le champ sur true. Effectuez une sauvegarde des fichiers de configuration avant d'effectuer les modifications. Redémarrez Monitor Service sur le Delivery Controller pour que les modifications soient appliquées.

- Vous disposez d'un droit Citrix Cloud actif pour Citrix Analytics for Performance.
- Votre compte Citrix Cloud est un compte Administrateur disposant de droits sur l'expérience d'enregistrement de produit. Pour plus d'informations sur les autorisations d'administrateur, consultez la section Modifier les autorisations d'administrateur.

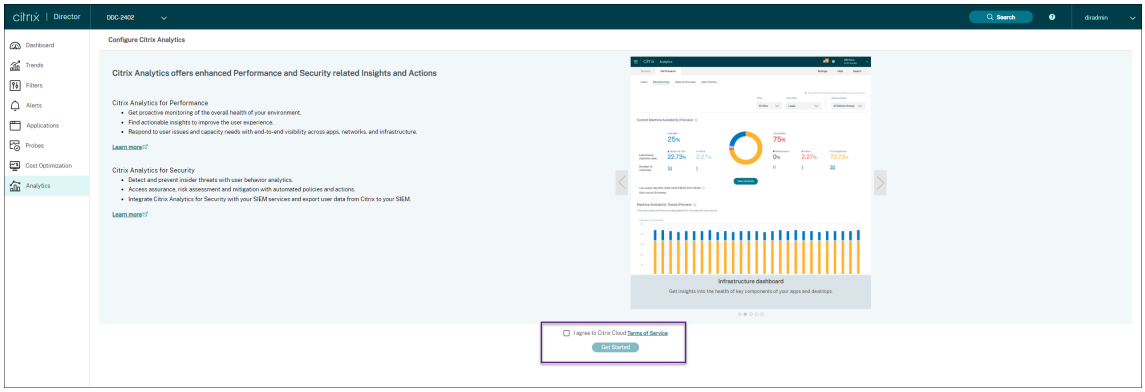
## Étapes de configuration

Après avoir vérifié les conditions préalables, procédez comme suit :

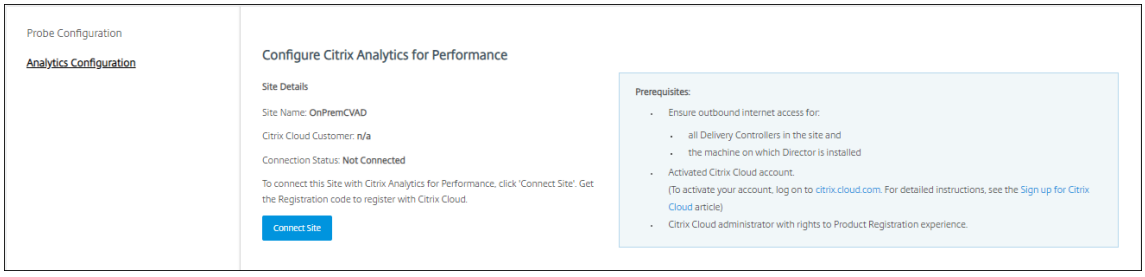
1. Connectez-vous à Director en tant qu'administrateur complet et sélectionnez le site que vous souhaitez configurer avec l'analyse des performances. La page Tableau de bord Director s'affiche.




2. Cliquez sur l'onglet **Analytics**. La page **Configurer Citrix Analytics** s'affiche.




3. Passez en revue les étapes, sélectionnez les conditions d'utilisation, puis cliquez sur **Mise en route**. La page **Détails du site** s'affiche.

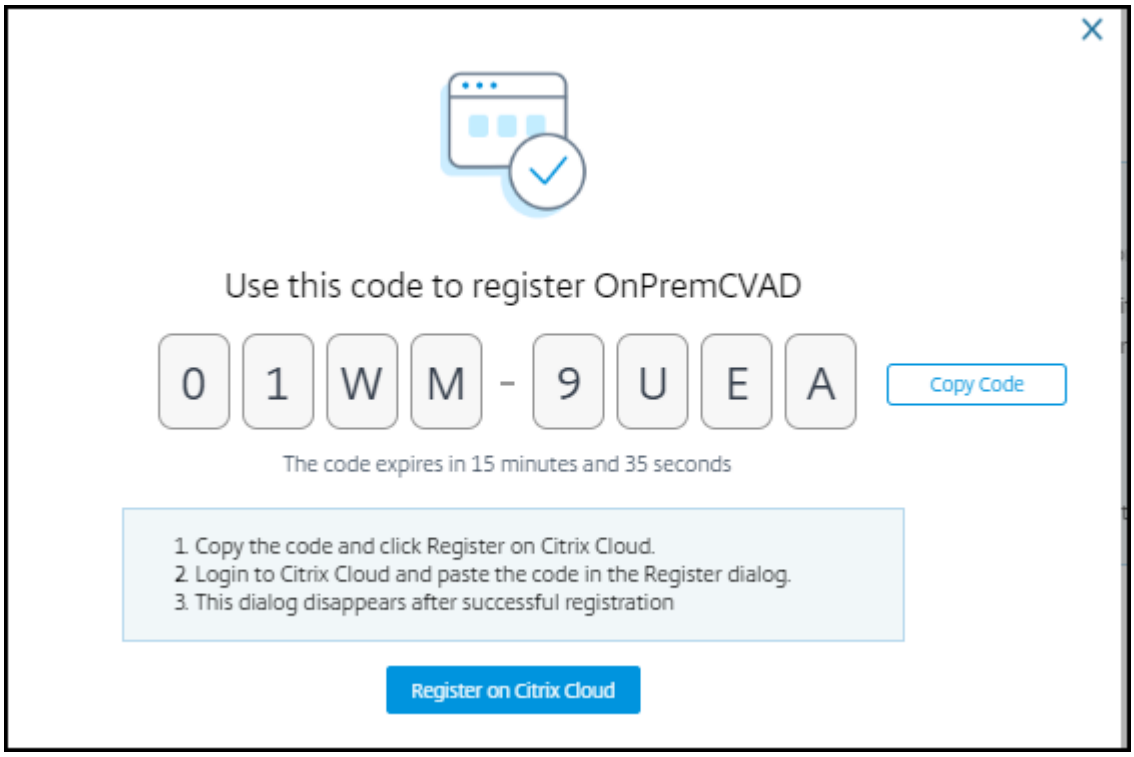



4. Examinez les conditions préalables et assurez-vous qu'elles sont remplies. Examinez les détails du site.

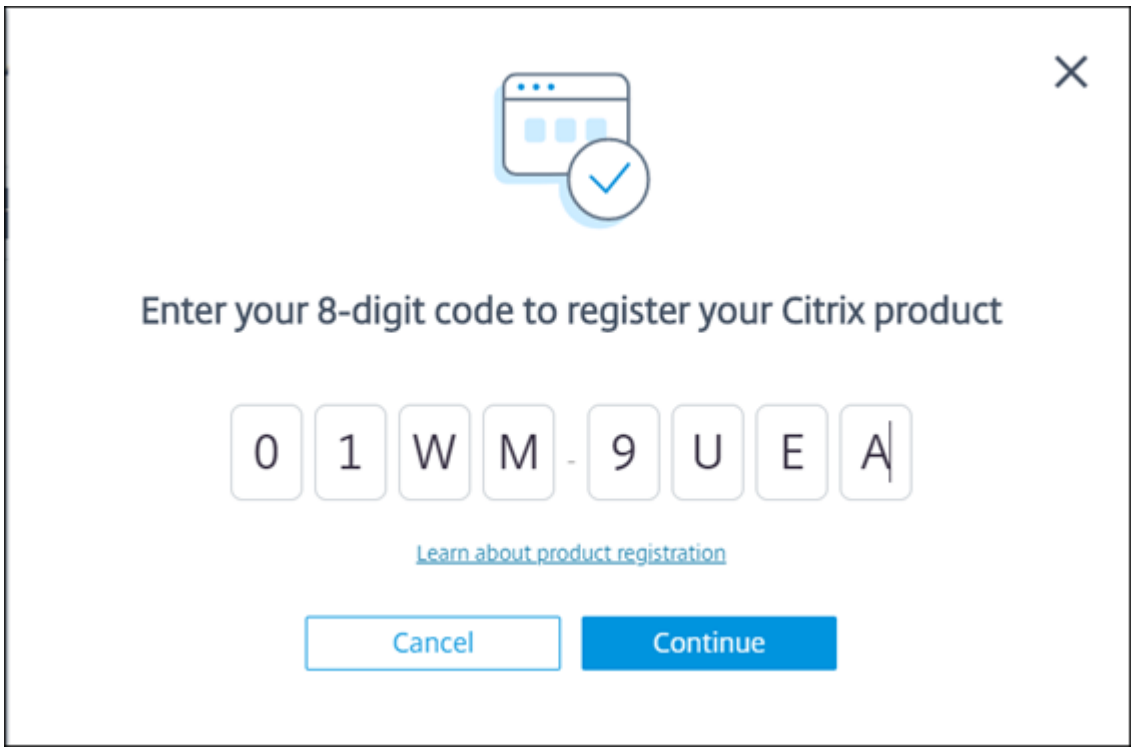
5. Cliquez sur **Connecter le site** pour démarrer le processus de configuration.

   Un code d'enregistrement unique à 8 chiffres est généré ; il sera utilisé pour enregistrer ce site auprès de Citrix Cloud.



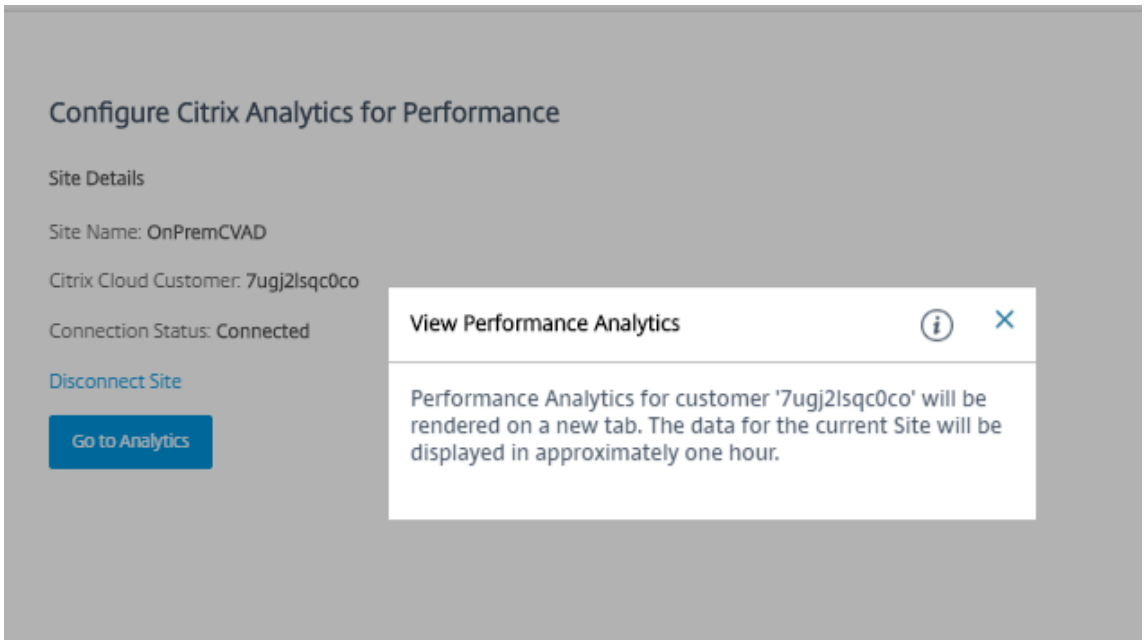

6. Cliquez sur **Copier le code** pour copier le code, puis cliquez sur **S'enregistrer sur Citrix Cloud**. Vous êtes redirigé vers l'URL d'enregistrement dans Citrix Cloud.
7. Connectez-vous avec vos informations d'identification Citrix Cloud, puis sélectionnez votre client.
8. Collez le code d'enregistrement copié dans la page Enregistrements de produits dans Citrix Cloud. Cliquez sur **Continuer** pour vous inscrire. Vérifiez les détails de l'enregistrement, puis cliquez sur **Enregistrer**.



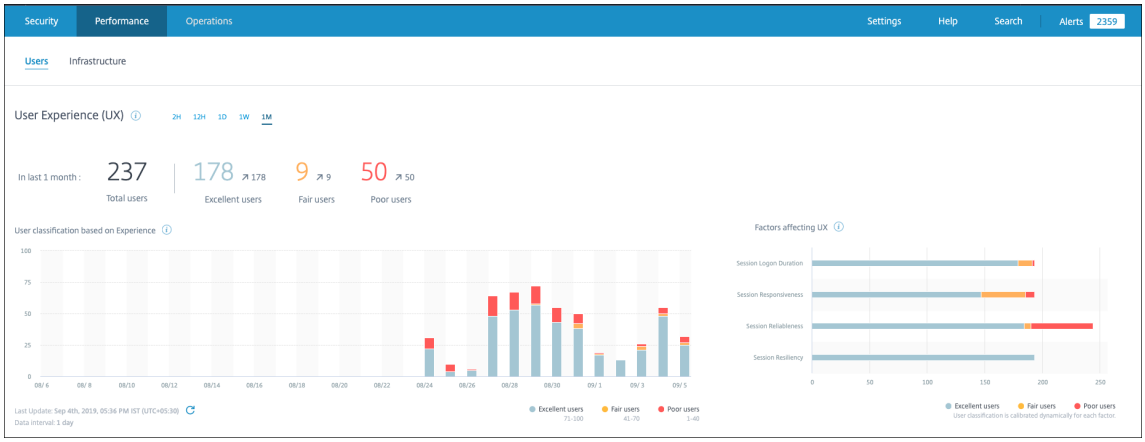

Votre site local s'enregistre auprès de Citrix Cloud.

9. Dans **Director**, cliquez sur **Aller à Analytics** dans l'onglet **Analytics**.




L'analyse des performances s'ouvre sur un nouvel onglet de votre navigateur.




Si votre session Citrix Cloud a expiré, vous pouvez être redirigé vers la page d'ouverture de session Citrix.com ou Mon compte Citrix.

10. Pour enregistrer plusieurs sites auprès de Performance Analytics, répétez les étapes de configuration précédentes pour chaque site depuis Director. Les mesures de tous les sites configurés sont affichées dans le tableau de bord Performance Analytics.

    Si plusieurs instances de Director sont exécutées par site, configurez à partir de n'importe quelle des instances de Director. Toutes les autres instances de Director connectées au site seront mises à jour lors de la prochaine actualisation après le processus de configuration.

11. Pour déconnecter votre site de Citrix Cloud, cliquez sur **Déconnecter le site**. Cette option supprime la configuration existante.

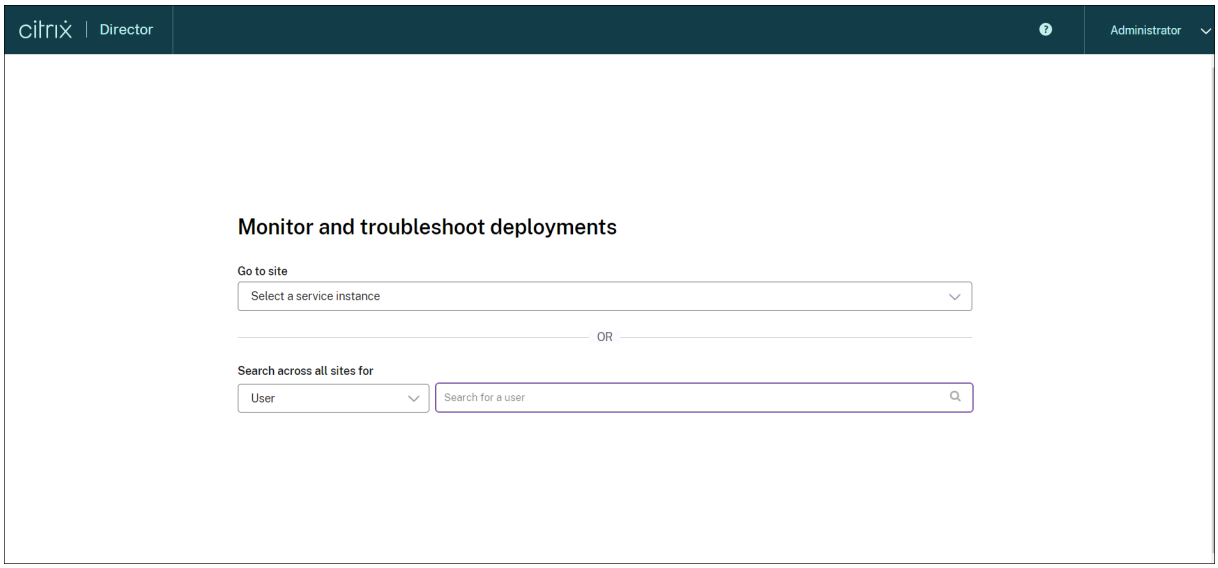
    > **Remarques :**
    >
    > La première fois que vous configurez un site, le traitement des événements du site peut prendre un certain temps (environ une heure), ce qui entraîne un retard dans l'affichage des mesures dans le tableau de bord Performance Analytics. Par la suite, les événements sont actualisés à intervalles réguliers.
    >
    > Lors de la déconnexion, la transmission des données à partir de l'ancien compte se poursuit pendant un certain temps jusqu'à ce que les événements du nouveau compte soient transmis. Pendant environ une heure après l'arrêt de la transmission des données, les analyses liées à l'ancien compte restent affichées dans le tableau de bord Performance Analytics.
    >
    > À l'expiration du droit au service Citrix Analytics, l'arrêt de l'envoi des mesures du site à Performance Analytics peut prendre jusqu'à un jour.

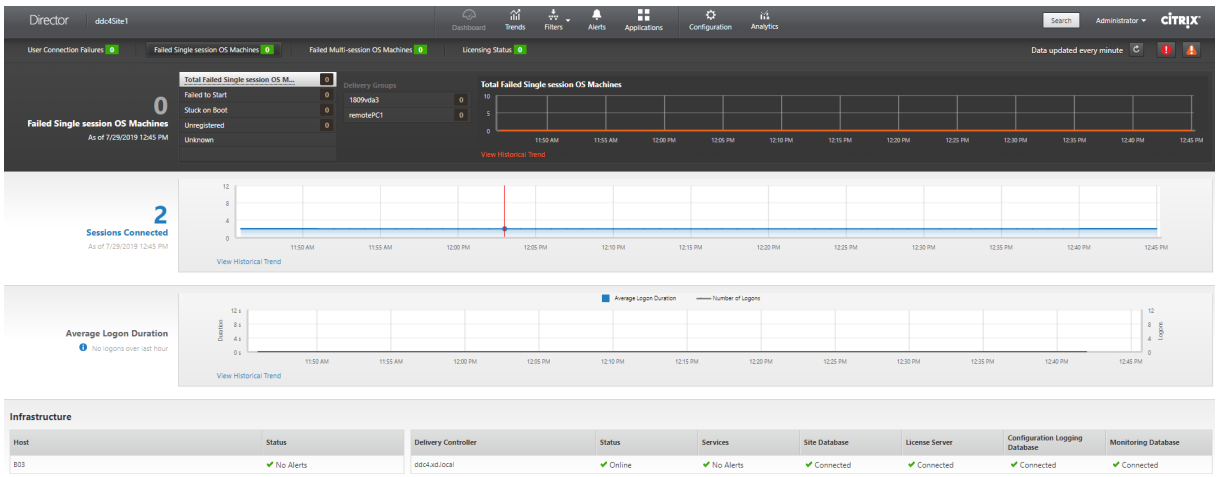
# Analyse de site

June 27, 2024

Vous pouvez surveiller l'état de santé de vos déploiements à l'aide de Director. Vous pouvez résoudre les problèmes de performances en recherchant un utilisateur, un terminal ou une machine sur tous les sites intégrés.




Avec une permission d'administrateur complet, lorsque vous ouvrez Director, le Tableau de bord fournit un emplacement centralisé permettant de surveiller l'intégrité et l'utilisation d'un site.




S'il n'existe actuellement aucune erreur et qu'aucune erreur ne s'est produite au cours des dernières 60 minutes, les panneaux ne s'affichent pas. Lorsqu'il existe des erreurs, le panneau d'échec spécifique s'affiche automatiquement.

> **Remarque :**
>
> En fonction des licences de votre organisation et des privilèges de l'administrateur, certaines options ou fonctionnalités risquent de ne pas être disponibles.

## Panneaux sur le tableau de bord Director

### Échecs de connexion utilisateur

Échecs de connexion lors des dernières 60 minutes. Cliquez sur les catégories situées en regard du nombre total pour afficher les métriques pour ce type d'échec. Dans la table suivante, ce nombre est réparti par groupe de mise à disposition. Échecs de connexion inclut les erreurs causées par les limites d'application qui sont atteintes. Pour de plus amples informations sur les limites d'application, consultez la section Applications.

### Machines en panne avec OS mono-session ou machines en panne avec OS multi-session

Nombre total d'échecs dans les dernières 60 minutes réparties par groupes de mise à disposition. Échecs répartis par types, y compris les échecs de démarrage, bloqués au démarrage, et non enregistrés. Pour les machines avec OS multi-session, les erreurs comprennent également le moment où les machines atteignent une charge maximale.

### État des licences

Les alertes du serveur de licences affichent des alertes envoyées par le serveur de licences et les actions requises pour la résolution des alertes. Requiert le serveur de licences 11.12.1 ou version ultérieure. Les alertes Delivery Controller affichent les détails de l'état des licences comme elles sont vues par le Controller et sont envoyées par le Controller. Requiert un Controller pour XenApp 7.6 ou XenDesktop 7.6 ou version ultérieure. Vous pouvez définir le seuil des alertes dans Studio. L'état de licence affiché dans **Delivery Controller** > **Détails** > **Édition du produit** > **PLT** indique **Premium** et non **Platinum**.

### État de grâce

Director affiche l'un des états de grâce suivants. Ces informations sont récupérées à partir du Delivery Controller.

1. **Non actif :** option non présente dans n'importe quel type de délai de grâce. Des limites normales au niveau des licences s'appliquent.

2. **Période de grâce d'urgence :** entre en vigueur lorsque le serveur de licences est inaccessible ou lorsque les informations de licence ne peuvent pas être récupérées lors de la négociation d'une connexion. Les utilisateurs ne sont pas affectés. Les erreurs affichées dans Director ne peuvent pas être rejetées tant que le serveur de licences n'est pas accessible.
3. **Période de grâce expirée :** la période de grâce d'urgence ou la période de grâce supplémentaire a expiré.

Pour plus d'informations, consultez Découvert de licences et Période de grâce supplémentaire.

#### Session(s) connectée(s)

Sessions connectées sur tous les groupes de mise à disposition pour les dernières 60 minutes.

#### Durée moyenne

Données d'ouverture de session pour les dernières 60 minutes. Le nombre important sur la gauche est la durée moyenne d'ouverture de session sur l'heure en cours. Les données d'ouverture de session pour les VDA antérieurs à XenDesktop 7.0 ne sont pas incluses dans cette moyenne. Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.

#### Infrastructure

Dresse la liste de l'infrastructure de votre site –hôtes et Controller. Pour l'infrastructure de XenServer ou VMware, vous pouvez afficher les alertes de performance. Par exemple, vous pouvez configurer XenCenter pour générer des alertes de performances lorsque l'utilisation de l'UC, E/S réseau ou E/S disque dépasse un seuil spécifié sur un serveur ou une machine virtuelle géré(e). Par défaut, l'intervalle de répétition d'alerte est de 60 minutes, mais vous pouvez le configurer. Pour en savoir plus, consultez la section Alertes de performance XenCenter dans la documentation produit XenServer.

> **Remarque :**
>
> L'absence d'icône pour une mesure donnée indique que cette mesure n'est pas prise en charge par le type de l'hôte utilisé. Par exemple, aucune information d'intégrité n'est disponible pour les hôtes System Center Virtual Machine Manager (SCVMM), AWS et CloudStack.

Continuez à résoudre les problèmes à l'aide de ces options (décrites dans les sections suivantes) :

- Contrôler l'alimentation de la machine utilisateur
- Empêcher les connexions aux machines

### Contrôler des sessions

Si une session devient déconnectée, elle reste active et ses applications continuent d'être exécutées, mais la machine cliente ne communique plus avec le serveur.

| Action | Description |
| --- | --- |
| Afficher la machine ou la session actuellement connectée de l'utilisateur | À partir des vues Gestionnaire d'activités et Détails de l'utilisateur, affichez la machine ou la session actuellement connectée de l'utilisateur et une liste de toutes les machines et des sessions auxquelles cet utilisateur a accès. Pour accéder à cette liste, cliquez sur l'icône de sélection de session dans la barre de titre utilisateur. Pour plus d'informations, consultez la section Restaurer les sessions. |
| Afficher le nombre total de sessions déconnectées sur tous les groupes de mise à disposition | Dans le tableau de bord, dans le volet **Sessions connectées**, affichez le nombre total de sessions connectées sur tous les groupes de mise à disposition pendant les 60 dernières minutes. Puis cliquez sur le nombre total, qui ouvre la vue Filtres, où vous pouvez afficher les données de session graphiques basées sur les groupes de mise à disposition sélectionnés et les plages et l'utilisation au travers des groupes de mise à disposition. |
| Mettre fin aux sessions inactives | La vue Filtres de session affiche des données relatives à toutes les sessions actives. Filtrez les sessions en fonction de l'utilisateur associé, du groupe de mise à disposition, de l'état de la session et du temps d'inactivité supérieur à un seuil spécifié. Dans la liste filtrée, sélectionnez les sessions à fermer. Pour obtenir davantage d'informations, veuillez consulter la section Résolution des problèmes d'applications. |

| Action | Description |
| --- | --- |
| Afficher les données sur une période plus longue | Dans la vue Tendances, sélectionnez l'onglet **Sessions** pour afficher des données d'utilisation plus spécifiques pour les sessions connectées et déconnectées sur une période de temps plus longue (nombre total de sessions antérieur aux 60 dernières minutes). Pour afficher ces informations, cliquez sur **Afficher les tendances historiques**. |

> **Remarque :**
>
> Si la machine utilisateur exécute un Virtual Delivery Agent (VDA) d'ancienne génération, telle qu'un VDA antérieur à la version 7 ou un Linux VDA, Director ne peut pas afficher d'informations complètes sur la session. Un message s'affiche indiquant que les informations ne sont pas disponibles.

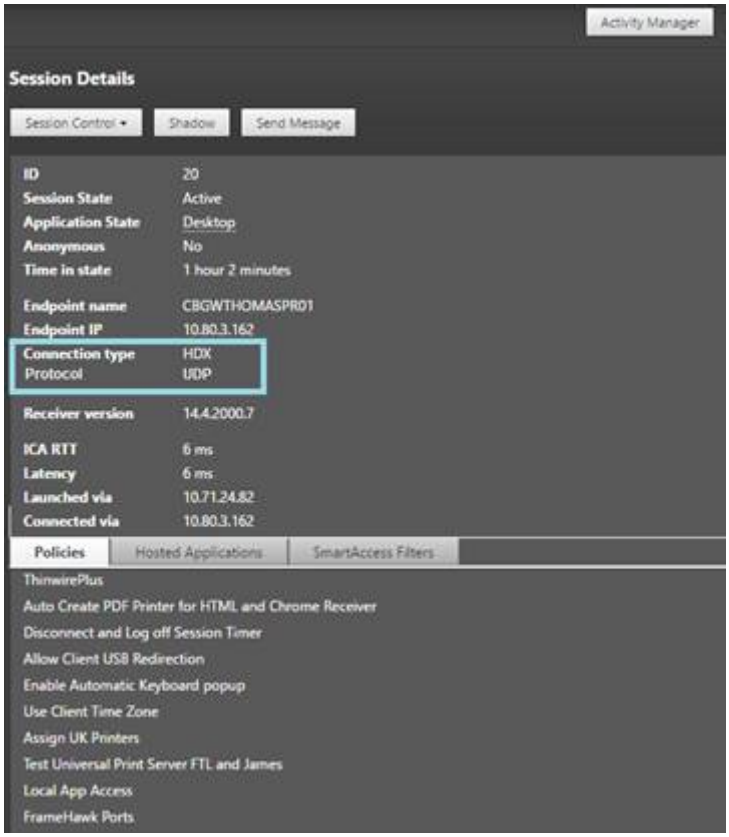
**Limite des règles d'attribution de bureau :**
Web Studio permet l'attribution de plusieurs règles d'attribution de bureau (DAR) pour différents utilisateurs ou groupes d'utilisateurs à un seul VDA du groupe de mise à disposition. StoreFront affiche le bureau attribué avec le **nom d'affichage** correspondant selon le DAR de l'utilisateur connecté. Toutefois, Director ne prend pas en charge les fichiers DAR et affiche le bureau attribué à l'aide du nom de groupe de mise à disposition indépendamment de l'utilisateur connecté. Par conséquent, vous ne pouvez pas mapper un bureau spécifique à une machine dans Director.
Vous pouvez mapper le bureau attribué affiché dans StoreFront au nom du groupe de mise à disposition affiché dans Director à l'aide de la commande PowerShell suivante :

```
Get-BrokerDesktopGroup | Where-Object {
  \$\_.Uid -eq \(Get-BrokerAssignmentPolicyRule | Where-Object {
  \$\_.PublishedName -eq \"\<Name on StoreFront\>\"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
```

### Protocole de transport de session

Affichez le protocole de transport utilisé pour le type de connexion HDX associé à la session en cours dans le panneau **Détails de session**. Ces informations sont disponibles pour les sessions lancées sur des VDA 7.13 ou version ultérieure.




- Pour le type de connexion **HDX** :
  - Le protocole affiché est **UDP**, si EDT est utilisé pour la connexion HDX.
  - Le protocole affiché est **TCP**, si TCP est utilisé pour la connexion HDX.
- Pour le type de connexion **RDP**, le protocole affiché est **S.O.**.

Lorsque le transport adaptatif est configuré, le protocole de transport de la session bascule dynamiquement entre EDT (via UDP) et TCP, selon les conditions de réseau. Si la session HDX ne peut pas être établie à l'aide d'EDT, elle utilise le protocole TCP.

Pour plus d'informations sur la configuration du transport adaptatif, consultez la section Transport adaptatif.

### Exporter des rapports

Vous pouvez exporter les données sur les tendances pour générer des rapports d'utilisation et de gestion de la capacité. L'exportation prend en charge les formats de rapport PDF, Excel et CSV. Les rapports aux formats PDF et Excel contiennent les tendances représentées sous la forme de graphiques et de tableaux. Les rapports au format CSV contiennent des données tabulaires pouvant être traitées pour générer des vues ou être archivées.

Pour exporter un rapport :

1. Accédez à l'onglet **Tendances**.
2. Définissez les critères de filtrage et la période, puis cliquez sur **Appliquer**. Le graphique et le tableau des tendances sont renseignés avec les données.
3. Cliquez sur **Exporter** et entrez le nom et le format du rapport.

Director génère le rapport en fonction des critères de filtre que vous avez sélectionnés. Si vous modifiez les critères de filtre, cliquez sur **Appliquer** avant de cliquer sur **Exporter**.

> **Remarque :**
>
> Exporter une grande quantité de données entraîne une augmentation significative de la consommation de mémoire et d'UC pour le serveur Director, le Delivery Controller et les serveurs SQL. Le nombre d'opérations d'exportation simultanées et le volume de données qui peuvent être exportées sont définis sur les limites par défaut permettant d'obtenir les meilleures performances d'exportation.

#### Limites d'exportation prises en charge

Les rapports PDF et Excel exportés contiennent des graphiques complets pour les critères de filtre sélectionnés. Toutefois, les données tabulaires de tous les formats de rapport sont tronquées au-delà des limites par défaut sur le nombre de lignes ou d'enregistrements dans le tableau. Le nombre de données pris en charge par défaut est défini en fonction du format du rapport.

Vous pouvez modifier la valeur par défaut en configurant les paramètres d'application Director dans Internet Information Services (IIS).

| Format de rapport | Nombre d'enregistrements pris en charge par défaut | Champs dans les paramètres d'application Director | Nombre maximal d'enregistrements pris en charge |
|---|---|---|---|
| PDF | 500 | UI.ExportPdfDrilldownLimit | 5 000 |
| Excel | 100 000 | UI.ExportExcelDrilldownLimit | 1 000 000 |
| CSV | 100 000 (10 000 000 dans l'onglet **Sessions**) | UI.ExportCsvDrilldownLimit | 10 000 000 |

Pour modifier la limite du nombre d'enregistrements que vous pouvez exporter :

1. Ouvrez la console du gestionnaire IIS.
2. Accédez au site Web Director sous le site Web par défaut.
3. Cliquez deux fois sur **Paramètres d'application**.

4. Modifiez ou ajoutez un paramètre pour les champs UI.ExportPdfDrilldownLimit, UI.ExportExcelDrilldownLim ou UI.ExportCsvDrilldownLimit selon vos besoins.

L'ajout de ces valeurs de champ dans Paramètres d'application remplace les valeurs par défaut.

> **Avertissement :**
>
> La définition de valeurs de champ supérieures au nombre maximal d'enregistrements pris en charge peut avoir un impact sur les performances d'exportation et n'est pas prise en charge.

#### Gestion des erreurs

Cette section explique comment gérer les erreurs que vous pourriez rencontrer lors de l'opération d'exportation.

- **Director a expiré**

Cette erreur peut se produire en raison de problèmes de réseau ou d'utilisation élevée des ressources sur le serveur Director ou par le service de surveillance.

Le délai d'expiration par défaut est de 100 secondes. Pour augmenter le délai d'expiration de Director Service, définissez la valeur du champ **Connector.DataServiceContext.Timeout dans** les paramètres d'application Director dans Internet Information Services (IIS) :

1. Ouvrez la console du gestionnaire IIS.
2. Accédez au site Web Director sous le site Web par défaut.
3. Cliquez deux fois sur **Paramètres d'application**.
4. Modifiez la valeur **Connector.DataServiceContext.Timeout**.

- **Le service de surveillance a expiré**

Cette erreur peut se produire en raison de problèmes de réseau ou d'utilisation élevée des ressources sur le serveur SQL ou par le service de surveillance.

Pour augmenter le délai d'expiration du service de surveillance, exécutez les commandes PowerShell suivantes sur le Delivery Controller :

```
asnp Citrix.*
Get-MonitorConfiguration
Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- **Opérations d'exportation ou d'aperçu max. simultanées en cours**

Director prend en charge une seule instance d'exportation ou d'aperçu. Si vous recevez une erreur concernant les **opérations d'exportation ou d'aperçu simultanées maximales**, attendez avant d'effectuer la prochaine opération d'exportation.

Il est possible d'augmenter le nombre d'opérations d'exportation ou d'aperçu simultanées, mais cela peut avoir un impact sur les performances de Director et n'est pas prise en charge :

1. Ouvrez la console du gestionnaire IIS.
2. Accédez au site Web Director sous le site Web par défaut.
3. Cliquez deux fois sur **Paramètres d'application**.
4. Modifiez la valeur **UI.ConcurrentExportLimit**.

- **Espace disque insuffisant dans Director**

Chaque opération d'exportation requiert un maximum de 2 Go d'espace disque disponible dans le dossier temporaire de Windows. Réessayez d'exporter après avoir libéré de l'espace ou ajouté de l'espace disque sur le serveur Director.

### Contrôler les corrections à chaud

Pour afficher les corrections à chaud installées sur un VDA de machine (physique ou machine virtuelle) spécifique, choisissez la vue **Détails de la machine**.

### Contrôler les états d'alimentation de la machine utilisateur

Pour contrôler l'état des machines que vous sélectionnez dans Director, utilisez les options de Contrôle de l'alimentation. Ces options sont disponibles pour les machines avec OS mono-session, mais peuvent ne pas être disponibles pour les machines avec OS multi-session.

> **Remarque :**
>
> Cette fonctionnalité n'est pas disponible pour les machines physiques utilisant Remote PC Access.

| Commande | Fonction |
| --- | --- |
| **Redémarrer** | Effectue une fermeture (en douceur) ordonnée de la machine virtuelle, et tous les processus en cours d'exécution sont arrêtés individuellement avant le redémarrage de la machine virtuelle. Par exemple, sélectionnez les machines qui s'affichent dans Director en tant que « n'a pas réussi à démarrer » et utilisez cette commande pour les redémarrer. |

| Commande | Fonction |
| --- | --- |
| **Forcer le redémarrage** | Redémarre la machine virtuelle sans tenter d'effectuer de procédure de fermeture. Cette commande ne fonctionne de la même manière que lorsque vous débranchez un serveur physique puis le rebranchez et le redémarrez à nouveau. |
| **Arrêter** | Effectue une fermeture (en douceur) ordonnée de la machine virtuelle Tous les processus en cours d'exécution sont arrêtés individuellement. |
| **Forcer l'arrêt** | Arrête la machine virtuelle sans effectuer tout d'abord une procédure de fermeture. Cette commande fonctionne de la même manière que lorsque vous débranchez un serveur physique. Il est possible que tous les processus en cours d'exécution ne soient pas arrêtés, et vous risquez de perdre des données si vous arrêtez la machine virtuelle de cette manière. |
| **Suspendre** | Permet de suspendre une machine virtuelle en cours d'exécution dans son état actuel et stocke cet état dans un fichier sur le référentiel de stockage par défaut. Cette option vous permet de fermer le serveur hôte de la machine virtuelle et plus tard, après le redémarrage, reprendre la machine virtuelle, le retourner à son état d'origine en cours d'exécution. |
| **Reprendre** | Reprend une machine virtuelle suspendue et restaure l'état en cours d'exécution d'origine. |
| **Démarrer** | Démarre une machine virtuelle lorsqu'elle est désactivée (également appelé un démarrage à froid). |

Si les actions du contrôle de l'alimentation échouent, placez le curseur de la souris sur l'alerte et un message contextuel s'affiche avec des détails sur l'échec.

### Empêcher les connexions aux machines

Utiliser le mode maintenance pour empêcher de nouvelles connexions temporairement lorsque l'administrateur approprié effectue des tâches de maintenance sur l'image.

Lorsque vous activez le mode maintenance sur les machines, aucune nouvelle connexion n'est autorisée jusqu'à ce que vous la désactiviez. Si la session des utilisateurs est actuellement ouverte, le mode maintenance prend effet dès que les sessions de tous les utilisateurs sont fermées. Pour les utilisateurs qui ne ferment pas leur session, envoyez un message les informant que les machines vont être arrêtées à un certain moment, et utilisez les commandes d'alimentation pour forcer la fermeture des machines.

1. Sélectionnez la machine dans la vue Détails de l'utilisateur ou un groupe de machines dans la vue Filtres.
2. Sélectionnez le **mode Maintenance** et activez l'option.

Si un utilisateur essaie de se connecter à un bureau affecté lors qu'il se trouve en mode maintenance, un message s'affiche indiquant que le bureau n'est pas disponible. Aucune nouvelle connexion ne peut être effectuée tant que vous n'aurez pas désactivé le mode maintenance.

### Analyse des applications

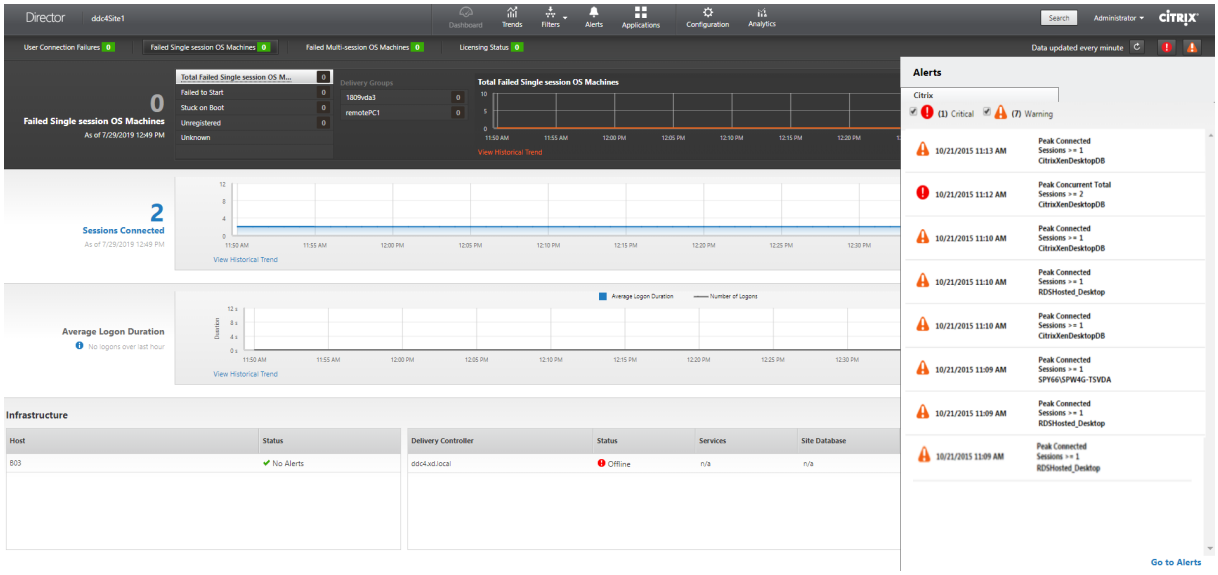
L'onglet **Applications** affiche des analyses basées sur les applications dans une vue consolidée unique pour faciliter l'analyse et la gestion efficaces des performances des applications. Vous pouvez obtenir des informations précieuses sur l'intégrité et l'utilisation de toutes les applications publiées sur le site. Il affiche des métriques telles que les résultats d'analyse, le nombre d'instances par application et les défaillances et erreurs associées aux applications publiées. Pour obtenir davantage d'informations, veuillez consulter la section Analyses des applications sous **Résolution des problèmes d'applications**.

## Alertes et notifications

June 27, 2024

Les alertes sont affichées dans Director sur le tableau de bord et dans d'autres vues de haut niveau avec des symboles d'avertissement et d'alerte critique. Des alertes sont disponibles pour les sites sous licence **Premium**. Les alertes sont mises à jour automatiquement toutes les minutes ; vous pouvez également mettre à jour les alertes à la demande.

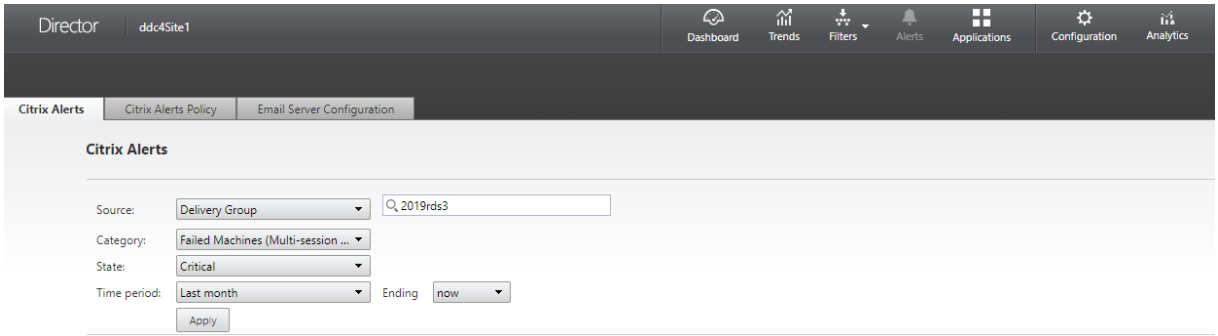



Une alerte d'avertissement (triangle de couleur ambre) indique que le seuil d'avertissement d'une condition a été atteint ou dépassé.

Une alerte critique (cercle rouge) indique que le seuil critique d'une condition a été atteint ou dépassé.

Vous pouvez afficher des informations plus détaillées sur les alertes en sélectionnant une alerte dans la barre latérale, en cliquant sur le lien **Aller aux alertes** dans le bas de la barre latérale ou en sélectionnant **Alertes** dans le haut de la page de Director.

Dans la vue Alertes, vous pouvez filtrer et exporter les alertes. Par exemple, les machines en panne avec OS multi-session pour un groupe de mise à disposition spécifique sur le dernier mois, ou toutes les alertes pour un utilisateur spécifique. Pour de plus amples informations, consultez la section Exporter des rapports.




## Alertes Citrix

Les alertes Citrix sont des alertes que vous pouvez surveiller dans Director provenant de composants Citrix. Vous pouvez configurer les alertes Citrix dans Director sous **Alertes** > **Stratégies d'alerte Citrix**. Dans le cadre de la configuration, vous pouvez définir l'envoi par e-mail de notifications à des

individus et des groupes lorsque les alertes dépassent les seuils que vous avez définis. Pour de plus amples informations sur la configuration des alertes Citrix, consultez la section Créer des stratégies d'alerte.

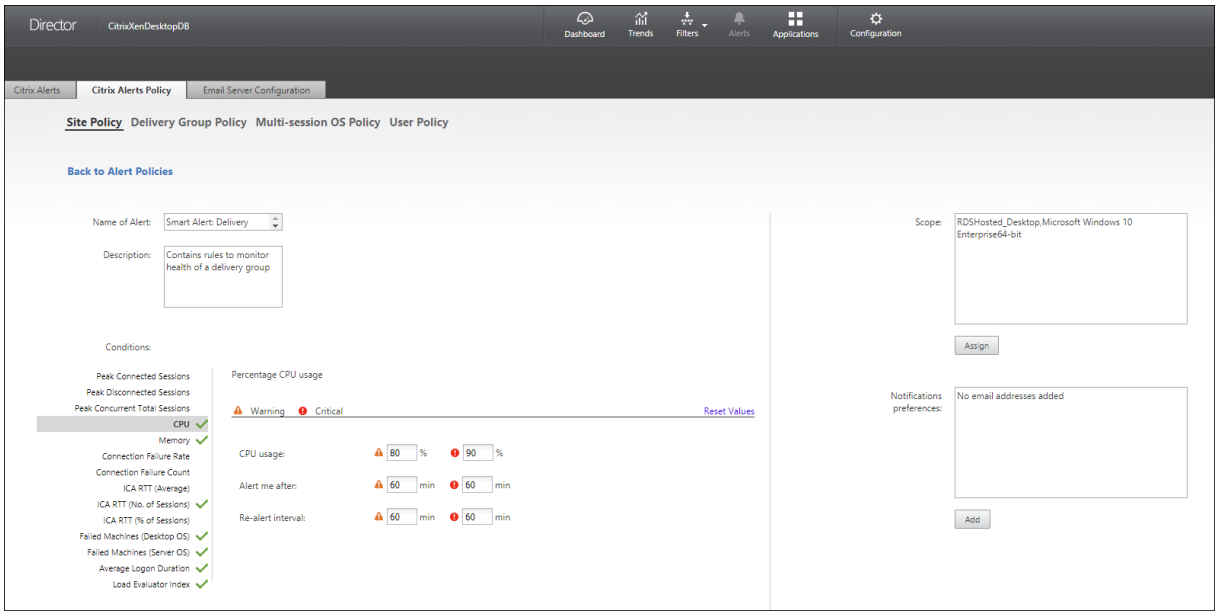
> **Remarque :**
>
> Assurez-vous que votre pare-feu, proxy ou Microsoft Exchange Server ne bloque pas les alertes par e-mail.

### Stratégies d'alertes intelligentes

Un ensemble de stratégies d'alerte intégrées avec des valeurs de seuil prédéfinies est disponible pour les groupes de mise à disposition et les VDA avec OS multi-session. Cette fonctionnalité requiert la version 7.18 ou ultérieure de Delivery Controller. Vous pouvez modifier les paramètres de seuil des stratégies d'alerte intégrées dans **Alertes** > **Stratégie d'alerte Citrix**.
Ces stratégies sont créées lorsqu'au moins une cible d'alerte, un groupe de mise à disposition ou un VDA pour OS multi-session, est définie sur votre site. De plus, ces alertes intégrées sont automatiquement ajoutées à un nouveau groupe de mise à disposition ou à un VDA avec OS multi-session.

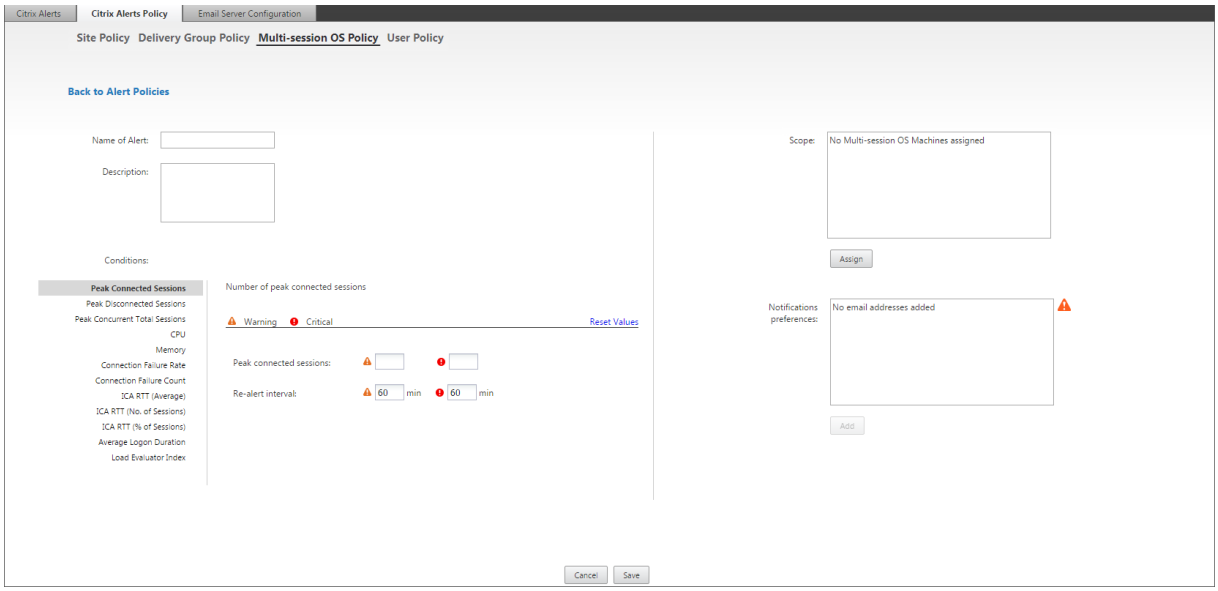
Si vous mettez à niveau votre instance de Director et votre site, les stratégies d'alerte de votre instance Director précédente sont transférées. Les stratégies d'alerte intégrées sont créées uniquement si aucune règle d'alerte correspondante n'existe dans la base de données de surveillance.

Pour les valeurs de seuil des stratégies d'alerte intégrées, consultez la section Conditions de stratégies d'alerte.



## Créer des stratégies d'alerte




Pour créer une stratégie d'alerte, par exemple pour générer une alerte lorsqu'un ensemble spécifique de critères concernant le nombre de sessions est rempli :

1. Accédez à **Alertes** > **Stratégies d'alerte Citrix** et sélectionnez, par exemple, Stratégie d'OS multi-session.
2. Cliquez sur **Créer**.
3. Fournissez un nom et une description pour la stratégie, puis définissez les conditions qui doivent être remplies pour que l'alerte soit déclenchée. Par exemple, spécifiez le nombre d'alertes d'avertissement et d'alertes critiques pour Sessions connectées maximales, Sessions déconnectées maximales et Total des sessions simultanées maximales. La valeur définie pour les alertes d'avertissement ne doit pas être supérieure à la valeur des alertes critiques. Pour de plus amples informations, consultez Conditions des stratégies d'alertes.
4. Définissez le paramètre Intervalle de répétition d'alerte. Si les conditions pour l'alerte sont toujours présentes, l'alerte est de nouveau déclenchée à cet intervalle et, si elle est configurée dans la stratégie, une notification par e-mail est générée. Une alerte ignorée ne génère pas de notification par e-mail à l'intervalle de répétition d'alerte.
5. Définissez l'étendue. Par exemple, sélectionnez un groupe de mise à disposition spécifique.
6. Dans les préférences de notification, spécifiez les personnes qui doivent être notifiées par e-mail lorsque l'alerte est déclenchée. Vous devez spécifier un serveur de messagerie dans l'onglet **Configuration du serveur de messagerie** pour définir les préférences de notification par e-mail dans les stratégies d'alertes.
7. Cliquez sur **Enregistrer**.

La création d'une stratégie comprenant plus de 20 groupes de mise à disposition dans l'étendue peut prendre environ 30 secondes. Un compteur s'affiche durant cette période.

La création de plus de 50 stratégies pour un maximum de 20 groupes de mise à disposition uniques (total de 1 000 cibles au maximum) peut entraîner une réponse plus rapide (environ 5 secondes).

Le déplacement d'une machine contenant des sessions actives d'un groupe de mise à disposition à un autre peut déclencher des alertes de groupe de mise à disposition erronées qui sont définies à l'aide des paramètres de la machine.

> **Remarque :**
> une fois que vous avez supprimé une stratégie d'alerte, l'arrêt des notifications d'alerte générées par cette stratégie peut prendre jusqu'à 30 minutes.

## Conditions de stratégies d'alerte

Vous trouverez ci-dessous les catégories d'alertes, les actions recommandées et les conditions de stratégie intégrée si elles sont définies. Les stratégies d'alerte intégrées sont définies pour des intervalles d'alerte et de répétition d'alerte de 60 minutes.

### Sessions connectées max

- Vérifier la vue Tendances de session dans Director pour les sessions connectées maximales.
- S'assurer qu'il y a suffisamment de capacité pour gérer la charge de session.
- Ajouter des machines si nécessaire

### Sessions déconnectées max

- Vérifier la vue Tendances de session dans Director pour les sessions déconnectées maximales.
- S'assurer qu'il y a suffisamment de capacité pour gérer la charge de session.
- Ajouter des machines si nécessaire.
- Fermer les sessions déconnectées si nécessaire

### Total des sessions simultanées max

- Vérifier la vue Tendances de session dans Director pour les sessions simultanées maximales.
- S'assurer qu'il y a suffisamment de capacité pour gérer la charge de session.
- Ajouter des machines si nécessaire.
- Fermer les sessions déconnectées si nécessaire

#### UC

Le pourcentage d'utilisation UC indique la consommation globale UC sur le VDA, y compris celle des processus. Vous pouvez obtenir plus d'informations sur l'utilisation UC par processus individuels sur la page **Détails de la machine** du VDA correspondant.

- Accédez à **Détails de la machine > Afficher utilisation historique > 10 processus les plus utilisés**, identifiez les processus consommant l'UC. Assurez-vous que la stratégie de surveillance des processus est activée pour lancer la collecte de statistiques d'utilisation des ressources au niveau des processus.
- Arrêter le processus si nécessaire.
- L'arrêt du processus entraîne la perte des données non enregistrées.
- Si tout fonctionne comme prévu, ajouter des ressources d'UC dans le futur.

  > **Remarque :**
  >
  > Le paramètre de stratégie **Activer le suivi des ressources** est autorisé par défaut pour le contrôle des compteurs de performances de l'UC et de la mémoire sur les machines avec des VDA. Si ce paramètre de stratégie est désactivé, les alertes avec conditions d'UC et de mémoire ne seront pas déclenchées. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie Surveillance.

  **Conditions de la stratégie intelligente :**

  - **Étendue :** Groupe de mise à disposition, OS multi-session
  - **Valeurs de seuil :** Avertissement - 80 %Critique - 90 %

#### Memory

Le pourcentage d'utilisation de la mémoire indique la consommation globale de mémoire sur le VDA, y compris celle des processus. Vous pouvez obtenir plus d'informations sur l'utilisation de la mémoire par des processus individuels sur la page **Détails de la machine** du VDA correspondant.

- Accédez à **Détails de la machine > Afficher utilisation historique > 10 processus les plus utilisés**, identifiez les processus consommant de la mémoire. Assurez-vous que la stratégie de surveillance des processus est activée pour lancer la collecte de statistiques d'utilisation des ressources au niveau des processus.
- Arrêter le processus si nécessaire.
- L'arrêt du processus entraîne la perte des données non enregistrées.
- Si tout fonctionne comme prévu, ajouter plus de mémoire dans le futur.

> **Remarque :**
>
> Le paramètre de stratégie **Activer le suivi des ressources** est autorisé par défaut pour le contrôle des compteurs de performances de l'UC et de la mémoire sur les machines avec des VDA. Si ce paramètre de stratégie est désactivé, les alertes avec conditions d'UC et de mémoire ne seront pas déclenchées. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie Surveillance.

**Conditions de la stratégie intelligente :**

- **Étendue :** Groupe de mise à disposition, OS multi-session
- **Valeurs de seuil :** Avertissement - 80 %Critique - 90 %

#### Taux d'échecs de connexion

Pourcentage d'échecs de connexion au cours de la dernière heure.

- Calculé en fonction du nombre total d'échecs de tentatives de connexions.
- Vérifier la vue Tendance des défaillances dans Director pour les événements consignés dans le journal de configuration.
- Déterminer si les applications ou bureaux sont accessibles.

#### Nombre d'échecs de connexion

Nombre d'échecs de connexion au cours de la dernière heure.

- Vérifier la vue Tendance des défaillances dans Director pour les événements consignés dans le journal de configuration.
- Déterminer si les applications ou bureaux sont accessibles.

#### RTT ICA (moyenne)

Durée moyenne de la boucle ICA.

- Vérifier la répartition du RTT ICA dans Citrix ADM pour déterminer la cause. Pour en savoir plus, consultez la documentation Citrix ADM.
- Si Citrix ADM n'est pas disponible, vérifier le RTT ICA et la latence dans la vue Détails utilisateur de Director et déterminer s'il s'agit d'un problème de réseau ou d'un problème avec les applications ou bureaux.

#### RTT ICA (nbre de sessions)

Nombre de sessions qui dépassent la durée seuil de la boucle ICA

- Vérifier dans Citrix ADM le nombre de sessions avec un RTT ICA élevé. Pour en savoir plus, consultez la documentation Citrix ADM.
- Si Citrix ADM n'est pas disponible, collaborer avec l'équipe du réseau pour déterminer la cause.

  **Conditions de la stratégie intelligente :**

  - **Étendue :** Groupe de mise à disposition, OS multi-session
  - **Valeurs de seuil :** Avertissement - 300 ms pour 5 sessions ou plus, Critique - 400 ms pour 10 sessions ou plus

#### RTT ICA (% de sessions)

Pourcentage de sessions qui dépassent la durée moyenne des boucles ICA

- Vérifier dans Citrix ADM le nombre de sessions avec un RTT ICA élevé. Pour en savoir plus, consultez la documentation Citrix ADM.
- Si Citrix ADM n'est pas disponible, collaborer avec l'équipe du réseau pour déterminer la cause.

#### RTT ICA (utilisateur)

Durée de la boucle ICA qui est appliquée aux sessions lancées par l'utilisateur spécifié. L'alerte est déclenchée si le RTT ICA est supérieur à la valeur de seuil dans au moins une session.

#### Machines en panne (OS mono-session)

Nombre de machines défectueuses avec OS mono-session. Les échecs peuvent se produire pour diverses raisons comme indiqué dans les vues Tableau de bord et Filtres de Director.

- Exécuter les diagnostics Citrix Scout pour déterminer la cause.

  **Conditions de la stratégie intelligente :**

  - **Étendue :** Groupe de mise à disposition, OS multi-session
  - **Valeurs de seuil :** Avertissement - 1, Critique - 2

#### Machines en panne (OS multi-session)

Nombre de machines défectueuses avec OS multi-session. Les échecs peuvent se produire pour diverses raisons comme indiqué dans les vues Tableau de bord et Filtres de Director.

- Exécuter les diagnostics Citrix Scout pour déterminer la cause.

  **Conditions de la stratégie intelligente :**

  - **Étendue :** Groupe de mise à disposition, OS multi-session
  - **Valeurs de seuil :** Avertissement - 1, Critique - 2

#### Machines défectueuses (en %)

Pourcentage de machines avec OS mono-session et multi-session défectueuses dans un groupe de mise à disposition, calculé en fonction du nombre de machines défectueuses. Cette condition d'alerte vous permet de configurer des seuils d'alerte sous la forme d'un pourcentage de machines défectueuses dans un groupe de mise à disposition. Le calcul s'effectue toutes les 30 secondes.
Les échecs peuvent se produire pour diverses raisons comme indiqué dans les vues Tableau de bord et Filtres de Director. Exécuter les diagnostics Citrix Scout pour déterminer la cause. Pour de plus amples informations, consultez la section Résoudre les problèmes utilisateur.

#### Durée moyenne

Durée moyenne des ouvertures de session au cours de la dernière heure.

- Vérifier le tableau de bord de Director pour obtenir des mesures à jour sur la durée des ouvertures de session. Les ouvertures de session peuvent prendre plus de temps si un grand nombre d'utilisateurs ouvrent des sessions dans un délai très court.
- Vérifier la ligne de base et le détail des ouvertures de session pour déterminer la cause. Pour en savoir plus, consultez la section Diagnostiquer les problèmes d'ouverture de session utilisateur

  **Conditions de la stratégie intelligente :**

  - **Étendue :** Groupe de mise à disposition, OS multi-session
  - **Valeurs de seuil :** Avertissement - 45 secondes Critique - 60 secondes

#### Durée d'ouverture de session (Utilisateur)

Durée des ouvertures de session au cours de la dernière heure pour l'utilisateur spécifié.

#### Indice de calculateur de charge

Valeur de l'indice de calculateur de charge pour les 5 dernières minutes.

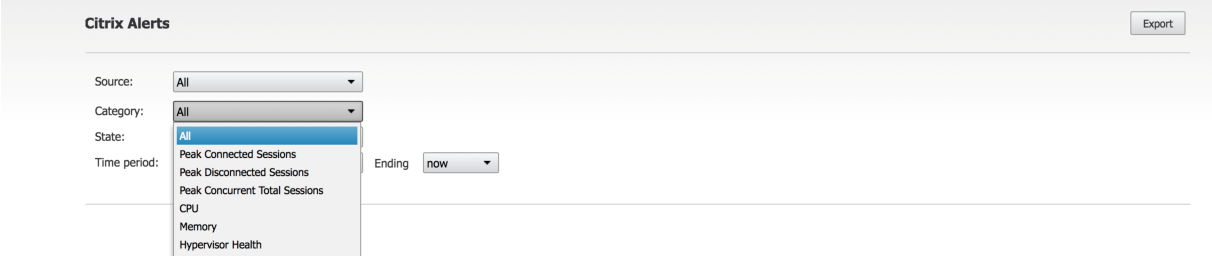
- Vérifier dans Director s'il existe des machines avec OS multi-session connaissant un pic de charge (charge max.). Afficher le tableau de bord (échecs) et le rapport de tendances de l'indice de calculateur de charge.

  **Conditions de la stratégie intelligente :**

  - **Étendue :** Groupe de mise à disposition, OS multi-session
  - **Valeurs de seuil :** Avertissement - 80 %Critique - 90 %

### Surveillance des alertes d'hyperviseur

Director affiche des alertes pour surveiller l'état de l'hyperviseur. Les alertes provenant de XenServer et VMware vSphere aident à surveiller les paramètres et les états de l'hyperviseur. L'état de la connexion à l'hyperviseur est également surveillé pour envoyer une alerte si le cluster ou pool d'hôtes est redémarré ou non disponible.

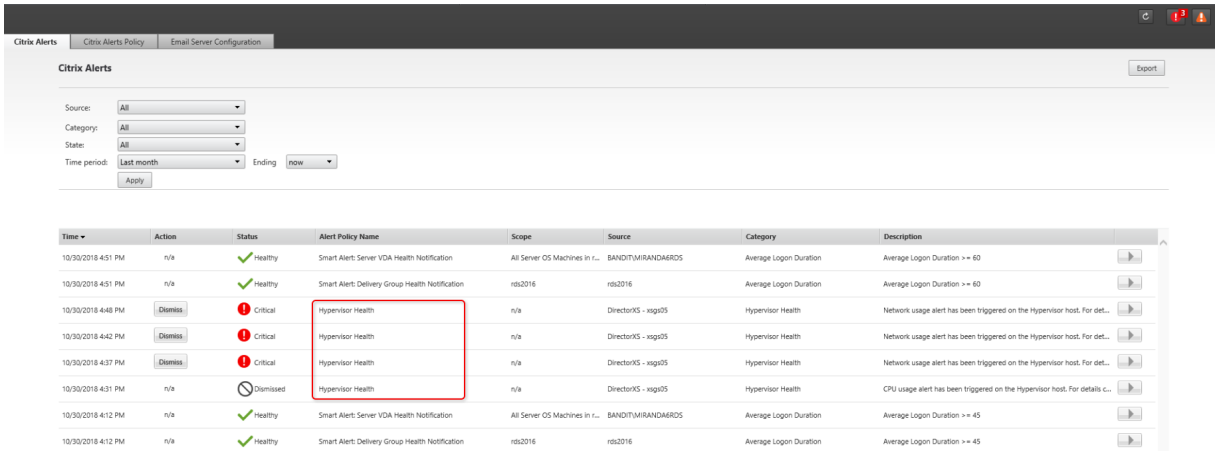



Pour recevoir des alertes d'hyperviseur, assurez-vous qu'une connexion d'hébergement a été créée dans Web Studio. Pour de plus amples informations, consultez les articles Connexions et ressources. Seules ces connexions sont surveillées pour les alertes d'hyperviseur.

Ces alertes sont affichées lorsque les seuils sont atteints ou dépassés. Les alertes d'hyperviseur peuvent être :

- Critique : le seuil critique de la stratégie d'alerte de l'hyperviseur a été atteint ou dépassé.
- Avertissement : le seuil d'avertissement de la stratégie d'alerte de l'hyperviseur a été atteint ou dépassé
- Ignorée : l'alerte n'est plus affichée en tant qu'alerte active




Cette fonctionnalité requiert la version 7 1811 ou ultérieure de Delivery Controller. Si vous utilisez une version plus ancienne de Director avec sites 7 1811 ou version ultérieure, seul le nombre d'alertes d'hyperviseur est affiché. Pour afficher les alertes, vous devez mettre à niveau Director.

Le tableau suivant décrit les différents paramètres et états des alertes d'hyperviseur.

| Alerte | Hyperviseurs pris en charge | Déclenchée par | Condition | Configuration |
|---|---|---|---|---|
| Utilisation du processeur | XenServer, VMware vSphere | Hypervisor | Le seuil d'alerte d'utilisation UC est atteint ou dépassé | Les seuils d'alerte doivent être configurés dans l'hyperviseur. |
| Utilisation de la mémoire | XenServer, VMware vSphere | Hypervisor | Le seuil d'alerte d'utilisation de la mémoire est atteint ou dépassé | Les seuils d'alerte doivent être configurés dans l'hyperviseur. |
| Utilisation du réseau | XenServer, VMware vSphere | Hypervisor | Le seuil d'alerte d'utilisation du réseau est atteint ou dépassé | Les seuils d'alerte doivent être configurés dans l'hyperviseur. |
| Utilisation du disque | VMware vSphere | Hypervisor | Le seuil d'alerte d'utilisation du disque est atteint ou dépassé | Les seuils d'alerte doivent être configurés dans l'hyperviseur. |

| Alerte | Hyperviseurs pris en charge | Déclenchée par | Condition | Configuration |
|---|---|---|---|---|
| État de l'alimentation ou de la connexion de l'hôte | VMware vSphere | Hypervisor | L'hôte de l'hyperviseur a été redémarré ou n'est pas disponible | Les alertes sont prédéfinies dans VMware vSphere. Aucune configuration supplémentaire n'est nécessaire. |
| Connexion d'hyperviseur non disponible | XenServer, VMware vSphere | Delivery Controller | La connexion à l'hyperviseur (pool ou cluster) est perdue, mise hors tension ou redémarrée. Cette alerte est générée toutes les heures tant que la connexion est indisponible. | Les alertes sont prédéfinies avec le Delivery Controller. Aucune configuration supplémentaire n'est nécessaire. |

> **Remarque :**
>
> Pour plus d'informations sur la configuration des alertes, voir Alertes Citrix XenCenter ou consultez la documentation Alertes VMware vCenter.

Les préférences de notification par courrier électronique peuvent être configurées sous **Stratégies d'alerte Citrix > Stratégie de site > Intégrité de l'hyperviseur**. Les conditions de seuil pour les stratégies d'alerte d'hyperviseur peuvent être configurées, modifiées, désactivées ou supprimées depuis l'hyperviseur uniquement et non depuis Director. Toutefois, vous pouvez modifier les préférences de courrier électronique et ignorer une alerte dans Director. Vous pouvez désactiver l'alerte si votre rôle n'implique pas la surveillance de l'infrastructure.

> **Important :**
>
> - Les alertes déclenchées par l'hyperviseur sont récupérées et affichées dans Director. Toutefois, les changements apportés dans le cycle de vie/l'état des alertes de l'hyperviseur ne sont pas reflétés dans Director.
> - Les alertes qui sont intègres, rejetées ou désactivées dans la console de l'hyperviseur continuent à apparaître dans Director et doivent être rejetées explicitement.

> - Les alertes rejetées dans Director ne sont pas rejetées automatiquement dans la console de l'hyperviseur.

## Filtrer les données pour résoudre les échecs

June 27, 2024

Lorsque vous cliquez sur des nombres sur le tableau de bord ou que vous sélectionnez un filtre pré défini depuis le menu Filtres, la vue Filtres s'ouvre pour afficher les données basées sur la machine sélectionnée ou le type d'échec.

Les filtres prédéfinis ne peuvent être modifiés, mais vous pouvez enregistrer un filtre pré défini en tant que filtre personnalisé puis le modifier. De plus, vous pouvez créer des vues de filtres personnalisés de machines, de connexions, de sessions et d'instances d'applications sur tous les groupes de mise à disposition.

1. Sélectionner une vue :

   - **Machines**. Sélectionnez Machines avec OS mono-session ou Machines avec OS multi-session. Ces vues illustrent le nombre de machines configurées. L'onglet Machines avec OS multi-session comprend également l'index de calculateur de charge, qui indique la distribution des compteurs de performances et les info-bulles du nombre de sessions si vous survolez le lien avec la souris.
   - **Sessions**. Vous pouvez également afficher le nombre de sessions depuis la vue Sessions. Utilisez les mesures de délai d'inactivité pour identifier les sessions qui restent inactives au-delà d'une période de temps donnée. Cliquez sur l'**utilisateur associé** pour ouvrir le gestionnaire d'activités de cet utilisateur. Cliquez sur le nom du **point de terminaison** pour ouvrir le gestionnaire d'activités du point de terminaison. Cliquez sur **Afficher les détails** pour ouvrir la page **Détails de l'utilisateur** ou **Détails du point de terminaison**, respectivement. Pour plus d'informations, consultez la section Détails de l'utilisateur.
   - **Connexions**. Filtrez les connexions par différentes périodes de temps, y compris les 60 dernières minutes, les dernières 24 heures ou les derniers 7 jours.
   - **Instances d'application**. Cette vue affiche les propriétés de toutes les instances d'application sur les VDA d'OS de serveur et mono-session. Les mesures de délai d'inactivité de session sont disponibles pour les instances d'application sur les VDA d'OS multi-session.

   > **Remarque :**
   >
   > Si vous avez lancé des sessions de bureau sur des VDA installés sur un ordinateur Windows 10 1809, le Gestionnaire d'activités de Director peut parfois afficher Microsoft Edge et Office

> comme des applications en cours d'exécution alors qu'elles ne s'exécutent réellement qu'en arrière-plan.

2. Pour **Filtrer par**, sélectionnez le critère.
3. Utilisez les onglets supplémentaires pour chaque vue, selon vos besoins, pour terminer le filtre.
4. Sélectionnez des colonnes supplémentaires, selon vos besoins, pour résoudre plus de problèmes.
5. Enregistrez votre filtre et attribuez-lui un nom.
6. Pour accéder aux filtres de plusieurs serveurs Director, stockez les filtres sur un dossier partagé accessible à partir de ces serveurs :
   - Le dossier partagé doit avoir des autorisations Modifier pour les comptes sur le serveur Director.
   - Les serveurs Director doivent être configurés pour accéder au dossier partagé. Pour configurer, exécutez le **Gestionnaire des services Internet (IIS)**. Dans **Sites > Site Web par défaut > Director> Paramètres de l'application**, modifiez le paramètre **Service.UserSettingsPath** pour qu'il reflète le chemin d'accès UNC du dossier partagé.
7. Pour ouvrir le filtre plus tard, depuis le menu **Filtres**, sélectionnez le type de filtre (Machines, Sessions, Connexions ou Instances d'application), puis sélectionnez le filtre enregistré.
8. Cliquez sur **Exporter** pour exporter les données vers des fichiers au format CSV. Des données pouvant atteindre 100 000 enregistrements peuvent être exportées. Cette fonctionnalité est disponible sur Delivery Controller version 1808 ou ultérieure.
9. Si nécessaire, pour les vues **Machines** ou **Connexions**, utilisez les commandes de puissance pour toutes les machines que vous sélectionnez dans la liste filtrée. Pour la vue Sessions, utilisez les commandes ou l'option de session pour envoyer des messages.
10. Dans les vues **Machines** et **Connexions**, cliquez sur **Raison de l'échec** pour une machine ou une connexion en échec afin d'obtenir une description détaillée de l'échec et des actions recommandées pour résoudre le problème. Les raisons de l'échec et les actions recommandées pour des défaillances de machines et de connexion sont disponibles sur la page Dépannage et raison des échecs de Citrix Director.
11. Dans la vue **Machines**, cliquez sur le lien du nom d'une machine pour accéder à la page **Détails de la machine** correspondante. Cette page affiche les détails de la machine, fournit des contrôles de l'alimentation, et affiche les graphiques liés au processeur, à la mémoire, à la surveillance des disques et à la surveillance des GPU. Cliquez aussi sur **Afficher utilisation historique** pour afficher les tendances d'utilisation des ressources pour la machine. Pour obtenir davantage d'informations, veuillez consulter la section Dépanner les machines.

12. Dans la vue **Instances d'application**, triez ou filtrez en fonction d'un **temps d'inactivité** supérieur à une période de temps donnée. Sélectionnez les instances d'application inactives à fermer. La fin de session ou la déconnexion d'une instance d'application met fin à toutes les instances de l'application actives dans la même session. Pour obtenir davantage d'informations, veuillez consulter la section Résolution des problèmes d'applications. La page de filtre des instances d'application et les mesures de délai d'inactivité dans les pages de filtre des sessions sont disponibles si Director, les Delivery Controller et les VDA sont à la version 7.13 ou ultérieure.

> **Remarque :**
> Web Studio permet l'attribution de plusieurs règles d'attribution de bureau (DAR) pour différents utilisateurs ou groupes d'utilisateurs à un seul VDA du groupe de mise à disposition. StoreFront affiche le bureau attribué avec le nom d'affichage correspondant selon le DAR de l'utilisateur connecté. Toutefois, Director ne prend pas en charge les fichiers DAR et affiche le bureau attribué à l'aide du nom de groupe de mise à disposition indépendamment de l'utilisateur connecté. Par conséquent, vous ne pouvez pas mapper un bureau spécifique à une machine dans Director. Pour mapper le bureau attribué affiché dans StoreFront au nom du groupe de mise à disposition affiché dans Director, utilisez la commande PowerShell suivante :

```
Get-BrokerDesktopGroup | Where-Object {
  $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

## Contrôler les tendances historiques sur un site

June 27, 2024

La vue Tendances accède aux informations sur les tendances historiques de chaque site pour les paramètres suivants :

- les sessions
- échecs de connexion
- défaillances de machines
- performances d'ouverture de session
- calcul de charge
- gestion de la capacité
- utilisation de machine
- utilisation des ressources

- analyse du réseau pour chaque site

Pour trouver ces informations, cliquez sur le menu **Tendances**.

Cette fonctionnalité d'exploration vous permet de naviguer au travers des diagrammes de tendances en effectuant un zoom avant sur une période de temps (en cliquant sur un point de données dans le diagramme) et en effectuant un éclatement pour afficher les détails associés avec la tendance. Elle vous permet de mieux comprendre les détails des personnes ou éléments affecté(e)s.

Pour modifier l'étendue par défaut de chaque graphique, appliquez un filtre différent aux données.

Choisissez une période pour laquelle vous avez besoin des informations de tendance historique. La disponibilité de la période dépend de votre déploiement de Director comme suit :

- des rapports de tendance pour l'année écoulée (365 jours) sont disponibles sur les sites sous licence Premium ;
- des rapports de tendance pour le mois écoulé (31 jours) sont disponibles sur les sites sous licence Advanced ;
- des rapports de tendance pour la semaine écoulée (7 jours) sont disponibles sur les sites sans licence Premium et Advanced.

> **Remarque :**
>
> - Dans tous les déploiements de Director, les informations de tendances Sessions, Échecs et Performances d'ouverture de session sont présentées sous forme de graphiques et de tableaux lorsque la période de temps est définie sur Mois dernier (**se terminant maintenant**) ou une période plus courte. Lorsque la période de temps est définie sur Mois dernier avec une date de fin personnalisée ou Année dernière, les informations de tendance sont disponibles sous forme de graphiques et non de tableaux.
> - Les valeurs de rétention de nettoyage de Monitor Service contrôlent la disponibilité des données de tendance. Les valeurs par défaut sont disponibles dans la section Granularité de données et rétention. Les clients sur sites avec licence Premium peuvent modifier la rétention de nettoyage sur leur nombre de jours de rétention désirés.
> - Dans le Gestionnaire des services Internet, les paramètres suivants contrôlent la plage de dates de fin personnalisées disponibles pour la sélection. Toutefois, la disponibilité des données pour les dates sélectionnées dépend du paramètre de rétention de nettoyage pour la mesure spécifique mesurée.

| Paramètre | Valeurs par défaut |
|---|---|
| UI.TrendsLast2HoursRange | 3 |
| UI.TrendsLast24HoursRange | 32 |

| Paramètre | Valeurs par défaut |
| --- | --- |
| UI.TrendsLast7DaysRange | 32 |
| UI.TrendsLastMonthRange | 365 |

### Tendances disponibles

**Afficher les tendances des sessions :** dans l'onglet **Sessions**, sélectionnez le groupe de mise à disposition et la période pour afficher des informations plus détaillées sur le nombre de sessions simultanées.

La colonne **Nombre de reconnexions automatiques de sessions** affiche le nombre de reconnexions automatiques dans une session. La reconnexion automatique est activée lorsque les stratégies Fiabilité de session ou Reconnexion automatique du client sont en vigueur. En cas d'interruption du réseau sur le point de terminaison, les stratégies suivantes entrent en vigueur :

- Fiabilité de session, (par défaut pendant 3 minutes) lorsque l'application Citrix Receiver ou Citrix Workspace tente de se connecter au VDA.
- Reconnexion automatique des clients, pendant 3 à 5 minutes lorsque le client tente de se connecter au VDA.

Ces deux reconnexions sont capturées et présentées à l'utilisateur. Ces informations peuvent prendre un maximum de 5 minutes pour apparaître sur l'interface utilisateur de Director après la reconnexion.

Les informations de reconnexion automatique vous aident à consulter et résoudre les problèmes de connexion réseau présentant des interruptions. Elles analysent également les réseaux qui ne font l'objet d'aucune interruption. Vous pouvez afficher le nombre de reconnexions pour un groupe de mise à disposition spécifique ou une période sélectionnée dans les filtres. L'affichage des détails fournit des informations supplémentaires telles que Fiabilité de session ou Reconnexion automatique des clients, les horodatages, l'adresse IP du point de terminaison et le nom du point de terminaison de la machine sur laquelle l'application Workspace est installée.

Par défaut, les journaux sont triés par horodatage des événements dans l'ordre décroissant. Cette fonctionnalité est disponible pour l'application Citrix Workspace pour Windows, l'application Citrix Workspace pour Mac, Citrix Receiver pour Windows et Citrix Receiver pour Mac. Cette fonctionnalité requiert la version 7 1906 ou ultérieure de Delivery Controller et la version 1906 ou ultérieure de VDA.

Pour plus d'informations sur les reconnexions de session, consultez la section Sessions.

Pour obtenir des informations supplémentaires sur les stratégies, reportez-vous à Paramètres de stratégie Reconnexion automatique des clients et Paramètres de stratégie Fiabilité de session.

Parfois, les données de reconnexion automatique peuvent ne pas apparaître dans Director pour les raisons suivantes :

- L'application Workspace n'envoie pas de données de reconnexion automatique au VDA.
- Le VDA n'envoie pas de données au service de surveillance.
- Les charges utiles VDA sont rejetées par les Delivery Controller car elles n'ont peut-être pas les sessions correspondantes.

> **Remarque :**
>
> Parfois, l'adresse IP du client peut ne pas être obtenue correctement si certaines stratégies Citrix Gateway sont définies.

**Afficher les tendances pour les échecs de connexion :** depuis l'onglet Échecs, sélectionnez la connexion, le type de machine, le type d'échec, le groupe de mise à disposition et la période de temps pour afficher un graphique contenant des informations plus détaillées sur les échecs de connexion utilisateur sur votre site.

**Afficher les tendances des échecs de machine :** depuis l'onglet **Échecs d'OS mono-session** ou Machines avec OS multi-session, sélectionnez le type de défaillance, le groupe de mise à disposition et la période de temps pour afficher un graphique contenant des informations plus détaillées sur les échecs de machine sur votre site.

**Afficher les tendances pour les performances d'ouverture de session :** dans l'onglet **Performances d'ouverture de session**, sélectionnez le groupe de mise à disposition et la période de temps pour afficher un graphique contenant des informations plus détaillées sur la durée d'ouverture de session de l'utilisateur sur votre site et si le nombre d'ouvertures de session affecte les performances. Cette vue affiche également la durée moyenne des phases d'ouverture de session, telles que la durée de la négociation et la durée de démarrage de la machine virtuelle.
Ces données sont spécifiques aux ouvertures de session des utilisateurs et ne comprennent pas les utilisateurs essayant de se reconnecter à des sessions déconnectées.
Le tableau en dessous du diagramme affiche la Durée de connexion par session utilisateur. Vous pouvez choisir les colonnes à afficher et trier le rapport en fonction de n'importe colonne.
Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.

**Afficher les tendances de charge évaluées :** dans l'onglet **Index du calculateur de charge**, affichez un graphique contenant des informations plus détaillées sur la charge distribuée entre les machines avec OS multi-session. Les options de filtre de ce graphique incluent le groupe de mise à disposition ou la machine avec OS multi-session dans un groupe de mise à disposition, la machine avec OS multi-session (disponible uniquement si la machine avec OS multi-session d'un groupe de mise à disposition a été sélectionnée), et la plage.

**Afficher l'utilisation des applications hébergées :** la disponibilité de cette fonctionnalité dépend

de la licence de votre organisation.
Dans l'onglet **Gestion de la capacité**, sélectionnez l'onglet **Utilisation d'applications hébergées**. Sélectionnez le groupe de mise à disposition et la période de temps pour afficher un graphique affichant la période d'utilisation simultanée maximale et une table affichant l'utilisation de l'application. À partir de la table affichant l'utilisation de l'application, vous pouvez choisir une application spécifique pour voir les détails et une liste des utilisateurs qui utilisent, ou ont utilisé l'application.

**Afficher l'utilisation des OS mono-session et multi-session :** la vue Tendances affiche l'utilisation des OS mono-session par site et par groupe de mise à disposition. Lorsque vous sélectionnez **Site**, l'utilisation est affichée par groupe de mise à disposition. Lorsque vous sélectionnez Groupe de mise à disposition, l'utilisation est indiquée par utilisateur.
La vue Tendances affiche également l'utilisation des OS multi-session par site, par groupe de mise à disposition et par machine. Lorsque vous sélectionnez **Site**, l'utilisation est affichée par groupe de mise à disposition. Lorsque vous sélectionnez Groupe de mise à disposition, l'utilisation est indiquée par machine et par utilisateur. Lorsque vous sélectionnez Machine, l'utilisation est indiquée par utilisateur.

**Afficher l'utilisation de machine virtuelle :** à partir de l'onglet **Utilisation de machine**, sélectionnez **Machines avec OS mono-session ou Machines avec OS multi-session** pour obtenir une vue en temps réel de votre utilisation des machines virtuelles, ce qui vous permet d'évaluer rapidement les besoins en capacité de votre site.
Disponibilité d'OS mono-session : affiche l'état actuel des machines avec OS mono-session (VDI) par disponibilité pour la totalité du site ou un groupe de mise à disposition spécifique.
Disponibilité d'OS multi-session : affiche l'état actuel des machines avec OS multi-session par disponibilité pour la totalité du site ou un groupe de mise à disposition spécifique.

> **Remarque :**
> Le nombre de machines affichées dans le compteur Disponible inclut les machines en mode de maintenance.

**Afficher l'utilisation des ressources :** à partir de l'onglet **Utilisation des ressources**, sélectionnez **Machines avec OS mono-session ou Machines avec OS multi-session** pour afficher les tendances historiques d'utilisation d'UC et de mémoire et les données E/S par seconde et latence de disque pour chaque machine VDI afin de mieux planifier les capacités.
Cette fonctionnalité requiert la **version 7.11** ou ultérieure de Delivery Controller et de VDA.
Les graphiques affichent des données d'UC moyenne, de mémoire moyenne, de nombre moyen d'E/S par seconde, de latence de disque et de sessions simultanées maximales. Vous pouvez accéder aux détails de la machine et afficher des données et des graphiques pour les 10 processus consommant le plus d'UC.

Filtrez par groupe de mise à disposition et période. Les graphiques pour CPU, utilisation de la mémoire et sessions simultanées maximum sont disponibles pour les 2 dernières heures, les dernières

24 heures, les 7 derniers jours, le dernier mois et la dernière année. Les graphiques de nombre moyen d'E/S par seconde et de latence de disque sont disponibles pour les dernières 24 heures, le dernier mois et la dernière année.

> **Remarque :**
>
> - Le paramètre de stratégie Surveillance, **Activer le suivi des processus**, doit être défini sur **Autorisé** pour collecter et afficher les données dans le tableau des 10 processus les plus utilisés sur la page Utilisation historique des machines. Par défaut, la stratégie est définie sur **Interdite**. Toutes les données d'utilisation des ressources sont collectées par défaut. Cela peut être désactivé à l'aide du paramètre de stratégie **Activer le suivi des ressources**. Le tableau sous les graphiques affiche les données d'utilisation des ressources par machine. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie Surveillance.
> - Nbre moyen d'E/S par seconde indique les moyennes quotidiennes. E/S par seconde max. est calculé comme la moyenne la plus élevée d'E/S pour la période sélectionnée. (Le nombre moyen d'E/S par seconde est la moyenne d'E/S par seconde collectée au cours de l'heure sur le VDA).
> - L'analyse détaillée de la machine répertorie les processus pour lesquels l'utilisation moyenne du processeur ou de la mémoire est supérieure à 1 %, ce qui peut signifier que parfois moins de 10 processus sont répertoriés.

**Afficher les données d'analyse du réseau :** la disponibilité de cette fonctionnalité dépend de la licence de votre organisation et vos permissions d'administrateur. Cette fonctionnalité requiert la **version 7.11** ou ultérieure de Delivery Controller.

Dans l'onglet **Réseau**, surveillez votre analyse réseau, qui fournit une vue contextuelle utilisateur, application et bureau du réseau. Grâce à cette fonctionnalité, Director fournit des analyses avancées du trafic ICA dans votre déploiement via les rapports HDX Insight de Citrix ADM. Pour de plus amples informations, consultez la section Configurer l'analyse réseau.

**Afficher les échecs applicatifs :** l'onglet **Échecs applicatifs** affiche les échecs associés aux applications publiées sur les VDA.

Cette fonctionnalité requiert la **version 7.15** ou ultérieure de Delivery Controller et de VDA. Les VDA avec OS mono-session exécutant Windows Vista ou version ultérieure, et les VDA avec OS multi-session exécutant Windows Server 2008 et versions ultérieures sont pris en charge.
Pour plus d'informations, consultez la section Détection des défaillances applicatives.

Par défaut, seuls les échecs applicatifs de VDA avec OS multi-session sont détectés. Vous pouvez configurer la détection des échecs applicatifs à l'aide de stratégies de surveillance. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie Surveillance.

**Afficher les résultats de l'analyse** : l'onglet **Résultats de l'analyse** affiche les résultats de l'analyse

pour les applications et bureaux configurés pour l'analyse dans la page Configuration. Ici, l'étape de lancement au cours de laquelle l'échec s'est produit est enregistrée.

Pour plus d'informations, consultez Analyse d'applications et de bureaux.

**Créer des rapports personnalisés :** l'onglet Rapports personnalisés offre une interface utilisateur pour générer des rapports personnalisés contenant des données en temps réel et des données historiques provenant de la base de données de surveillance sous forme de tableau.

Cette fonctionnalité requiert la **version 7.12** ou ultérieure de Delivery Controller.

À partir de la liste des requêtes de rapport personnalisé enregistrées précédemment, vous pouvez cliquer sur **Exécuter et télécharger** pour exporter le rapport au format CSV, cliquer sur **Copier OData** pour copier et partager la requête OData correspondante, ou cliquer sur **Modifier** pour modifier la requête.
Vous pouvez créer une requête de rapport personnalisé basée sur les machines, les connexions, les sessions, ou les instances d'application. Spécifiez les conditions de filtrage à l'aide de champs tels que la machine, le groupe de mise à disposition ou la période de temps. Spécifiez les colonnes supplémentaires requises dans votre rapport personnalisé. L'aperçu affiche un exemple des données du rapport. L'enregistrement de la requête de rapport personnalisé l'ajoute à la liste des requêtes enregistrées.

Vous pouvez créer un rapport personnalisé basé sur une requête OData copiée. Pour ce faire, sélectionnez l'option Requête OData et collez la requête OData copiée. Vous pouvez enregistrer la requête résultante pour l'exécuter ultérieurement.

> **Remarque :**
> Les noms de colonne dans les rapports Aperçu et Exporter générés à l'aide de requêtes OData ne sont pas localisés, mais s'affichent en anglais.

Les icônes de drapeaux sur le graphique indiquent des actions ou événements significatifs pour cette période spécifique. Placez le pointeur sur un drapeau et cliquez pour obtenir la liste des événements ou actions.

> **Remarque :**
>
> - les données d'ouverture de session de la connexion HDX ne sont pas collectées pour les VDA antérieurs à la version 7. Pour les VDA antérieurs, les données du graphique sont affichées en tant que 0.
> - Les groupes de mise à disposition supprimés dans Citrix Studio sont disponibles pour sélection dans les filtres de tendances Director jusqu'à ce que les données y afférent soient nettoyées. La sélection d'un groupe de mise à disposition supprimé affiche des graphiques pour les données disponibles entrant dans le cadre de la période de rétention des données. Toutefois, les tableaux n'affichent aucune donnée.

> - Si vous déplacez une machine contenant des sessions actives d'un groupe de mise à disposition à un autre, les tableaux **Utilisation des ressources et Indice de calculateur de charge** du nouveau groupe de mise à disposition affichent les mesures consolidées des anciens et des nouveaux groupes de mise à disposition.

## Surveiller les machines gérées par Autoscale

June 27, 2024

Autoscale est une fonction de gestion de l'alimentation qui permet une gestion proactive de l'alimentation de toutes les machines avec OS multi-session et mono-session enregistrées dans un groupe de mise à disposition. Vous pouvez configurer Autoscale pour un groupe de mise à disposition sélectionné dans Web Studio. Pour plus d'informations, consultez la section Autoscale.
Vous pouvez surveiller les indicateurs clés des machines compatibles avec Autoscale à l'aide de Director.

### Utilisation des machines

La page **Utilisation des machines** affiche le nombre de machines avec OS multi-session et mono-session gérées par Autoscale qui sont mises sous tension pour un groupe de mise à disposition et une période sélectionnés. Cet indicateur montre l'utilisation réelle des machines dans le groupe de mise à disposition.
Dans l'onglet **Machines avec OS à session unique** ou **Machines avec OS multi-session**, sélectionnez le groupe de mise à disposition et la période.

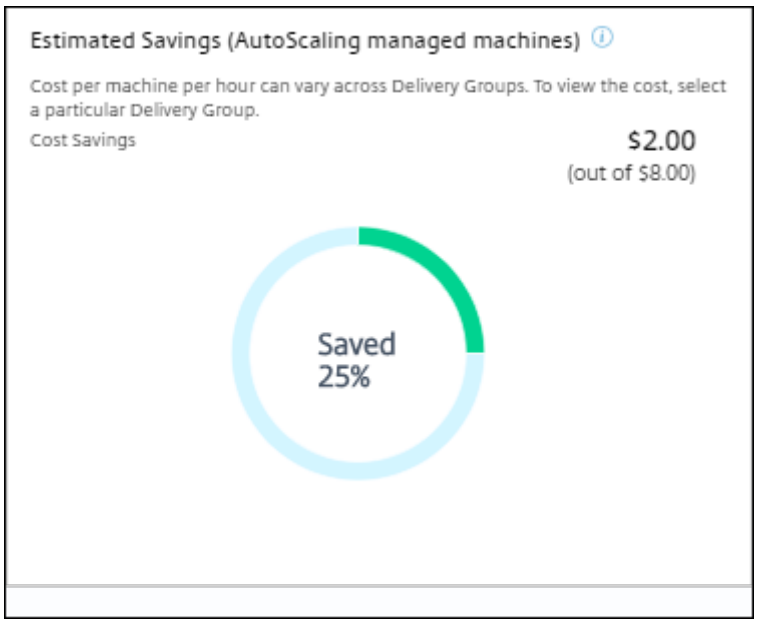
Le graphique représente les indicateurs suivants :

- **Machines actives** : nombre de machines gérées par Autoscale qui sont sous tension
- **Machines enregistrées** : nombre de machines avec OS multi-session ou mono-session enregistrées
- **Machines en maintenance** : nombre de machines avec OS multi-session ou mono-session avec le mode de maintenance activé

### Estimation des économies

La page **Utilisation des machines** affiche également les économies de coûts estimées réalisées en activant Autoscale dans le groupe de mise à disposition sélectionné.




Les économies estimées sont calculées sous forme de pourcentage d'économies par machine et par heure (en dollars US) tel que configuré dans **Modifier le groupe de mise à disposition** > **Autoscale**. Pour plus d'informations sur la configuration des économies par machine, reportez-vous à la section Autoscale.

Lorsque vous sélectionnez tous les groupes de mise à disposition, la valeur moyenne des économies estimées pour tous les groupes de mise à disposition s'affiche.

Les économies estimées aident les administrateurs à consolider l'infrastructure existante et à planifier la capacité pour obtenir des économies et une utilisation maximales.

### Notifications d'alerte pour les machines et les sessions

Le tableau de bord de l'onglet Director affiche des notifications d'alerte qui peuvent être affichées de manière plus détaillée. Les détails des alertes sont affichés sur la page **Alertes**.

- Pour créer une stratégie d'alerte dans un groupe de mise à disposition, accédez à **Alertes** > **Stratégie d'alertes Citrix** > **Stratégie de groupe de mise à disposition**.
- Ici, vous pouvez définir les seuils d'avertissement et critique suivants :
  - Machines en panne (OS mono-session) et machines en panne (OS multi-session)
  - Sessions connectées maximales, Sessions déconnectées maximales et Total des sessions simultanées maximales dans le groupe de mise à disposition
- Des alertes sont générées lorsque l'indicateur correspondant dans le groupe de mise à disposition atteint le seuil défini.

Pour plus d'informations sur les conditions de la stratégie d'alerte et la création de nouvelles stratégies d'alerte, reportez-vous à la section Alertes et notifications.

### État de machine

- Sur la page **Filtres** > **Machines**, vous pouvez afficher l'état d'alimentation de toutes les machines dans un format tabulaire. Vous pouvez filtrer par groupe de mise à disposition spécifique.
- Sur la page **Filtres** > **Sessions**, vous pouvez afficher un filtre par nom de machine pour voir les sessions associées et leur état en temps réel.
- Sur la page **Tendances** > **Sessions**, sélectionnez votre groupe de mise à disposition et votre période pour afficher la tendance des sessions et leurs indicateurs associés.

Pour plus d'informations, consultez la section Filtrer les données pour résoudre les échecs.

### Tendances du calculateur de charge

Sur la page **Tendances** > **Indice de calculateur de charge**, vous pouvez afficher un graphique contenant des informations détaillées sur la charge distribuée entre les machines avec OS multi-session. Les options de filtre de ce graphique incluent le groupe de mise à disposition ou la machine avec OS multi-session dans un groupe de mise à disposition, la machine avec OS multi-session (disponible uniquement si la machine avec OS multi-session d'un groupe de mise à disposition a été sélectionnée), et la plage. L'indice de calculateur de charge est affiché sous forme de pourcentages d'utilisation totale du processeur, de la mémoire, du disque ou des sessions et comparé avec le nombre d'utilisateurs connectés dans le dernier intervalle.

## Dépanner les déploiements

June 27, 2024

En tant qu'administrateur de service d'assistance, vous pouvez rechercher l'utilisateur qui signale un problème et afficher les détails des sessions ou des applications associées à cet utilisateur. De même, vous pouvez rechercher des machines ou des points de terminaison sur lesquels des problèmes sont signalés. Les problèmes peuvent être résolus rapidement en surveillant les indicateurs de mesure pertinents et en effectuant les actions appropriées.

Les actions disponibles sont les suivantes :

- Mettre fin à une demande ou à un processus qui ne répond pas

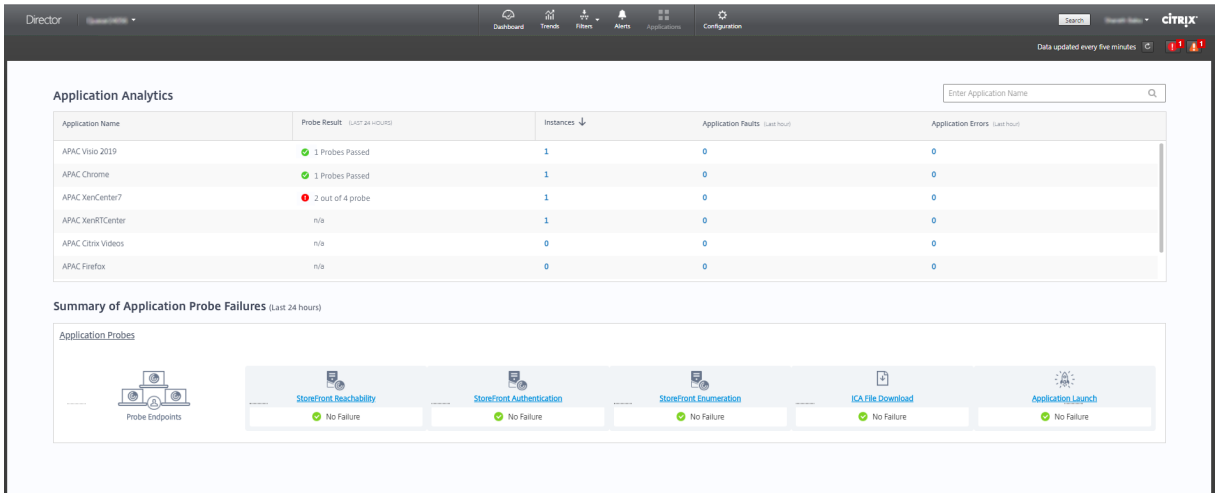
- Opérations d'observation sur la machine de l'utilisateur
- Déconnexion d'une session qui ne répond pas
- Redémarrage de la machine
- Placement de la machine en mode de maintenance
- Réinitialisation du profil utilisateur

# Résolution des problèmes d'applications

June 27, 2024

## Analyse des applications

La vue **Applications** affiche des analyses basées sur les applications dans une vue consolidée unique pour faciliter l'analyse et la gestion efficaces des performances des applications. Vous pouvez obtenir des informations précieuses sur l'intégrité et l'utilisation de toutes les applications publiées sur le site. La vue par défaut permet d'identifier les applications les plus utilisées.
Cette fonctionnalité requiert la version 7.16 ou ultérieure de Delivery Controller et la version 7.15 ou ultérieure de VDA.




La colonne **Résultat de l'analyse** affiche le résultat de l'analyse d'application exécutée au cours des dernières 24 heures. Cliquez sur le lien du résultat de l'analyse pour voir plus de détails dans la page **Tendances** > **Résultats de l'analyse d'application**. Pour plus de détails sur la configuration des analyses d'application, voir Analyse d'applications et de bureaux.

La colonne **Instances** affiche l'utilisation des applications. Elle indique le nombre d'instances d'application en cours d'exécution (instances connectées et déconnectées). Pour résoudre des problèmes,

cliquez sur le champ **Instances** pour afficher la page de filtres **Instances d'application**. Dans cette page, vous pouvez sélectionner les instances d'application à fermer ou à déconnecter.

> **Remarque :**
>
> Pour les administrateurs avec une étendue personnalisée, Director n'affiche pas les instances d'application créées sous Groupes d'applications. Pour afficher toutes les instances d'application, vous devez être un administrateur complet. Pour plus d'informations, consultez l'article CTX256001 du centre de connaissances.

Contrôlez l'intégrité des applications publiées dans votre site avec les colonnes **Défaillances applicatives** et **Erreurs applicatives**. Ces colonnes affichent le nombre cumulé de défaillances et d'erreurs survenues lors du lancement de l'application correspondante au cours de la dernière heure. Cliquez sur le champ **Défaillances applicatives** ou **Erreurs applicatives** pour afficher les détails de l'échec sur la page **Tendances** > **Défaillances applicatives** correspondant à l'application sélectionnée.

Les paramètres de stratégie d'échec de l'application régissent la disponibilité et l'affichage des défaillances et des erreurs. Pour de plus amples informations sur les stratégies et comment les modifier, consultez la section Stratégies pour la détection des défaillances applicatives dans les paramètres de **stratégie Surveillance**.

### Surveillance des applications en temps réel

Vous pouvez résoudre les problèmes d'applications et de sessions à l'aide de la mesure de délai d'inactivité pour identifier les instances qui restent inactives au-delà d'une durée spécifique.

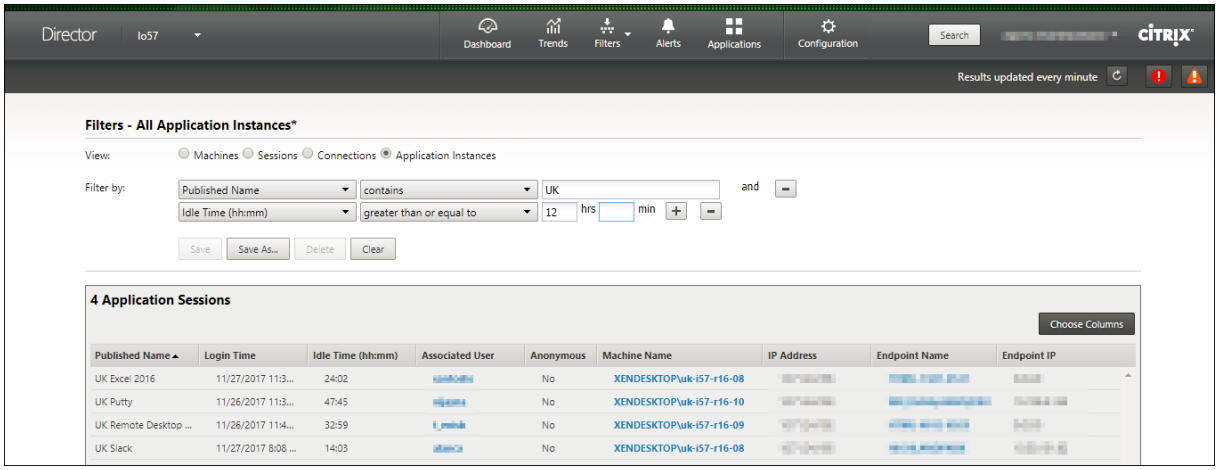
Le secteur de la santé, dans lequel les employés partagent les licences d'application, représente un cas d'utilisation typique pour la résolution de problèmes d'applications. En effet, vous devez mettre fin aux instances d'applications et aux sessions inactives pour purger l'environnement Citrix Virtual Apps and Desktops, pour reconfigurer les serveurs avec problèmes de performances, ou pour gérer et mettre à niveau les applications.

La page de filtre **Instances d'application** répertorie toutes les instances d'application sur les VDA d'OS de serveur et mono-session. Les mesures de délai d'inactivité associées sont affichées pour les instances d'application sur VDA d'OS multi-session qui sont inactives depuis au moins 10 minutes.

> **Remarque :**
> Les mesures Instances d'application sont disponibles sur les sites de toutes les éditions de licence.

Utilisez ces informations pour identifier les instances d'application qui restent inactives au-delà d'une période de temps spécifique et mettez fin à la session ou déconnectez-les en fonction des besoins. Pour ce faire, sélectionnez **Filtres > Instances d'application** et sélectionnez un filtre pré-enregistré ou choisissez **Toutes les instances d'application** et créez votre propre filtre.

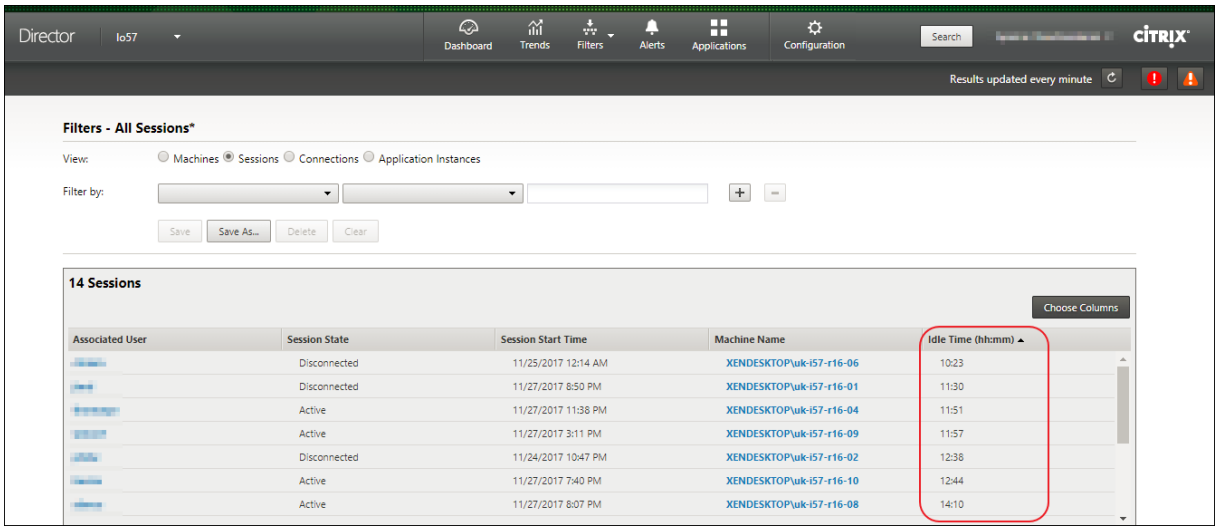
 




Voici un exemple de filtre. Comme critère **Filtrer par**, choisissez **Nom publié** (de l'application) et **Durée d'inactivité**. Définissez ensuite la **durée d'inactivité** sur **supérieur ou égal à** un délai spécifique et enregistrez le filtre pour une éventuelle réutilisation. Dans la liste filtrée, sélectionnez les instances d'application. Sélectionnez l'option pour envoyer des messages ou à partir du menu déroulant **Contrôle de la session**, choisissez **Fermer la session** ou **Déconnecter** pour mettre fin aux instances.

> **Remarque :**
> La fermeture de session ou la déconnexion d'une instance d'application ferme ou déconnecte la session en cours, ce qui entraîne l'arrêt de toutes les instances d'application qui appartiennent à la même session.

Vous pouvez identifier les sessions inactives dans la page de filtre **Sessions** à l'aide des informations d'état de session et de mesure de durée d'inactivité de session. Triez selon la colonne **Délai d'inactivité** ou définissez un filtre pour identifier les sessions qui restent inactives au-delà d'une durée spécifique. Le délai d'inactivité est indiqué pour les sessions sur VDA d'OS multi-session qui sont inactives depuis au moins 10 minutes.



Le **délai d'inactivité** s'affiche en tant que **N/A** lorsque l'instance de la session ou de l'application

- n'a pas été inactive pendant plus de 10 minutes,
- est démarrée sur un VDA d'OS mono-session, ou
- est démarrée sur un VDA exécutant la version 7.12 ou antérieure.

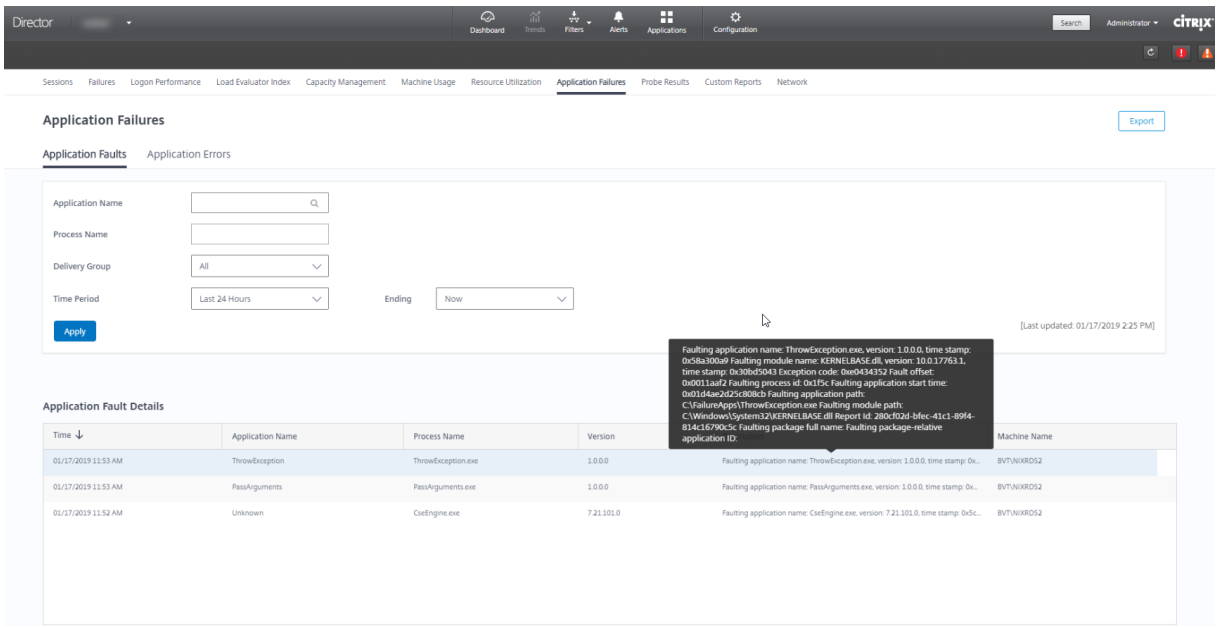
### Historique de détection des défaillances applicatives

L'onglet **Tendances** -> **Échecs applicatifs** affiche les échecs associés aux applications publiées sur les VDA.

Les tendances d'échecs applicatifs sont disponibles pour les 2 dernières heures, 24 dernières heures, 7 derniers jours et le dernier mois pour les sites sous licence Premium et Advanced. Elles sont disponibles pour les 2 dernières heures, 24 dernières heures et 7 derniers jours pour les autres types de licence. Les échecs applicatifs qui sont consignés dans l'Observateur d'événements avec la source « Erreurs applicatives » seront surveillés. Cliquez sur **Exporter** pour générer des rapports aux formats CSV, Excel ou PDF

Les paramètres de rétention de nettoyage pour la détection des échecs applicatifs, GroomApplicationErrorsRetentionDays et GroomApplicationFaultsRetentionDays, sont configurés sur un jour par défaut pour les sites avec licence Premium et non-Premium. Vous pouvez modifier ce paramètre à l'aide de la commande PowerShell :

```
PowerShell command Set-MonitorConfiguration -\<setting name\> \<value
\> <!--NeedCopy-->
```




Les échecs sont affichés en tant que **Défaillances applicatives** ou **Erreurs applicatives** en fonction de leur niveau de gravité. L'onglet Défaillances applicatives affiche les échecs associés à la perte de

données ou de fonctionnalité. Les erreurs applicatives indiquent des problèmes qui ne sont pas immédiats ; ils indiquent des conditions qui peuvent entraîner des problèmes futurs.

Vous pouvez filtrer les échecs selon les paramètres **Nom de l'application publiée**, **Nom du processus** ou **Groupe de mise à disposition** et **Période**. Le tableau affiche le code d'erreur ou d'incident et une brève description de l'échec. La description détaillée de l'échec s'affiche en tant qu'info-bulle.

> **Remarque :**
> Le nom de l'application publiée est affiché comme « Inconnu » lorsque le nom de l'application correspondante ne peut pas être déterminé. Cela se produit généralement lorsqu'une application publiée échoue dans une session de bureau, ou lorsqu'elle échoue en raison d'une exception non prise en charge causée par un exécutable dépendant.

Par défaut, seuls les échecs d'applications hébergées sur des VDA avec OS multi-session sont détectés. Vous pouvez modifier les paramètres de détection dans les stratégies de groupe de surveillance : Activer la détection des défaillances applicatives et Activer la détection des défaillances applicatives sur les VDA d'OS mono-session et Liste des applications exclues de la détection des défaillances. Pour de plus amples informations, consultez la section Stratégies pour la détection des défaillances applicatives dans Paramètres de stratégie Surveillance.

La page **Tendances > Résultats de l'analyse d'application** affiche les résultats des analyses d'application exécutées sur le site au cours des dernières 24 heures et des 7 derniers jours. Pour plus de détails sur la configuration des analyses d'application, voir Analyse d'application.

## Dépanner les machines

June 27, 2024

> **Remarque :**
>
> **Citrix Health Assistant** est un outil qui permet de résoudre les problèmes de configuration dans les VDA non enregistrés. L'outil automatise un certain nombre de vérifications de l'état pour identifier les causes possibles des échecs d'enregistrement de VDA et des problèmes de lancement de session et de configuration de la redirection de fuseau horaire. L'article du centre de connaissances, Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch contient les instructions de téléchargement et d'utilisation de l'outil **Citrix Health Assistant**.

La vue **Filtres > Machines** de la console Director affiche les machines configurées sur le site. L'onglet Machines avec OS multi-session comprend l'index de calculateur de charge, qui indique la distribution des compteurs de performances et les info-bulles du nombre de sessions si vous survolez le lien avec la souris.

Cliquez sur la colonne **Raison de l'échec** pour une machine en échec afin d'obtenir une description détaillée de l'échec et des actions recommandées pour résoudre le problème. Les raisons de l'échec et les actions recommandées pour des défaillances de machines et de connexion sont disponibles sur la page Dépannage et raison des échecs de Citrix Director.

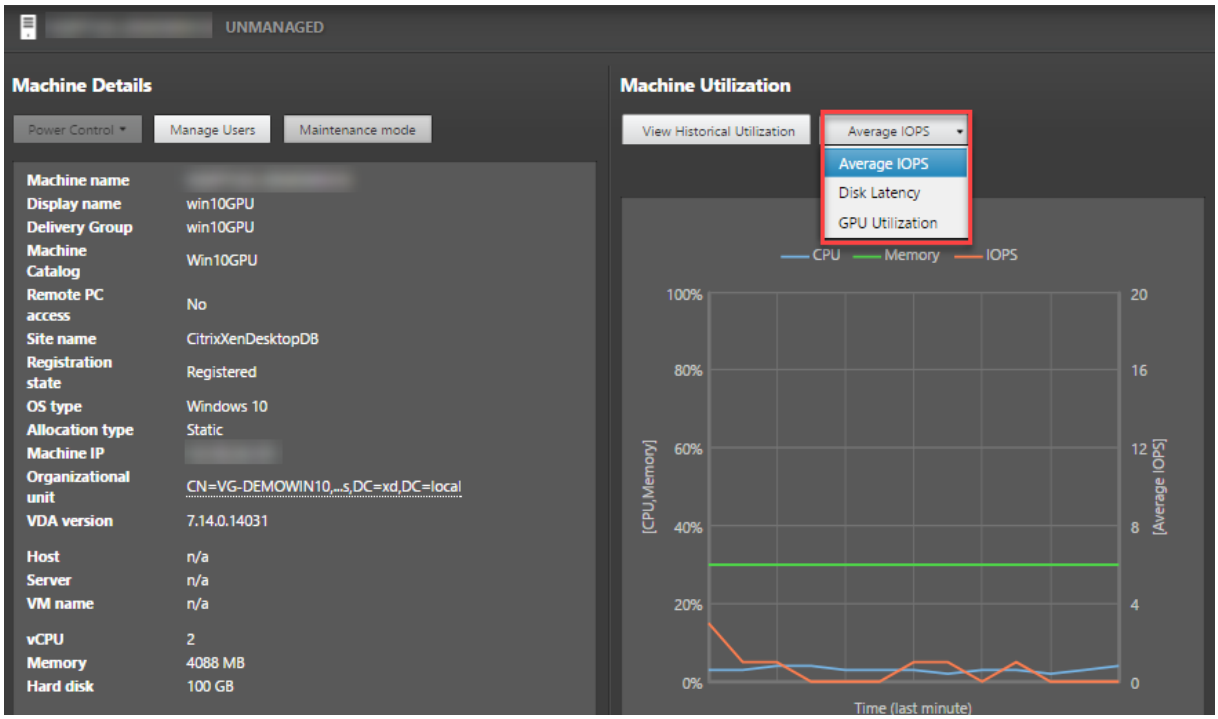
Cliquez sur le lien du nom d'une machine pour accéder à la page **Détails de la machine**.

La page Détails de la machine présente les détails de la machine, les détails de l'infrastructure, et les détails des correctifs appliqués sur la machine.

### Utilisation des ressources en temps réel par machine

Le panneau **Utilisation de machine** affiche des graphiques montrant l'utilisation en temps réel du processeur et de la mémoire. En outre, les graphiques de surveillance de GPU et de disque sont disponibles pour les sites avec Delivery Controller et VDA version **7.14** ou ultérieure.

Les graphiques de surveillance de disque, les nombres moyens d'E/S par seconde et la latence du disque sont des mesures importantes de performance qui vous aident à surveiller et à résoudre les problèmes liés aux disques VDA. Le graphique Nbre moyen d'E/S par seconde affiche le nombre moyen de lectures et d'écritures sur un disque. Sélectionnez **Latence de disque** pour afficher un graphique du délai entre une requête de données et son retour à partir du disque, mesuré en millisecondes.



### Utilisation du GPU

Sélectionnez **Utilisation du GPU** pour afficher le pourcentage d'utilisation du GPU, de la mémoire du GPU et de l'encodeur et du décodeur afin de résoudre les problèmes liés au GPU sur des VDA avec OS mono-session et multi-session.

**Versions de GPU prises en charge :**

- GPU NVIDIA Tesla M60 exécutant le pilote d'affichage version 369.17 ou ultérieure. Pour plus d'informations, consultez la section Logiciel NVIDIA vGPU.
- GPU AMD Radeon Instinct MI25 et processeurs AMD EPYC 7V12 (Rome). Pour plus d'informations, consultez la section Pilotes AMD et support.

**Pilotes :**

Les pilotes ou extensions appropriés doivent être installés sur les VDA.

- Pour les GPU NVIDIA, installez les pilotes GRID manuellement ou via des extensions. Pour plus d'informations, consultez la section Logiciel NVIDIA vGPU.
  - Notez que pour NVIDIA, seuls les pilotes GRID sont pris en charge. Les pilotes CUDA ne fonctionnent pas avec NVadsA10 v5-series et ne sont pas pris en charge.
  - Pour un exemple de processus d'installation de pilotes GPU Nvidia Grid via des extensions sur des machines basées sur Azure, consultez la section Pilotes NVIDIA GRID. Extension du pilote GPU NVIDIA - VM Azure Windows - Machines virtuelles Azure.
  - Pour obtenir un exemple de processus d'installation manuelle des pilotes GPU Nvidia Grid, consultez Azure N-series NVIDIA GPU driver setup for Windows - Azure Virtual Machines.
- Pour les GPU AMD, installez les pilotes graphiques AMD manuellement ou via des extensions. Pour plus d'informations, consultez la section Pilotes AMD et support.
  - Pour obtenir un exemple de processus d'installation de pilotes GPU AMD via des extensions sur des machines basées sur Azure, consultez AMD GPU Driver Extension - Azure Windows VMs - Azure Virtual Machines.
  - Pour obtenir un exemple de processus d'installation manuelle des pilotes GPU AMD sur des machines Azure, consultez Installer des pilotes GPU AMD sur des VM de série N exécutant Windows.

**Remarques d'utilisation :**

- Les graphiques d'utilisation du GPU ne sont disponibles que pour les VDA exécutant Windows 64 bits.
- HDX 3D Pro doit être activé sur le VDA pour que ce dernier puisse proposer l'accélération GPU. Pour de plus amples informations, consultez les sections Accélération GPU pour OS mono-session Windows et Accélération GPU pour OS multi-session Windows.

- Lorsqu'un VDA accède à plusieurs GPU, le graphique d'utilisation affiche la moyenne des mesures de GPU collectées à partir des GPU individuels. Les mesures GPU sont collectées pour le VDA complet et non pour des processus individuels.
- Pour AMD, l'utilisation de l'encodeur et du décodeur n'est pas prise en charge séparément. Toute charge de travail d'encodage/de décodage utilisant le GPU sera signalée comme charge 3D générale liée à l'utilisation du GPU.
- Assurez-vous d'installer le NVIDIA WMI lors de l'installation. Cette fenêtre n'est disponible que lors de l'installation manuelle.
- Si des pilotes sont installés mais que Director ne détecte pas le GPU
  - Vérifiez le Gestionnaire des tâches. Si les pilotes sont correctement installés, le GPU devrait apparaître dans le Gestionnaire des tâches.
  - Vérifiez si la machine est enregistrée. Parfois, les machines peuvent mettre un certain temps à être détectées comme étant en ligne.
- Si l'utilisation du GPU ne montre aucune activité dans Director, assurez-vous que la charge de travail que vous exécutez utilise le GPU. Pour les charges de travail graphiques, cela peut être activé depuis Paramètres > Système > Affichage > Paramètres graphiques > Choisissez l'application pour définir les préférences. Assurez-vous d'activer les hautes performances. Parfois, Windows utilise par défaut le processeur pour les charges de travail graphiques lorsque celui-ci est défini sur les valeurs par défaut du système ou le paramètre Économie d'énergie, en fonction d'autres paramètres.
- Les données sont mises à jour toutes les minutes et la visualisation des données commence dans la minute qui suit la sélection de **Utilisation du GPU**.

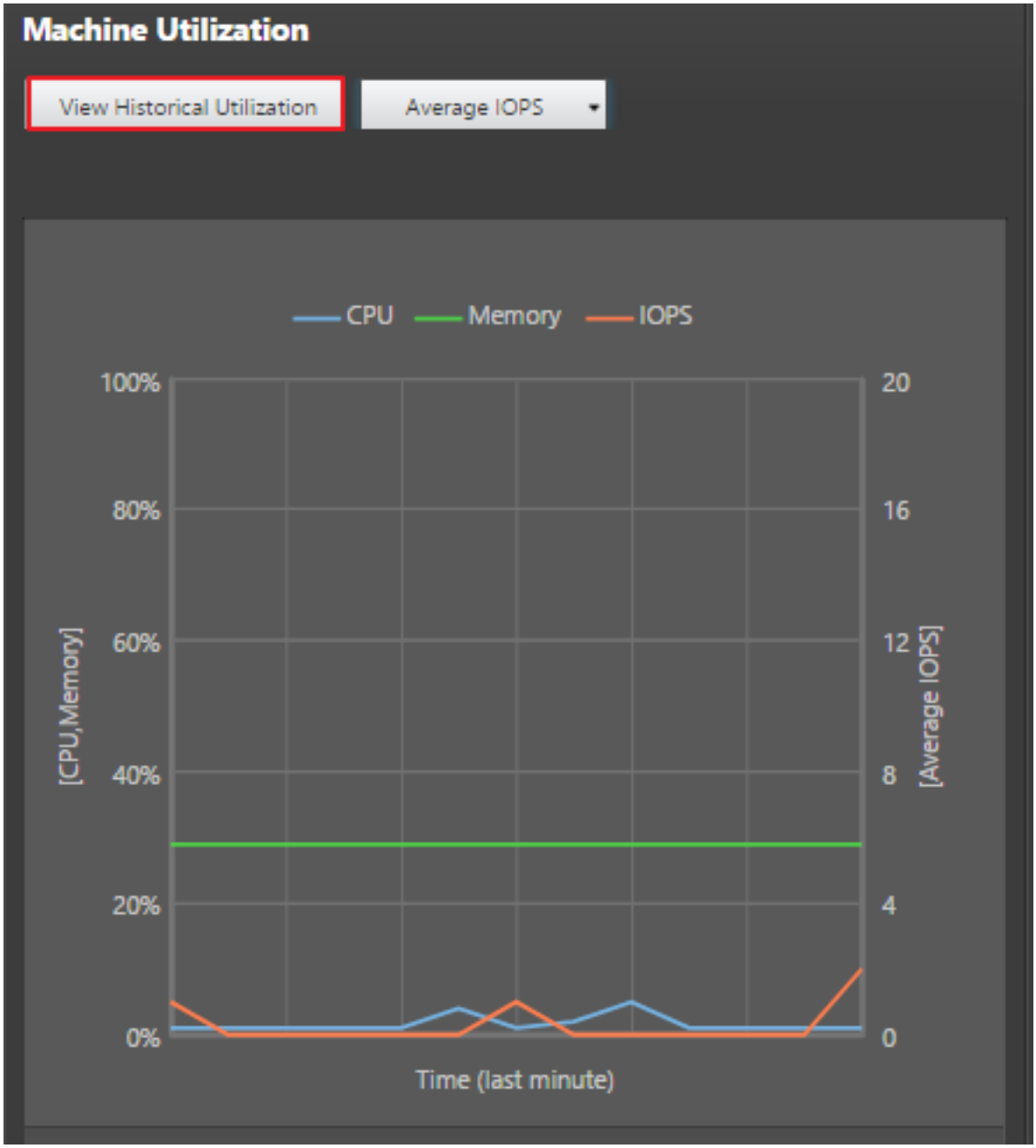
### Utilisation des ressources historiques par machine

Dans le panneau **Utilisation de machine**, cliquez sur **Afficher utilisation historique** pour afficher l'historique d'utilisation des ressources sur la machine sélectionnée.
Les graphiques d'utilisation comprennent les compteurs de performance critiques liés au processeur, à la mémoire, aux sessions simultanées maximales, au nombre moyen d'E/S par seconde et à la latence du disque.

> **Remarque :**
>
> Le paramètre de stratégie Surveillance, **Activer le suivi des processus**, doit être défini sur « Autorisé » pour collecter et afficher les données dans le tableau des 10 processus les plus utilisés sur la page Utilisation historique des machines. La collecte n'est pas autorisée par défaut.

Les données d'utilisation de l'UC et de la mémoire, du nombre moyen d'E/S par seconde et de latence de disque sont collectées par défaut. Vous pouvez désactiver la collecte à l'aide du paramètre de stratégie **Activer le suivi des ressources**.



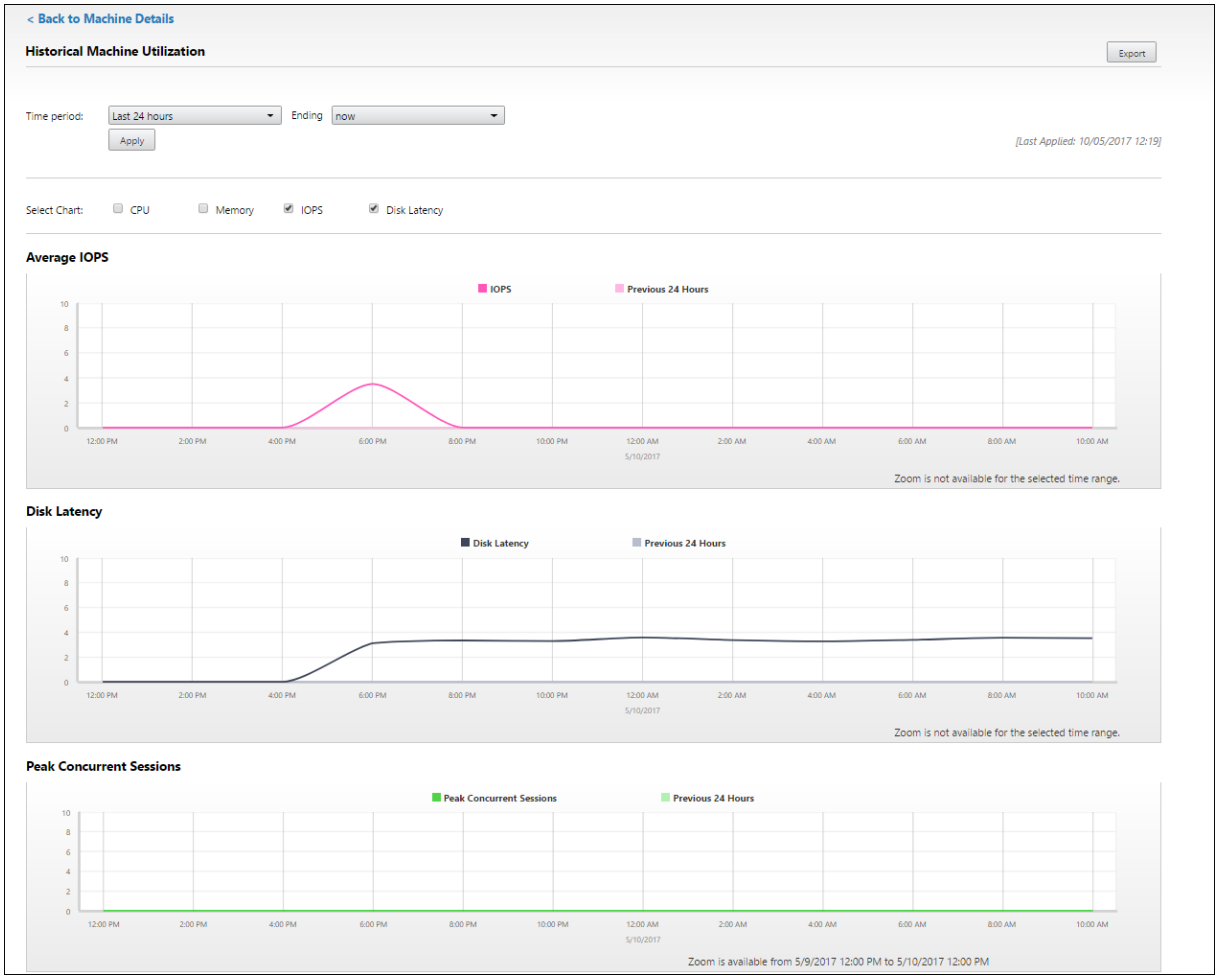

1. Dans le panneau **Utilisation de machine** de la vue de **Détails de machine**, sélectionnez **Afficher utilisation historique**.
2. Dans la page **Utilisation historique des machines**, définissez la **période** d'affichage : 2 dernières heures, 24 dernières heures, 7 derniers jours, dernier mois ou dernière année.

> **Remarque :**
>
> Les données de nombre moyen d'E/S par seconde et d'utilisation de latence de disque sont disponibles uniquement pour les 24 dernières heures, le dernier mois et l'année se

> terminant. L'heure de fin personnalisée n'est pas prise en charge.

3. Cliquez sur **Appliquer** et sélectionnez les graphiques requis.
4. Placez le pointeur de la souris sur les différentes sections du graphique pour afficher de plus amples informations sur la période sélectionnée.




Par exemple, si vous sélectionnez les **2 dernières heures**, la période de référence correspond aux 2 heures avant l'intervalle sélectionné. Affichez la tendance d'UC, de mémoire et de session au cours des 2 dernières heures et de la période de référence. Si vous sélectionnez **Mois dernier**, la période de référence est le mois précédent. Sélectionnez cette option pour afficher le nombre moyen d'E/S par seconde et la latence de disque au cours du dernier mois et la période de référence.

1. Cliquez sur **Exporter** pour exporter les données d'utilisation des ressources pendant la période sélectionnée. Pour de plus amples informations, consultez la section Exporter des rapports dans Surveiller les déploiements.
2. Sous les graphiques, le tableau dresse la liste des 10 processus utilisant le plus d'UC ou de mémoire. Vous pouvez trier par colonne pour la durée sélectionnée : nom de l'application, nom

d'utilisateur, ID de session, utilisation moyenne et max. de l'UC et utilisation moyenne et max. de la mémoire. Les colonnes E/S par seconde et Latence de disque ne peuvent pas être triées.

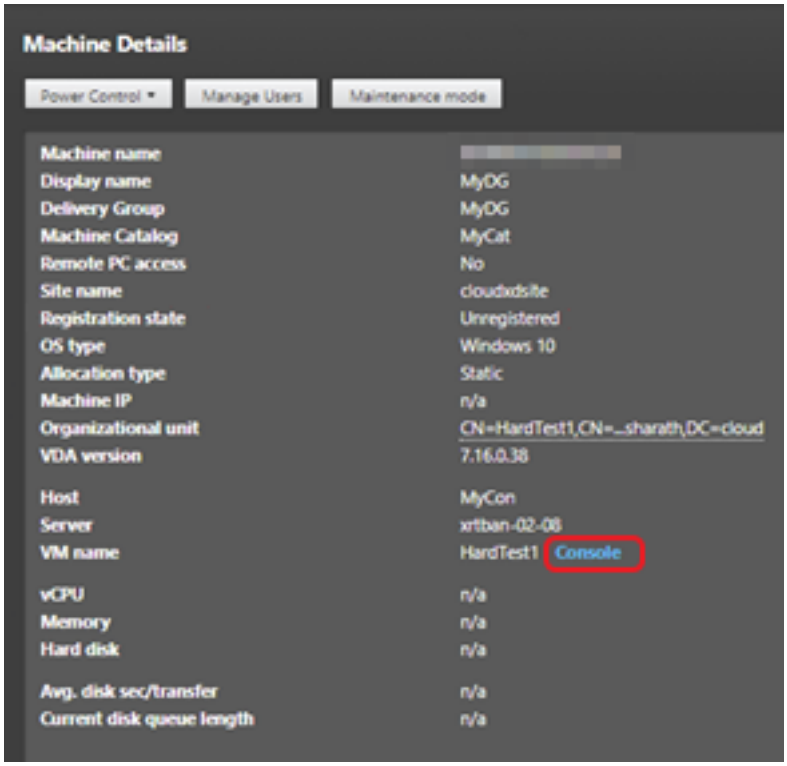
> **Remarque :**
>
> L'ID de session pour les processus système s'affiche en tant que « 0000 ».

3. Pour afficher les tendances historiques de consommation de ressources d'un processus particulier, accédez aux détails d'un des 10 processus les plus utilisés.

### Accès à la console machine

Vous pouvez accéder aux consoles des machines avec OS mono-session et OS multi-session hébergées sur XenServer version 7.3 et ultérieure directement à partir de Director. De cette façon, vous n'avez pas besoin de XenCenter pour résoudre les problèmes sur les VDA hébergés par XenServer. Pour que cette fonctionnalité soit disponible :

- La version 7.16 ou ultérieure de Delivery Controller est requise.
- La version 7.3 ou ultérieure du serveur XenServer hébergeant la machine est requise et doit être accessible depuis l'interface utilisateur de Director.




Pour dépanner une machine, cliquez sur le lien **Console** dans le panneau Détails de la machine correspondant. Après l'authentification des informations d'identification de l'hôte que vous fournissez,

la console de la machine s'ouvre dans un onglet distinct en utilisant noVNC, un client VNC basé sur le Web. Vous avez maintenant accès au clavier et à la souris sur la console.

> **Remarque :**
>
> - Cette fonctionnalité n'est pas prise en charge sur Internet Explorer 11.
> - Si le pointeur de la souris sur la console de la machine est mal aligné, consultez CTX230727 pour connaître les étapes permettant de résoudre le problème.
> - Director lance l'accès à la console dans un nouvel onglet ; assurez-vous que les paramètres de votre navigateur autorisent les fenêtres contextuelles.
> - Pour des raisons de sécurité, Citrix vous recommande d'installer des certificats SSL sur votre navigateur.

### Intégrité des licences Microsoft RDS

Vous pouvez afficher l'état de la licence Microsoft RDS sur le panneau Détails de la machine dans **Détails de la machine** et la page **Détails de l'utilisateur** pour les machines avec OS multi-session.


L'un des messages suivants s'affiche :

- Licence disponible
- Incorrectement configuré (avertissement)
- Erreur de licence (erreur)
- Version du VDA non compatible (erreur)

> **Remarque :**
>
> L'état d'intégrité des licences Microsoft RDS pour les machines sous période de grâce avec licence valide affiche le message **Licence disponible** en vert. Renouvelez votre licence avant son

> expiration.

Pour les messages d'avertissement et d'erreur, passez le curseur sur l'icône d'information pour afficher les informations supplémentaires indiquées dans le tableau suivant.

| Type de message | Messages dans Director |
|---|---|
| Erreur | Disponible pour les VDA versions 7.16 et ultérieures. |
| Erreur | Les nouvelles connexions RDS ne sont pas autorisées. |
| Erreur | La licence Microsoft RDS a dépassé sa période de grâce. |
| Erreur | Aucun serveur de licences n'est configuré pour le niveau d'OS requis avec le type de licence d'accès client par appareil. |
| Erreur | Le serveur de licences configuré n'est pas compatible avec le niveau d'OS de l'hôte RDS avec le type de licence d'accès client par appareil. |
| Avertissement | Le Service Terminal Server Personnel n'est pas un type de licence RSD valide dans un déploiement Citrix Virtual Apps and Desktops. |
| Avertissement | Bureau à distance pour administration n'est pas un type de licence valide dans un déploiement Citrix Virtual Apps and Desktops. |
| Avertissement | Aucun type de licence RDS n'est configuré. |
| Avertissement | Le contrôleur de domaine ou le serveur de licences est inaccessible avec le type de licence RDS d'accès client par utilisateur. |
| Avertissement | Avec le type de licence d'accès client par appareil, la licence de l'appareil client ne peut pas être déterminée car le serveur de licences est inaccessible pour le niveau d'OS requis. |

> **Remarque :**
>
> Cette fonctionnalité s'applique uniquement à la licence d'accès client Microsoft RDS.

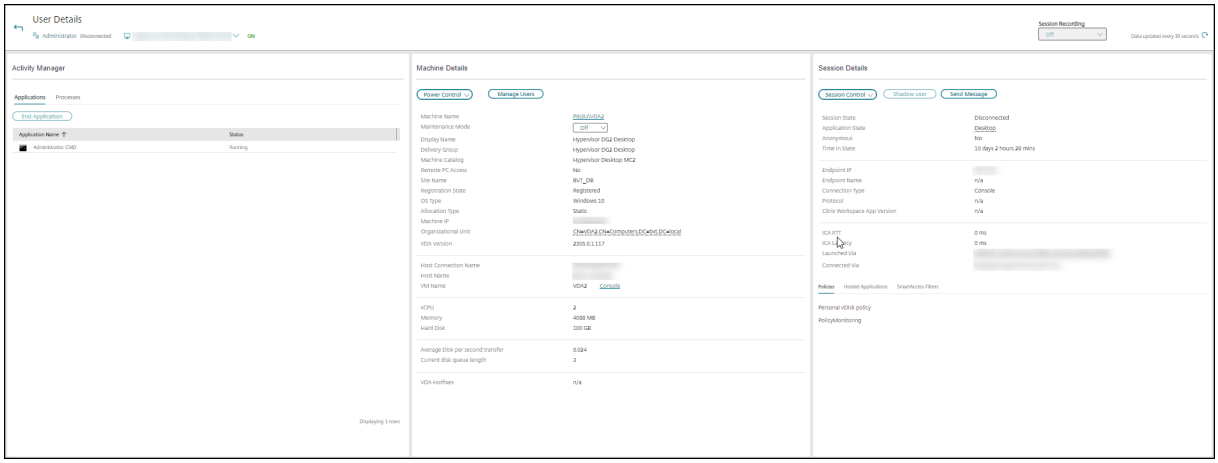
 

# Résoudre les problèmes utilisateur

June 27, 2024

Utilisez la vue **Assistance** de Director (page **Gestionnaire d'activités**) pour afficher des informations sur l'utilisateur ou la session :


Cliquez sur **Afficher les détails** dans le gestionnaire d'activités d'un utilisateur pour ouvrir la page **Détails de l'utilisateur**.
Cliquez sur **Afficher les détails** depuis le gestionnaire d'activités d'un point de terminaison pour ouvrir la page **Détails du point de terminaison**.




## Sélecteur de session

Si l'utilisateur a ouvert plusieurs sessions, le sélecteur de session aide à sélectionner une session.


Choisissez une session pour en voir les détails.

- Vérifiez les détails de la session, de l'expérience de connexion de l'utilisateur, du démarrage de la session, de la connexion et des applications.
- Vous pouvez observer la machine de l'utilisateur.
- Enregistrez la session ICA.

### État d'optimisation de Microsoft Teams

Director affiche l'état d'optimisation de Microsoft Teams pour les sessions HDX dans la page **Détails de l'utilisateur** > panneau **Détails de la session** > champ **Optimisation MS Teams**. L'optimisation de Microsoft Teams est essentielle pour une meilleure expérience utilisateur, notamment pour un son et une vidéo clairs. La visibilité de l'état d'optimisation de Microsoft Teams permet de réduire le temps nécessaire à la résolution des tickets et aide les administrateurs à identifier les mesures importantes lors du dépannage.

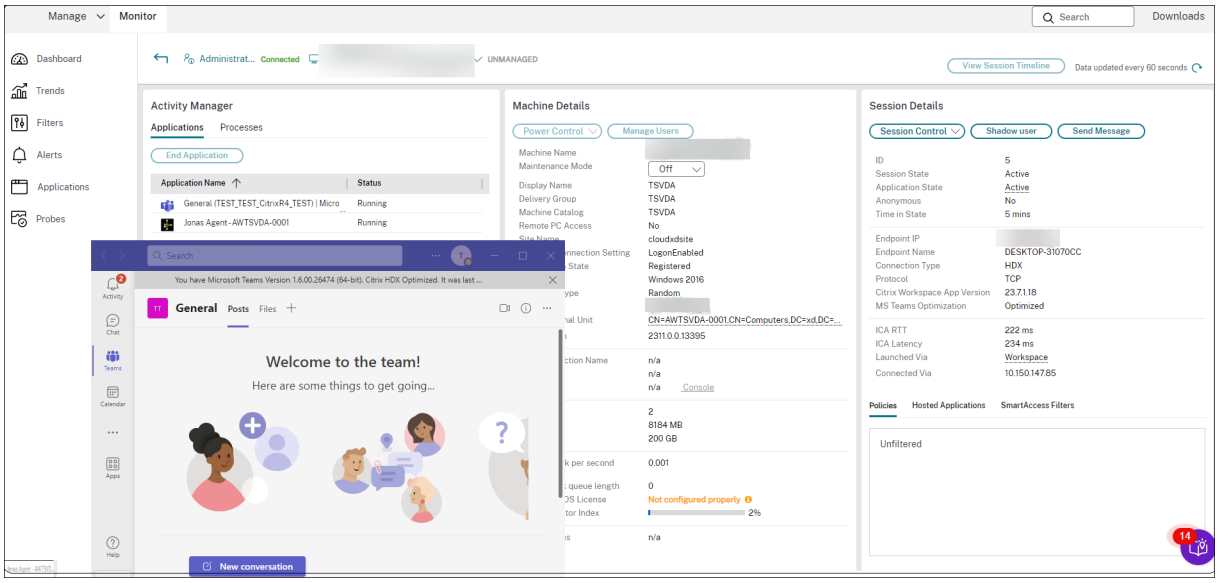
> **Remarque :**
>
> Citrix Director prend en charge Microsoft Teams 2.1 ou la version antérieure.

Pré-requis :

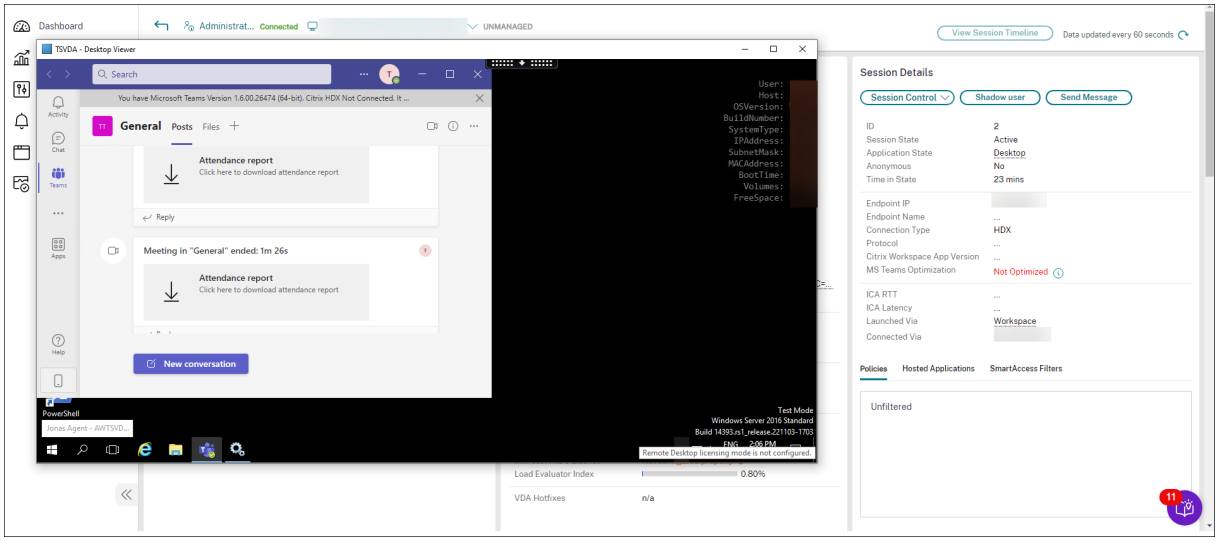
- VDA exécute les versions 2311 et ultérieures.
- Les versions de l'application Citrix Workspace prises en charge sont répertoriées dans Optimisation pour Microsoft Teams.
- Microsoft Teams s'exécute en tant qu'application publiée ou sur un bureau publié.

- Des services essentiels tels que le service de redirection vidéo Citrix HDX HTML5 sont en cours d'exécution.




Si Microsoft Teams n'est pas optimisé, l'info-bulle fournit un lien vers un article de résolution externe en direct de HDX contenant des conseils pour optimiser Microsoft Teams. Résolution des problèmes liés à l'optimisation HDX.




## Conseils de dépannage

Résolvez le problème avec les actions recommandées dans le tableau suivant, et, si nécessaire, informez l'administrateur du problème.

| Problème utilisateur | Suggestions |
| --- | --- |
| L'ouverture de session prend beaucoup de temps ou échoue par intermittence ou de manière répétée | Diagnostiquer les problèmes de connexion utilisateur |
| Le démarrage de session prend beaucoup de temps ou échoue par intermittence ou de manière répétée | Diagnostiquer les problèmes de démarrage de session |
| La réponse de session est lente ou la session ne répond pas | Diagnostiquer les problèmes de performance des sessions |
| L'application est lente ou ne répond pas | Résoudre les échecs applicatifs |
| Échec de la connexion | Restaurer les connexions aux bureaux |
| La session est lente ou ne répond pas | Restaurer les sessions |
| Enregistrer les sessions | Enregistrer les sessions |
| La vidéo est lente ou de qualité médiocre | Exécuter des rapports système sur le canal HDX |

> **Remarque :**
> Pour vous assurer que la machine n'est pas en mode de maintenance, vérifiez le panneau Détails de la machine à partir de la vue Détails de l'utilisateur.

### Ouverture de session

L'onglet **Affichage des détails de l'utilisateur** > onglet **Ouverture de session** affiche une vue complète du processus d'ouverture de session. L'onglet contient le graphique des étapes de durée d'ouverture de session avec les différentes étapes d'ouverture de session tracées. Utilisez ces données pour résoudre les problèmes de connexion des utilisateurs. Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.

### Performances des sessions

L'onglet **Performances des sessions** a amélioré les flux de travail de résolution des problèmes, en commençant par la possibilité de corréler des mesures en temps réel pour identifier les problèmes au cours des sessions utilisateur. Le panneau **Topologie de session** fournit une représentation visuelle du parcours en session pour les sessions HDX connectées. Le panneau **Mesures de performance** affiche les tendances de mesure de session telles que le RTT ICA, la latence ICA, le nombre d'images par seconde, la bande passante de sortie disponible et la bande passante de sortie consommée, qui

permettent d'évaluer l'évolution de ces mesures au fil du temps. Pour en savoir plus, voir la section Diagnostiquer les problèmes de performances des sessions.

### Astuces de recherche

Lorsque vous entrez le nom de l'utilisateur dans le champ Rechercher, Director recherche dans Active Directory les utilisateurs de tous les sites configurés pour prendre en charge Director.

Lorsque vous entrez un nom de machine à plusieurs utilisateurs dans le champ Rechercher, Director affiche les Détails de la machine pour la machine spécifiée.

Lorsque vous entrez un nom de point de terminaison dans le champ Rechercher, Director utilise les sessions non authentifiées (anonymes) et authentifiées connectées à un point de terminaison spécifique. Cette recherche permet de résoudre les sessions non authentifiées. Assurez-vous que les noms de points de terminaison sont uniques pour activer la résolution des problèmes des sessions non authentifiées.

Les résultats de la recherche incluent également les utilisateurs qui ne sont pas connectés ou attribués à une machine.

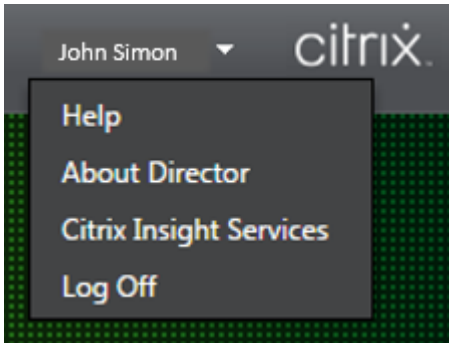
- Les recherches ne sont pas sensibles à la casse.
- Les entrées partielles produisent une liste de correspondances possibles.
- Lorsque vous entrez les premières lettres d'un nom en deux parties en les séparant par un espace, les résultats comprennent les correspondances pour les deux chaînes. Exemples de noms en deux parties : nom d'utilisateur, nom de famille et prénom, nom d'affichage. Par exemple, si vous entrez jo rob, les résultats peuvent inclure des chaînes telles que « John Robertson » ou « Robert, Jones ».

Pour revenir à la page d'accueil, cliquez sur le **logo Director**.

### Accéder à Citrix Insight Services

Vous pouvez accéder à Citrix Insight Services (CIS) à partir de la liste déroulante **Utilisateur** dans Director pour accéder à des informations de diagnostic supplémentaires. Les données disponibles dans CIS sont fournies à partir de sources telles que Call Home et Citrix Scout.




**Charger des informations de dépannage pour le support technique Citrix**

Exécutez Citrix Scout à partir d'un Delivery Controller ou d'un VDA pour capturer les points de données clés et les traces Citrix Diagnostic Facility (CDF) pour dépanner les ordinateurs sélectionnés. Scout offre la possibilité de charger des données en toute sécurité vers la plate-forme CIS pour aider l'assistance technique de Citrix à résoudre les problèmes. L'assistance technique de Citrix utilise la plate-forme CIS pour réduire la durée de résolution des problèmes signalés par les clients.

Scout est installé avec les composants Citrix Virtual Apps and Desktops. En fonction de la version de Windows, Scout s'affiche dans le menu **Démarrer de Windows** ou l'écran d'accueil lorsque vous installez ou mettez à niveau vers Citrix Virtual Apps and Desktops.

Pour démarrer Scout, sélectionnez **Citrix > Citrix Scout** depuis le menu Démarrer ou l'écran d'accueil.

Pour plus d'informations sur l'utilisation et la configuration de Scout et accéder aux questions fréquemment posées, consultez CTX130147.

## Diagnostiquer les problèmes de démarrage de session

June 27, 2024

Outre les phases de processus d'ouverture de session mentionnées dans la section Diagnostiquer les problèmes de connexion utilisateur, Director affiche la durée de démarrage de session. Cette durée est divisée en Démarrage de session dans l'application Workspace et Démarrage de session dans le VDA dans les pages **Détails de l'utilisateur** et **Détails de la machine**. Ces deux durées contiennent en outre des phases individuelles dont les durées de démarrage sont également affichées. Ces données vous aident à comprendre et à résoudre les problèmes de démarrage de session lent. En outre, la durée de chaque phase impliquée dans le démarrage de session aide à résoudre les problèmes associés à des phases individuelles. Par exemple, si le temps de mappage de lecteur est élevé, vous pouvez vérifier si tous les lecteurs valides sont correctement mappés dans l'objet de stratégie de groupe ou le

script. Cette fonctionnalité est disponible sur Delivery Controller version 7 1906 et versions ultérieures et VDA 1903 et versions ultérieures.

### Logiciel requis

Assurez-vous que les conditions préalables suivantes sont remplies pour que les données de durée de démarrage de session soient affichées :

- Delivery Controller 7 1906 ou version ultérieure.
- VDA 1903 ou version ultérieure.
- Le service EUEM (End User Experience Monitoring) de Citrix doit être exécuté sur le VDA.

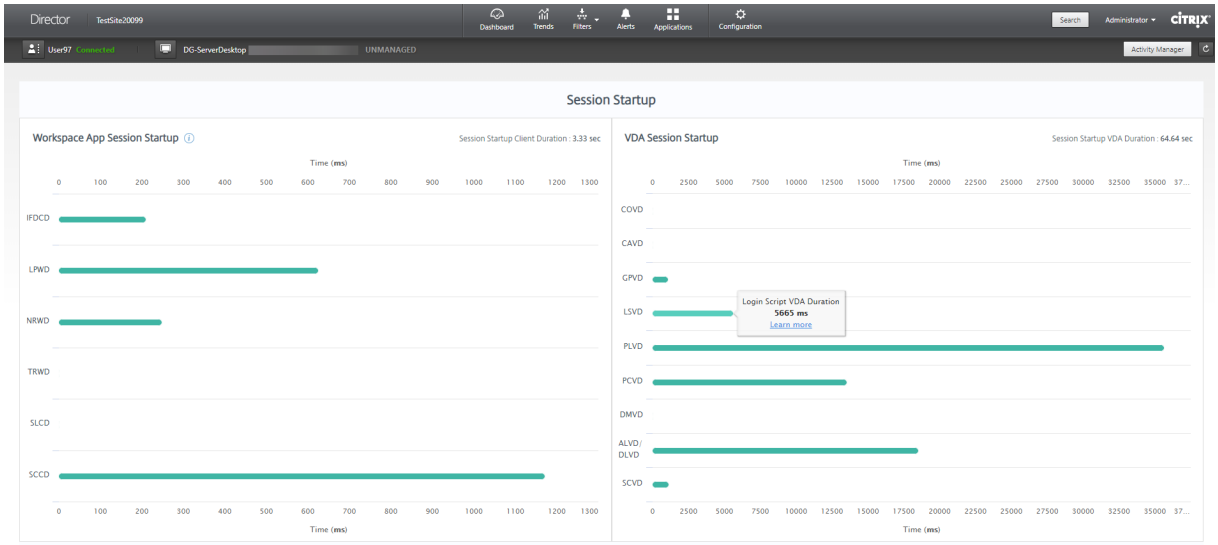
### Limitations

Les limitations suivantes s'appliquent lorsque Director affiche les données de durée de démarrage de session.

- La durée de démarrage de session est disponible uniquement pour les sessions HDX.
- Pour les lancements de session depuis iOS et Android OS, seule la durée de démarrage VDA est disponible.
- La durée de téléchargement du fichier ICA (IFDCD) n'est disponible que si l'application Workspace est détectée lors du lancement à partir d'un navigateur.
- Pour les lancements de session à partir de Mac OS, IFDCD est disponible uniquement pour l'application Workspace 1902 ou version ultérieure.
- Pour les lancements de session à partir du système d'exploitation Windows, IFDCD est disponible pour l'application Workspace 1902 et versions ultérieures. Pour les versions antérieures, IFDCD est affiché uniquement pour les lancements d'application à partir du navigateur avec l'application Workspace détectée.

> **Remarques :**
>
> - Si vous rencontrez des problèmes avec l'affichage de la durée de démarrage des sessions alors que les conditions préalables sont remplies, affichez les journaux du serveur Director et du VDA comme décrit à la section CTX130320.
>
>  Pour les sessions partagées (plusieurs applications lancées dans la même session), les délais de démarrage de l'application Workspace s'affichent pour la dernière connexion ou le dernier lancement de l'application.
> - Certains délais du démarrage de session VDA ne sont pas applicables avec les reconnexions. Dans ce cas, un message s'affiche.




## Phases de démarrage de session de l'application Workspace

### Durée du client de démarrage de session (SSCD)

Lorsque ce délai est élevé, il indique un problème côté client qui cause de longs démarrages. Examinez les délais suivants pour déterminer la cause probable du problème. SSCD démarre aussi près que possible du moment de la demande (clic de souris). Il se termine lorsque la connexion ICA entre la machine client et le VDA a été établie. Dans le cas d'une session partagée, ce délai est beaucoup plus court, car une grande partie des coûts de configuration associés à la création d'une nouvelle connexion au serveur ne sont pas engagés. Au niveau suivant, plusieurs mesures détaillées sont disponibles.

### Durée de téléchargement du fichier ICA

Il s'agit du temps nécessaire au client pour télécharger le fichier ICA à partir du serveur. Le processus global est le suivant :

1. L'utilisateur clique sur une ressource (application ou bureau) dans l'application Workspace.
2. Une demande de l'utilisateur est envoyée à StoreFront via Citrix Gateway (si configuré), qui envoie la demande au Delivery Controller.
3. Le Delivery Controller trouve une machine disponible pour la demande et envoie les informations de la machine et d'autres détails à StoreFront. En outre, StoreFront demande et reçoit un ticket unique de Secure Ticket Authority.
4. StoreFront génère un fichier ICA et l'envoie à l'utilisateur via Citrix Gateway (si configuré).

IFDCD représente le temps requis pour le processus complet (étapes 1 à 4). La durée IFDCD prend fin lorsque le client reçoit le fichier ICA.

LPWD est le composant StoreFront du processus.

Si la valeur IFDCD est élevée (mais LPWD est normal), le traitement côté serveur du lancement a réussi, mais il y a eu des problèmes de communication entre la machine client et StoreFront. Cela indique des problèmes de réseau entre les deux machines. Vous pouvez donc d'abord résoudre les problèmes réseau potentiels.

#### Durée de lancement des pages sur le serveur Web (LPWD)

Temps nécessaire pour traiter la page de lancement (launch.aspx) sur StoreFront. Si la valeur LPWD est élevée, il existe peut-être un goulot d'étranglement sur StoreFront.

Les causes possibles sont les suivantes :

- Charge élevée sur StoreFront. Essayez d'identifier la cause du ralentissement en vérifiant les journaux et les outils de surveillance Internet Information Services (IIS), le Gestionnaire des tâches, le Moniteur de performances et ainsi de suite.
- StoreFront rencontre des problèmes de communication avec d'autres composants tels que le Delivery Controller. Vérifiez si la connexion réseau entre StoreFront et le Delivery Controller est lente ou si certains Delivery Controller sont hors service ou surchargés.

#### Durée de résolution des noms sur le serveur Web (NRWD)

Temps requis par le Delivery Controller pour résoudre le nom d'une application publiée ou d'un bureau publié en une adresse IP de machine VDA.

Lorsque cette valeur est élevée, elle indique que le Delivery Controller prend beaucoup de temps pour résoudre le nom d'une application publiée en une adresse IP.

Les causes possibles incluent un problème sur le client, des problèmes avec le Delivery Controller, tels que le Delivery Controller en surcharge, ou un problème avec la liaison réseau entre eux.

#### Durée de réponse à des tickets sur le serveur Web (TRWD)

Cette durée indique le temps requis pour obtenir un ticket (si nécessaire) auprès du serveur Secure Ticket Authority (STA) ou du Delivery Controller. Lorsque cette durée est élevée, cela indique que le serveur STA ou le Delivery Controller est surchargé.

#### Durée de recherche de sessions sur le client (SLCD)

Cette durée représente le temps nécessaire pour interroger chaque session pour héberger l'application publiée demandée. La vérification est effectuée sur le client pour déterminer si une session exis-

tante peut gérer la demande de lancement de l'application. La méthode utilisée dépend selon que la session est nouvelle ou partagée.

#### Durée de création de sessions sur le client (SCCD)

Cette durée représente le temps nécessaire à la création d'une session, à partir du moment où wfica32.exe (ou un fichier équivalent similaire) est lancé jusqu'au moment où la connexion est établie.

### Phases de démarrage de session VDA

#### Durée de démarrage de session sur le VDA (SSVD)

Cette durée correspond au temps de démarrage de la connexion côté serveur qui englobe le temps nécessaire au VDA pour exécuter l'ensemble de l'opération de démarrage. Lorsque ce délai est élevé, il indique un problème de VDA qui augmente les temps de démarrage de session. Cela inclut le temps passé sur le VDA pour effectuer l'intégralité de l'opération de démarrage.

#### Durée d'obtention des informations d'identification sur le VDA (COVD)

Temps nécessaire au VDA pour obtenir les informations d'identification de l'utilisateur.

Cette durée peut augmenter artificiellement si un utilisateur ne fournit pas les informations d'identification dans les délais. Par conséquent, elle n'est pas comprise dans la durée de démarrage du VDA. Cette durée est susceptible d'être significative uniquement si la connexion manuelle est utilisée et que la boîte de dialogue des informations d'identification côté serveur est affichée (ou si un avis légal est affiché avant le début de la connexion).

#### Durée d'authentification des informations d'identification sur le VDA (CAVD)

Il s'agit du temps nécessaire au VDA pour authentifier les informations d'identification de l'utilisateur par rapport au fournisseur d'authentification. Il peut s'agir de Kerberos, d'Active Directory ou d'une interface SSPI (Security Support Provider Interface).

#### Durée des stratégies de groupe sur le VDA (GPVD)

Cette durée est le temps nécessaire à l'application des objets de stratégie de groupe lors de l'ouverture de session.

#### Durée des scripts de connexion sur le VDA (LSVD)

Temps requis par le VDA pour exécuter les scripts de connexion de l'utilisateur.

Envisagez de rendre asynchrones les scripts de connexion de l'utilisateur ou du groupe. Envisagez d'optimiser les scripts de compatibilité des applications ou d'utiliser des variables d'environnement à la place.

#### Durée de chargement de profils sur le VDA (PLVD)

Temps requis par le VDA pour charger le profil de l'utilisateur.

Si cette durée est élevée, vérifiez la configuration de votre profil utilisateur. La taille et l'emplacement du profil itinérant contribuent au ralentissement des démarrages de session. Lorsqu'un utilisateur se connecte à une session où les profils itinérants des services Terminal Server et les dossiers personnels sont activés, le contenu du profil itinérant et l'accès à ce dossier sont mappés lors de l'ouverture de session. Cela consomme des ressources supplémentaires. Parfois, cela peut consommer une portion importante du processeur. Envisagez d'utiliser les dossiers de **base des services Terminal Server** avec des dossiers personnels redirigés pour atténuer ce problème. En général, pensez à utiliser Citrix Profile Management pour gérer les profils utilisateur dans les environnements Citrix. Si vous utilisez la gestion des profils Citrix et que les délais d'ouverture de session sont longs, vérifiez si votre logiciel antivirus bloque l'outil Citrix Profile Management.

#### Durée de création d'imprimantes sur le VDA (PCVD)

Il s'agit du temps nécessaire au VDA pour mapper les imprimantes clientes de l'utilisateur de manière synchrone. Si la configuration est définie pour que la création de l'imprimante soit effectuée de manière asynchrone, la valeur n'est pas enregistrée pour PCVD car cela n'affecte pas le démarrage de la session.

Un long délai de mappage des imprimantes est souvent lié aux paramètres de stratégie de création automatique de l'imprimante. Le nombre d'imprimantes ajoutées localement sur les machines client des utilisateurs et votre configuration d'impression peuvent affecter directement les délais de démarrage de session. Lorsqu'une session démarre, Citrix Virtual Apps and Desktops doit créer chaque imprimante mappée localement sur la machine cliente. Vous pouvez reconfigurer vos stratégies d'impression afin de réduire le nombre d'imprimantes créées, en particulier lorsque les utilisateurs disposent de nombreuses imprimantes locales. Pour ce faire, modifiez la stratégie de création automatique d'imprimante dans Delivery Controller et Citrix Virtual Apps and Desktops.

**Durée de mappage de lecteurs sur le VDA (DMVD)**

Temps requis par le VDA pour mapper les lecteurs, les périphériques et les ports du client de l'utilisateur.

Assurez-vous que vos stratégies de base incluent des paramètres permettant de désactiver les canaux virtuels inutilisés. Par exemple, le mappage de ports audio ou COM, pour optimiser le protocole ICA et améliorer les performances globales de la session.

**Durée de lancement des applications/bureaux sur le VDA (ALVD/DLVD)**

Cette phase est une combinaison des durées Userinit et Shell. Lorsqu'un utilisateur se connecte à une machine Windows, winlogon exécute userinit.exe. Userinit.exe exécute les scripts d'ouverture de session, rétablit les connexions réseau, puis démarre Explorer.exe. Userinit représente la durée entre le début de userinit.exe et le début de l'interface utilisateur pour le bureau virtuel ou l'application La durée Shell est le temps entre l'initialisation de l'interface utilisateur et le moment où l'utilisateur reçoit le contrôle du clavier et de la souris.

**Durée de création de sessions sur le VDA (SCVD)**

Cette durée inclut divers retards dans le temps de création de session sur VDA.

## Diagnostiquer les problèmes de connexion utilisateur

June 27, 2024

L'onglet **Affichage des détails de l'utilisateur** > onglet **Ouverture de session** affiche une vue complète du processus d'ouverture de session. Utilisez ces données pour résoudre les problèmes de connexion des utilisateurs.

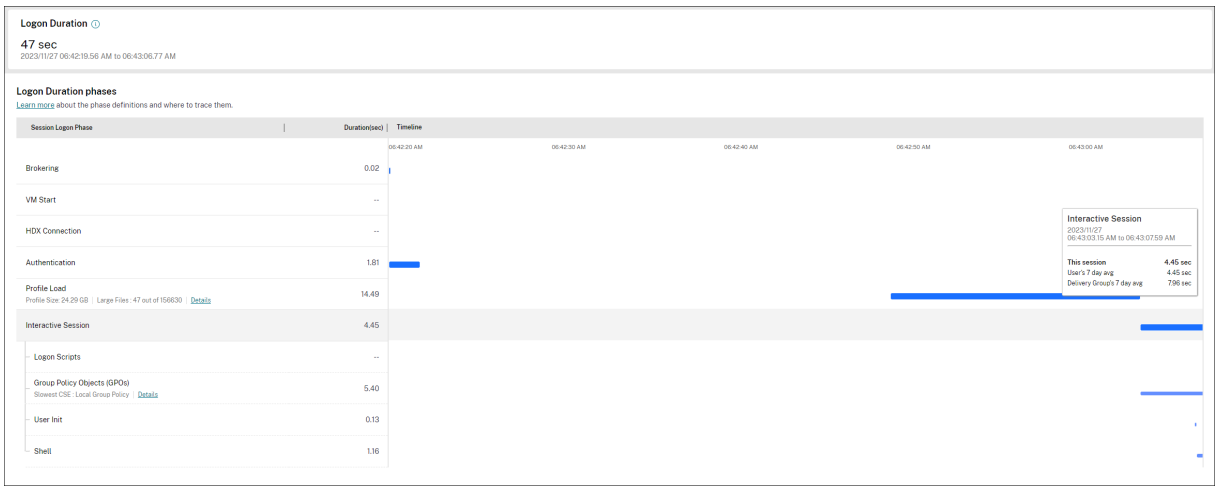
La durée d'ouverture de session est mesurée uniquement pour les connexions initiales à un ordinateur de bureau ou à une application à l'aide de HDX. Ces données n'incluent pas les utilisateurs essayant de se connecter au protocole RDP (Remote Desktop Protocol) ou de se reconnecter à partir de sessions déconnectées. Plus précisément, la durée d'ouverture de session n'est pas mesurée lorsqu'un utilisateur se connecte initialement à l'aide d'un protocole non-HDX et se reconnecte en utilisant HDX.

Lorsque les utilisateurs se connectent à Citrix Virtual Apps and Desktops, le service de surveillance suit les étapes du processus d'ouverture de session. Les étapes commencent du moment où l'utilisateur

se connecte depuis l'application Citrix Workspace jusqu'au moment où l'application ou le bureau est prêt à être utilisé.

L'onglet **Ouverture de session** présente le graphique des étapes de durée d'ouverture de session avec les différentes étapes d'ouverture de session tracées. La durée de connexion représente le temps passé à établir la connexion et à obtenir une application ou un bureau auprès de Delivery Controller, ainsi que le temps passé à s'authentifier et à se connecter à une application ou à un bureau virtuel. Les informations de durée sont présentées en secondes (ou fractions de secondes).




Le graphique des étapes de durée d'ouverture de session illustre de manière claire les différentes étapes d'ouverture de session et leurs heures de début et de fin. Le graphique montre le chevauchement des différentes étapes d'ouverture de session. La durée totale d'ouverture de session peut ne pas être égale à la somme des durées de chaque étape d'ouverture de session. Cela est dû au fait que les différentes étapes peuvent se chevaucher et qu'elles ne font pas toutes partie de cette représentation. En outre, certaines étapes peuvent se prolonger même après que l'utilisateur commence à interagir avec l'application ou le bureau virtuel, et cette durée n'est pas mesurée dans le cadre de la durée globale d'ouverture de session.

Utilisez cette vue pour identifier les étapes d'ouverture de session spécifiques qui retardent le lancement de la session. La définition de chaque étape d'ouverture de session et la source d'événements à partir de laquelle vous pouvez suivre les informations permettent d'approfondir le dépannage. Le fait de survoler le graphique affiche une info-bulle indiquant la durée de l'étape pour la session en cours ainsi que la moyenne sur 7 jours de l'utilisateur et la moyenne sur 7 jours du groupe de mise à disposition. Ces informations permettent de comparer la durée d'ouverture de session actuelle avec les valeurs moyennes sur 7 jours. Vous pouvez explorer les mesures des sous-phases dans le cas d'objectifs de stratégie de groupe et de détails de profil. Cet affichage permet de comprendre et de résoudre facilement les problèmes liés à la durée d'ouverture de session.

### Logiciel requis

Assurez-vous que les conditions préalables suivantes sont remplies pour que les données de durée de connexion et les détails apparaissent :

1. Installez **Citrix User Profile Manager** et **Citrix User Profile Manager WMI Plugin** sur le VDA.
2. Assurez-vous que le service Citrix Profile Management est en cours d'exécution.
3. Pour les sites XenApp et XenDesktop 7.15 et versions antérieures, désactivez le paramètre GPO, **Ne pas traiter la liste d'exécution héritée**.
4. L'option Auditer le suivi des processus doit être activée pour les détails de session interactive.
5. Pour les détails GPO, augmentez la taille des journaux opérationnels de la stratégie de groupe.

> **Remarques :**
>
> - La durée de connexion est prise en charge uniquement sur le shell Windows par défaut (explorer.exe) et non sur les shells personnalisés.
> - La durée d'ouverture de session pour Remote PC Access n'est disponible que lorsque **Citrix User Profile Manager** et le **plug-in WMI Citrix User Profile Manager** sont installés en tant que composants supplémentaires lors de l'installation de Remote PC Access. Pour de plus amples informations, consultez l'étape 4 dans Séquence de configuration et considérations pour Remote PC Access.

### Étapes pour résoudre les problèmes d'ouverture de session utilisateur

1. Dans la vue **Détails de l'utilisateur** > onglet **Ouverture de session**, résolvez les problèmes liés à l'état de connexion à l'aide du graphique de durée d'ouverture de session.
   - Si l'utilisateur ouvre une session, l'affichage indique le processus d'ouverture de session.
   - Si l'utilisateur est connecté, le panneau Durée de l'ouverture de session affiche le temps qu'il a fallu à l'utilisateur pour se connecter à la session en cours.
2. Examinez les phases du processus d'ouverture de session.

### Phases du processus d'ouverture de session

#### Négociation des connexions

Durée requise pour décider quel bureau à attribuer à l'utilisateur.

### Démarrage de machine virtuelle

Si la session requiert le démarrage d'une machine, Démarrage machine virtuelle est la durée requise pour démarrer la machine virtuelle.

### Connexion HDX

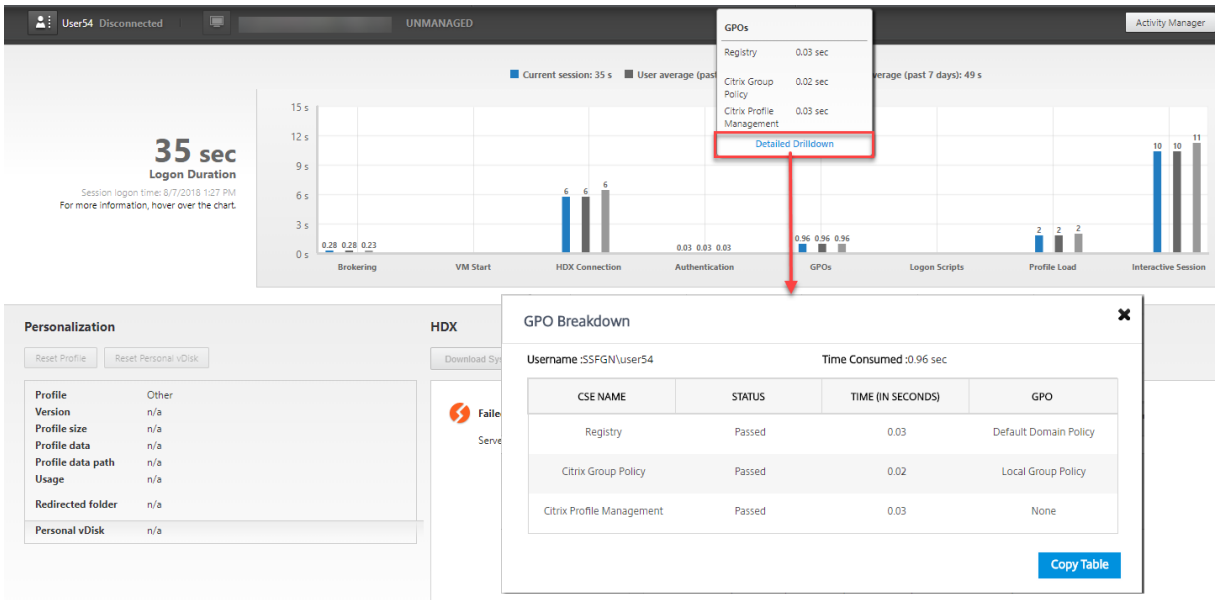
Durée requise pour effectuer les étapes permettant d'établir la connexion HDX du client vers la machine virtuelle.

### Authentification

Durée requise pour effectuer l'authentification sur la session distante.

### GPO

Si des paramètres de stratégie de groupe sont activés sur les machines virtuelles, durée requise pour appliquer les objets de stratégie de groupe au cours de l'ouverture de session. Les détails du temps nécessaire pour appliquer chaque stratégie conformément aux CSE (Extensions côté client) sont disponibles sous la forme d'une info-bulle lorsque vous passez la souris sur la barre GPO.




Cliquez sur **Détails** pour afficher un tableau avec l'état de la stratégie et le nom de l'objet de stratégie de groupe correspondant. Les durées indiquées dans le détail représentent uniquement la durée du traitement des CSE et ne correspondent pas à la durée totale du GPO. Vous pouvez copier le tableau détaillé pour un dépannage ou pour des rapports. La durée du GPO pour les stratégies est extraite des

journaux de l'Observateur d'événements. Les journaux peuvent être écrasés en fonction de la mémoire allouée aux journaux opérationnels (la taille par défaut est de 4 Mo). Pour plus d'informations sur l'augmentation de la taille des journaux opérationnels, voir l'article Microsoft TechNet Configuration des journaux d'événements.

### Scripts d'ouverture de session

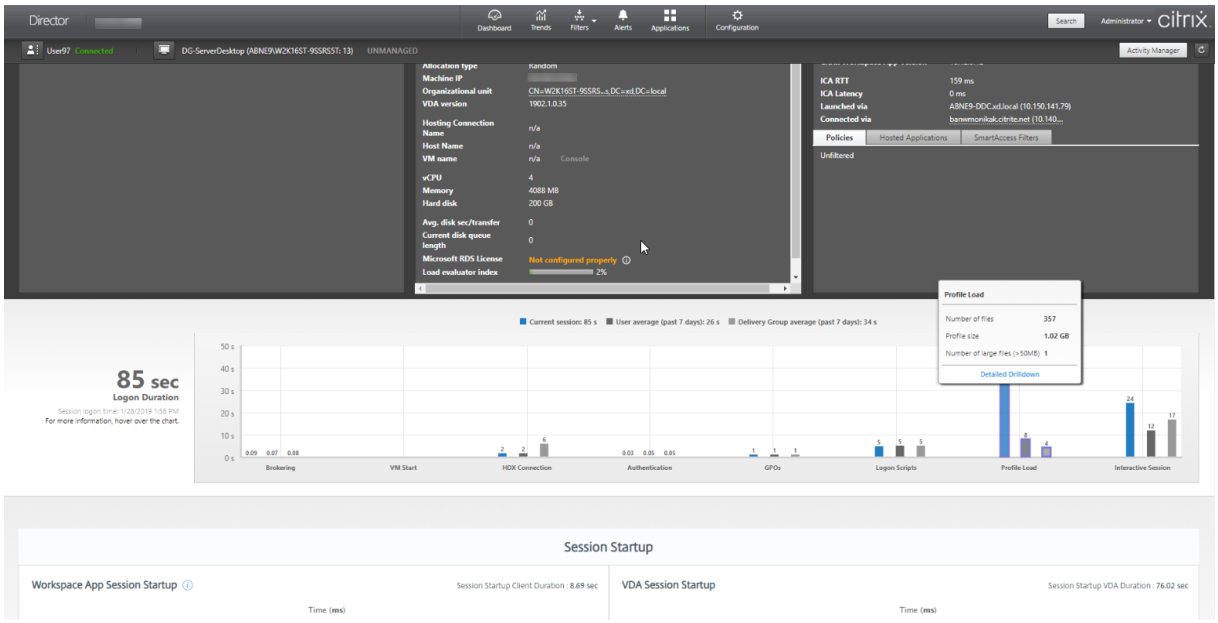
Si des scripts de connexion sont configurés pour la session, durée requise pour l'exécution des scripts de connexion.

### Chargement du profil

Si des paramètres de profil sont configurés pour l'utilisateur ou la machine virtuelle, durée requise pour charger le profil utilisateur.

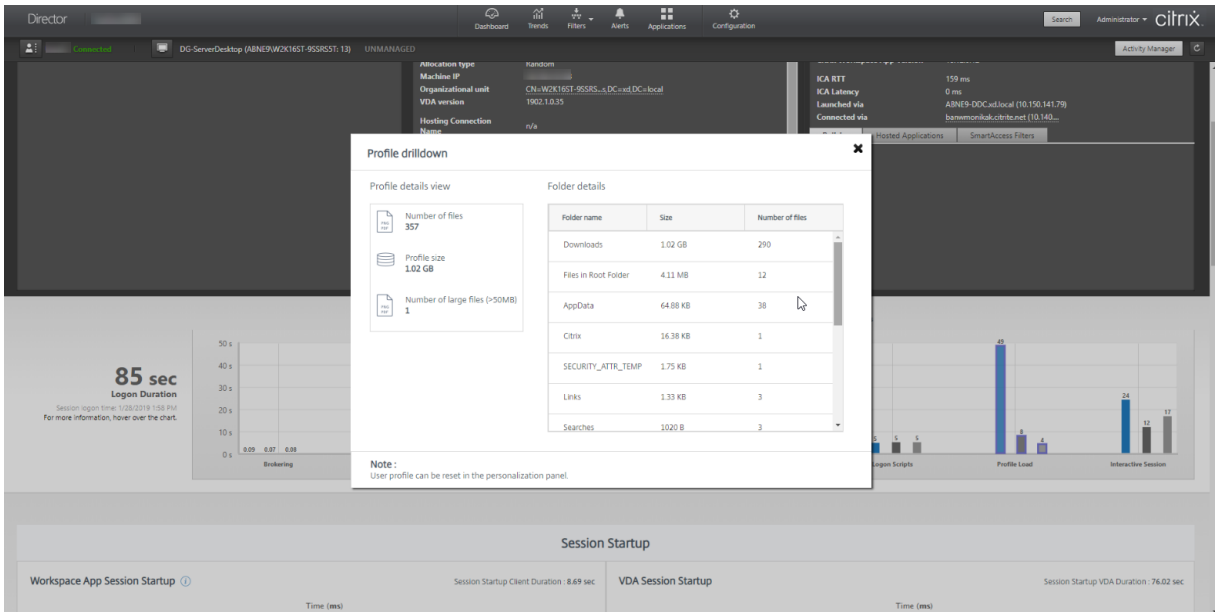
Si Citrix Profile Management est configuré, la barre de chargement du profil inclut le temps que met Citrix Profile Management à traiter les profils utilisateur. Ces informations aident les administrateurs à résoudre les durées de traitement de profil élevées. Lorsque Profile Management est configuré, la barre de chargement du profil affiche une durée accrue. Cette augmentation est causée par cette amélioration et ne reflète pas une dégradation des performances. Cette amélioration est disponible sur les VDA 1903 ou version ultérieure.

Le survol de la barre de chargement du profil affiche une info-bulle affichant les détails du profil utilisateur pour la session en cours.



Cliquez sur **Détails** pour afficher des détails sur chaque dossier du dossier racine du profil (par exemple, C:/Users/username), sa taille et le nombre de fichiers (y compris les fichiers contenus dans les dossiers imbriqués).




La fonctionnalité d'analyse détaillée est disponible sur Delivery Controller version 7 1811 ou ultérieure et les VDA 1811 ou version ultérieure. À l'aide des informations détaillées du profil, vous pouvez résoudre les problèmes impliquant une durée de chargement de profil élevée. Vous pouvez :

- Réinitialiser le profil utilisateur
- Optimiser le profil en supprimant les fichiers volumineux indésirables
- Réduire le nombre de fichiers pour réduire la charge du réseau
- Utiliser le streaming de profil

Par défaut, tous les dossiers de la racine du profil sont affichés dans les détails. Pour masquer la visibilité des dossiers, modifiez la valeur de registre suivante sur la machine VDA :

> **Avertissement :**
>
> L'ajout et la modification incorrects du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne garantit pas la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous assumez l'ensemble des risques liés à l'utilisation de l'Éditeur du Registre. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

1. Sur le VDA, ajoutez une nouvelle valeur de Registre **ProfileFoldersNameHidden** à HKEY_LOCAL_MACHINE\S
2. Définissez la valeur sur 1. Cette valeur doit être une valeur DWORD (32 bits). La visibilité des noms de dossier est maintenant désactivée.

3. Pour que les noms de dossier soient à nouveau visibles, définissez la valeur sur 0.

> **Remarque :**
> Vous pouvez utiliser un objet de stratégie de groupe ou des commandes PowerShell pour appliquer le changement de valeur de registre sur plusieurs machines. Pour plus d'informations sur l'utilisation des objets de stratégie de groupe pour déployer les modifications du registre, consultez le blog.

#### Informations supplémentaires

- Les détails du profil n'incluent pas les dossiers redirigés.
- Les fichiers NTUser.dat du dossier racine peuvent ne pas être visibles pour les utilisateurs finaux. Toutefois, ils sont inclus dans les détails du profil et affichés dans la liste des fichiers du **dossier racine**.
- Certains fichiers cachés dans le dossier AppData ne sont pas inclus dans l'exploration hiérarchique du profil.
- Le nombre de fichiers et les données de taille du profil peuvent ne pas correspondre aux données du panneau Personnalisation en raison de certaines limitations Windows.

#### Session interactive

La session interactive est la durée requise pour « transférer » le contrôle du clavier et de la souris à l'utilisateur une fois le profil utilisateur chargé. De toutes les phases du processus d'ouverture de session, il s'agit généralement de la durée la plus longue. Elle est calculée comme suit : **Durée de session interactive = heure à laquelle le bureau est prêt (EventId 1000 sur le VDA) - heure à laquelle le profil utilisateur est chargé (EventId 2 sur le VDA)**. La session interactive comporte trois sous-phases : Pre-userinit, Userinit et Shell. Passez la souris sur Session interactive pour afficher une info-bulle montrant les éléments suivants :

- phases secondaires
- durée de chaque phase secondaire
- délai cumulé total entre ces phases secondaires

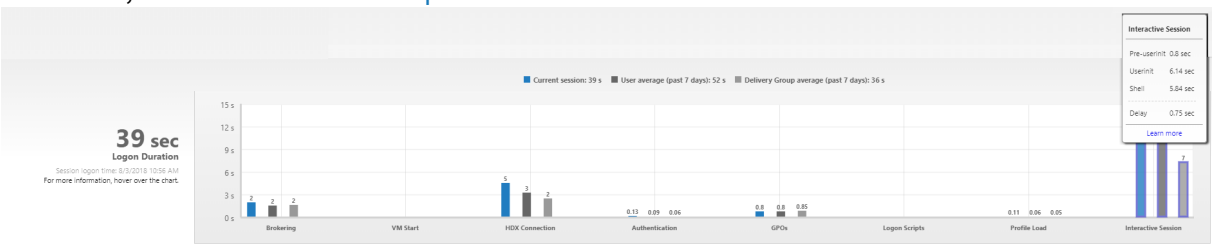
> **Remarque :**
>
> Cette fonctionnalité est disponible sur la version 1811 et ultérieure des VDA. Si vous avez lancé des sessions sur des sites antérieurs à 7.18 et que vous avez ensuite mis à niveau vers 7.18 ou une version ultérieure, le message « Exploration non disponible en raison d'une erreur du serveur » s'affiche. Toutefois, si vous avez lancé des sessions après la mise à niveau, aucun message d'erreur n'est affiché.

Pour afficher la durée de chaque sous-phase, activez Auditer le suivi des processus sur la machine virtuelle (VDA). Lorsque Auditer le suivi des processus est désactivé (par défaut), la durée de Pre-userinit et la durée combinée de Userinit et Shell sont affichées. Vous pouvez activer Auditer le suivi des processus via un objet de stratégie de groupe (GPO) comme suit :

1. Créez un objet de stratégie de groupe et modifiez-le à l'aide de l'éditeur de stratégie de groupe.
2. Accédez à **Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Stratégie d'audit**.
3. Dans le volet droit, double-cliquez sur **Auditer le suivi des processus**.
4. Sélectionnez **Réussite** et cliquez sur OK.
5. Appliquez cet objet de stratégie de groupe aux VDA ou au groupe requis.

Pour plus d'informations sur l'option Auditer le suivi des processus et savoir comment l'activer ou la désactiver, voir Auditer le suivi des processus dans la documentation Microsoft.




Panneau Durée d'ouverture de session dans la vue Détails de l'utilisateur

- **Session interactive –Pre-userinit :** c'est le segment de la session interactive qui chevauche les objets de stratégie de groupe (GPO) et les scripts. Cette sous-phase peut être réduite en optimisant les GPO et les scripts.
- **Session interactive –Userinit :** lorsqu'un utilisateur se connecte à une machine Windows, Winlogon exécute userinit.exe. Userinit.exe exécute les scripts d'ouverture de session, rétablit les connexions réseau, puis démarre Explorer.exe, l'interface utilisateur Windows. Cette sous-phase de la session interactive représente la durée entre le début de Userinit.exe et le début de l'interface utilisateur pour le bureau virtuel ou l'application
- **Session interactive –Shell :** dans la phase précédente, Userinit démarre l'initialisation de l'interface utilisateur Windows. La sous-phase Shell capture la durée entre l'initialisation de l'interface utilisateur et le moment où l'utilisateur reçoit le contrôle du clavier et de la souris.
- **Délai :** il s'agit du délai cumulé entre les sous-phases **Pre-userinit et Userinit** et les sous-phases **Userinit et Shell**.

La durée totale d'ouverture de session n'est pas la somme exacte de ces phases. Par exemple, certaines phases se produisent en parallèle, et dans certaines phases, un traitement supplémentaire se produit pouvant entraîner une durée d'ouverture de session plus longue que la somme.
La durée totale d'ouverture de session n'inclut pas la durée d'inactivité ICA correspondant au délai entre le téléchargement du fichier ICA et le lancement du fichier ICA pour une application.
Pour activer l'ouverture automatique du fichier ICA au lancement de l'application, configurez votre

navigateur pour le lancement automatique du fichier ICA lors du téléchargement d'un fichier ICA. Pour plus d'informations, veuillez consulter l'article CTX804493.

> **Remarque :**
> Le graphique Durée d'ouverture de session affiche les phases d'ouverture de session en secondes. Toutes les valeurs de durée inférieures à une seconde sont affichées en tant que fraction de seconde. Les valeurs supérieures à une seconde sont arrondies à la demi-seconde la plus proche. Le graphique a été conçu pour afficher la valeur la plus élevée de l'axe Y en tant que 200 secondes. Toute valeur supérieure à 200 secondes est montrée avec la valeur réelle affichée au-dessus de la barre.

### Conseils de dépannage

Pour identifier les valeurs inattendues ou inhabituelles dans le graphique, comparez la durée requise lors de chaque phase de la session en cours avec la durée moyenne pour cet utilisateur au cours des sept derniers jours, et avec la durée moyenne de tous les utilisateurs dans ce groupe de mise à disposition au cours des sept derniers jours.

Faites remonter le problème si nécessaire. Par exemple, si le démarrage de la machine virtuelle est lent, le problème peut provenir de l'hyperviseur, vous pouvez donc en informer l'administrateur de l'hyperviseur. Ou, si la durée de négociation est lente, vous pouvez adresser ce problème à l'administrateur de site pour vérifier l'équilibrage de charge sur le Delivery Controller.

Examinez les différences inhabituelles, notamment :

- Barres d'ouverture de session manquantes
- Écart important entre la durée actuelle et la durée moyenne de cet utilisateur. Causes potentielles :
  - Une nouvelle application a été installée.
  - Une mise à jour du système d'exploitation s'est produite.
  - Des modifications ont été apportées à la configuration.
  - La taille du profil utilisateur est élevée. Dans ce cas, le temps de chargement du profil est élevé.
- Écart important entre le nombre d'ouvertures de session de l'utilisateur (actuel et durée moyenne) et la durée moyenne du groupe de mise à disposition.

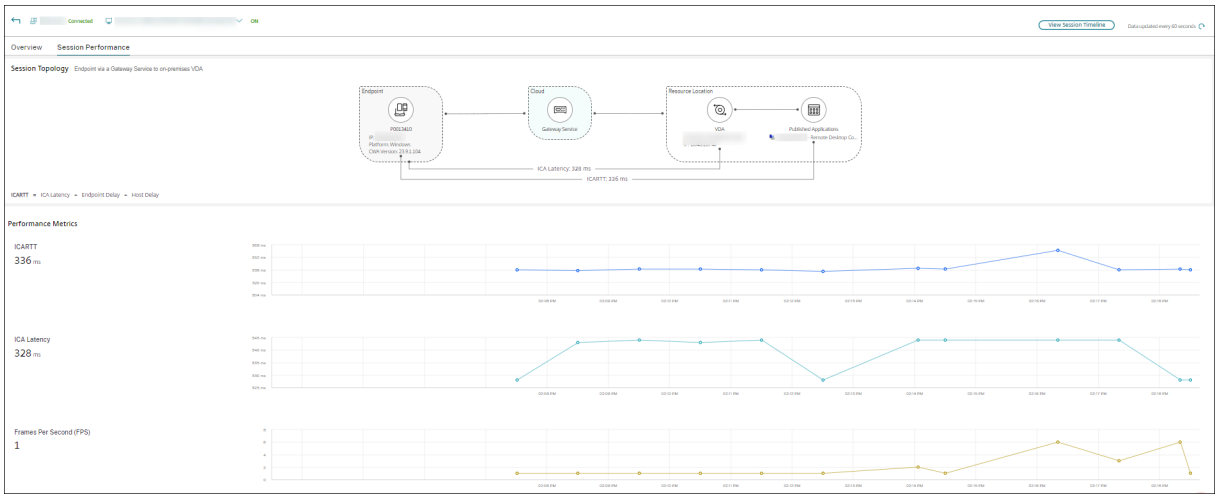
Si nécessaire, cliquez sur **Redémarrer** pour observer le processus d'ouverture de session de l'utilisateur pour résoudre les problèmes, tels que Démarrage de machine virtuelle ou Négociation.

# Diagnostiquer les problèmes de performance des sessions

June 27, 2024

L'onglet **Performances des sessions** de la page Détails de l'utilisateur propose des workflows de dépannage améliorés pour aider à identifier les problèmes au cours des sessions utilisateur HDX. Les panneaux Topologie de session et Indicateurs de performance permettent de mettre en corrélation la vue des composants et les multiples indicateurs de performance d'une session dans une seule vue, et de réduire le temps moyen de résolution des problèmes liés à l'expérience de session.




## Vue des sauts réseau de bout en bout

La visualisation des sauts réseau de bout en bout constitue la prochaine étape pour améliorer les workflows de dépannage. La section **Détails utilisateur** > **Performances de session** > **Topologie de session** affiche la vue des sauts réseau de bout en bout pour les sessions HDX connectées.

La topologie de session pour une session connectée montre les composants impliqués dans le parcours de session avec leurs métadonnées, le lien entre les composants et les applications publiées sur le VDA.
En outre, les indicateurs de performance de session suivants sont affichés pour la session :

- Latence ICA - La latence est en fait la latence du réseau. Ce paramètre indique si le réseau est lent.
- RTT ICA - Le RTT ICA est l'intervalle de temps entre l'action d'un utilisateur et la réponse graphique affichée sur son écran. Cet indicateur inclut la latence ICA, le délai du point de terminaison et le délai de l'hôte.

Vous pouvez utiliser cette vue pour comprendre les composants par lesquels les données de session circulent et identifier le saut spécifique susceptible d'entraîner des problèmes de performances.

Les indicateurs de performance de la vue Topologie de session ne sont disponibles que pour les sessions HDX à l'état connecté.

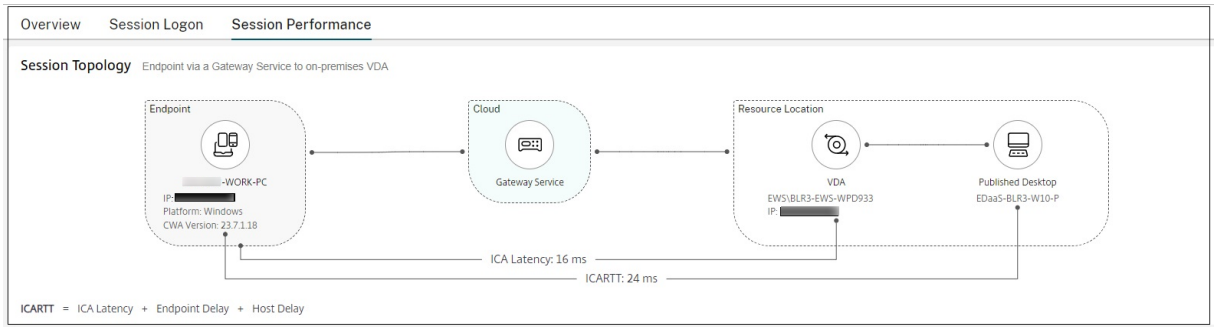
### Scénarios de topologie de session

Selon le scénario de déploiement du site, les composants impliqués dans une session sont tous les composants ou l'un des suivants :

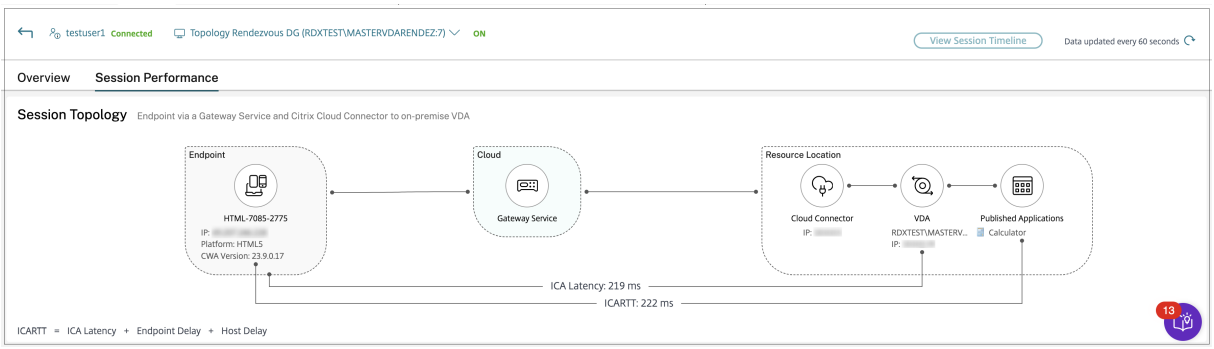
- Application Citrix Workspace sur point de terminaison
- Service de passerelle/passerelle sur site
- Cloud Connector —La passerelle est connectée à DaaS via un Cloud Connector dans le cas de connexions hybrides.
- VDA

En conséquence, les topologies de réseau possibles sont les suivantes :

- L'application Citrix Workspace sur le point de terminaison se connecte via Citrix Workspace et Gateway Service à un VDA local. Aucun Cloud Connector n'est utilisé pour se connecter au VDA.

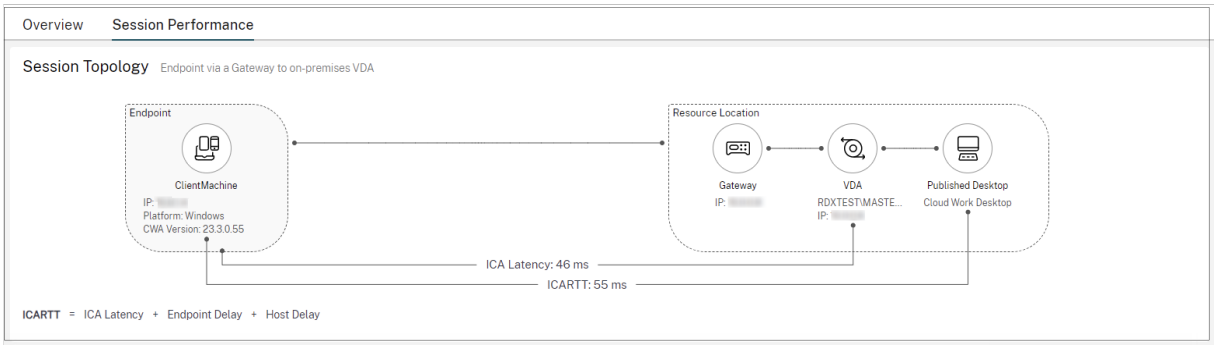



- L'application Citrix Workspace sur le point de terminaison se connecte via Citrix Workspace et Gateway Service à un VDA local via un Cloud Connector.

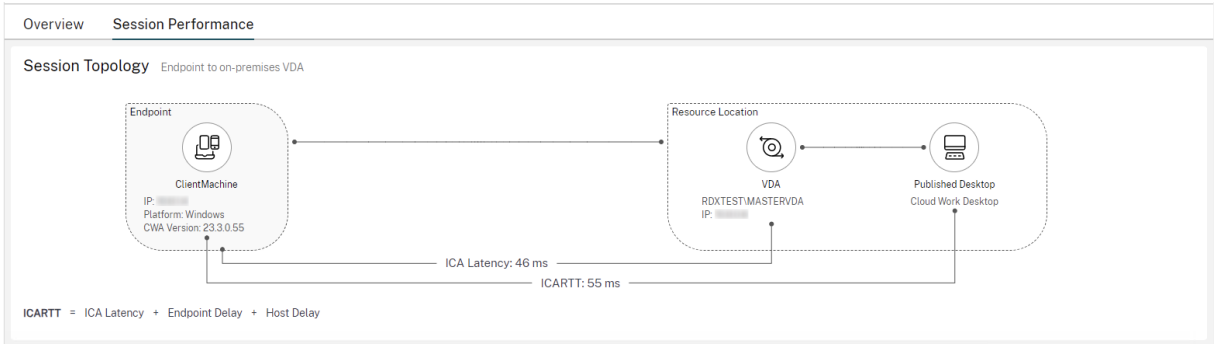



- L'application Citrix Workspace sur le point de terminaison se connecte via StoreFront et une passerelle locale au VDA local.




- L'application Citrix Workspace sur le point de terminaison se connecte via StoreFront au VDA local.




## Indicateurs de performance

Le panneau **Indicateurs de performance** permet de corréler les indicateurs en temps réel pour identifier les problèmes au cours des sessions utilisateur. Les tendances des indicateurs de session permettent d'indiquer les performances de ces indicateurs au fil du temps. Lorsque vous cliquez sur l'onglet **Performances des sessions**, vous pouvez voir les données en temps réel, ainsi que les données des 15 dernières minutes sans attendre le temps de chargement de la page. Les graphiques permettent de corréler les mesures de performance de plusieurs composants dans une seule vue.


> **Remarque :**
>
> Avec la prise en charge des mesures des 15 dernières minutes, le graphique est tracé pour la durée pendant laquelle la session est connectée et déconnectée. La mesure de la session déconnectée est affichée avec la valeur zéro.

Outre RTT ICA et Latence ICA, les indicateurs suivants sont disponibles :

- Images par seconde - Le nombre d'images par seconde est une mesure importante qui indique la réactivité de la session.
  Bande passante de sortie disponible - La bande passante de sortie disponible est une mesure de la bande passante totale disponible pour transmettre des données du VDA au point de terminaison.
- Bande passante de sortie consommée - La bande passante de sortie consommée indique la quantité réelle de données transmises du VDA au point de terminaison pour afficher les sessions pour les utilisateurs.

L'analyse de la bande passante de sortie disponible et de la bande passante de sortie consommée permet de vérifier si une bande passante suffisante est disponible pour les sessions et de détecter si une session est affectée par une bande passante insuffisante.

## Observer les utilisateurs

June 27, 2024

À partir de Director, utilisez la fonctionnalité d'observation utilisateur pour afficher ou travailler directement sur la machine virtuelle ou la session d'un utilisateur. Vous pouvez observer des VDA Win-

dows et Linux. L'utilisateur doit être connecté à la machine que vous souhaitez observer. Vérifiez ceci en vérifiant le nom de la machine dans la barre de titre utilisateur.

Director lance l'observation dans un nouvel onglet, vous devez donc mettre à jour les paramètres de votre navigateur pour autoriser les fenêtres contextuelles à partir de l'URL de Director.

Accédez à la fonctionnalité d'observation à partir de la vue **Détails de l'utilisateur**. Sélectionnez la session utilisateur et cliquez sur **Observer** dans la vue Gestionnaire d'activités ou dans le panneau Détails de la session.

### Observation de VDA Linux

L'observation est disponible pour les VDA Linux versions 7.16 ou ultérieures exécutant les distributions Linux RHEL7.3 ou Ubuntu version 16.04.

> **Remarque :**
>
> - Le VDA doit être accessible à partir de l'interface utilisateur de Director pour que l'observation fonctionne. Par conséquent, l'observation n'est possible que pour les VDA Linux dans le même intranet que le client Director.
> - Director utilise le nom de domaine complet pour se connecter au VDA Linux cible. Assurez-vous que le client Director peut résoudre le nom de domaine complet du VDA Linux.
> - Les packages python websockify et x11vnc doivent être installés sur le VDA.
> - La connexion noVNC au VDA utilise le protocole WebSocket. Par défaut, le protocole **ws://** WebSocket est utilisé. Pour des raisons de sécurité, Citrix vous recommande d'utiliser le protocole **wss://** sécurisé. Installez des certificats SSL sur chaque client Director et VDA Linux.

Suivez les instructions dans Observation de session pour configurer votre VDA pour l'observation.

1. Une fois que vous avez cliqué sur **Observer**, la connexion de l'observation s'initialise et une invite de confirmation s'affiche sur la machine utilisateur.
2. Demandez à l'utilisateur de cliquer sur **Oui** pour démarrer la machine ou le partage de session.
3. L'administrateur peut uniquement afficher la session observée.

### Observation de VDA Windows

Les sessions de VDA Windows sont observées à l'aide de l'Assistance à distance Windows. Activez la fonction **Assistance à distance de l'utilisateur Windows** lors de l'installation du VDA. Pour de plus amples informations, consultez la section Activer ou désactiver des fonctionnalités.

1. Une fois que vous avez cliqué sur **Observer**, la connexion de l'observation s'initialise et une boîte de dialogue vous invite à ouvrir ou enregistrer le fichier d'incident .msrc.

2. Ouvrez le fichier d'incident avec la Visionneuse de l'Assistance à distance, si elle n'est pas déjà sélectionnée par défaut. Une invite de confirmation s'affiche sur la machine utilisateur.
3. Demandez à l'utilisateur de cliquer sur **Oui** pour démarrer la machine ou le partage de session.
4. Pour un contrôle supplémentaire, demandez à l'utilisateur de partager le contrôle du clavier et de la souris.

#### Optimiser les navigateurs Microsoft Internet Explorer pour l'observation

Configurez votre navigateur Microsoft Internet Explorer pour ouvrir automatiquement le fichier Assistance à distance Microsoft téléchargé (.msra) à l'aide du le client Assistance à distance.

Pour ce faire, vous devez activer le paramètre Demander confirmation pour les téléchargements de fichiers dans l'éditeur de stratégie de groupe :

Configuration ordinateur > Modèles d'administration > Composants Windows > Internet Explorer > Panneau de configuration Internet > Page Sécurité > Zone Internet > Demander confirmation pour les téléchargements de fichiers.

Cette option est activée par défaut pour les sites de la zone d'intranet locale. Si le site Director est en dehors de la zone intranet locale, vous pouvez ajouter manuellement le site à la zone.

## Envoyer des messages aux utilisateurs

June 27, 2024

À partir de Director, envoyez un message à un utilisateur qui est connecté à une ou plusieurs machines. Utilisez cette fonctionnalité pour envoyer des notifications immédiates sur des actions administratives telles que la maintenance de bureau imminente, les fermetures de session et les redémarrages de machine et les réinitialisations de profil.

1. Dans la vue Gestionnaire d'activités, sélectionnez l'utilisateur, puis cliquez sur Détails.
2. Dans la vue Détails de l'utilisateur, situez le panneau Détails de session, puis cliquez sur Envoyer un message.
3. Tapez votre message d'informations dans les champs Objet et Message, puis cliquez sur Envoyer.

Si le message n'est pas envoyé avec succès, un message de confirmation s'affiche dans Director. Le message s'affiche dans la machine de l'utilisateur.

Si le message n'est pas envoyé avec succès, un message d'erreur s'affiche dans Director. Résoudre le problème en fonction du message d'erreur. Lorsque vous avez terminé, tapez l'objet et le texte du message, puis cliquez sur **Réessayer**.

# Résoudre les échecs applicatifs

June 27, 2024

Dans la vue **Gestionnaire d'activités**, cliquez sur l'onglet Applications. Vous pouvez afficher toutes les applications sur toutes les machines auxquelles cet utilisateur a accès, y compris les applications locales et hébergées pour la machine actuellement connectée ainsi que l'état de chacune.

> **Remarque :**
>
> Si l'onglet Applications est grisé, contactez un administrateur avec les permissions nécessaires à l'activation de l'onglet.

La liste contient uniquement ces applications qui ont été lancée dans la session.

Pour les machines avec OS multi-session et les machines avec OS mono-session, les applications sont répertoriées pour chaque session déconnectée. Si l'utilisateur n'est pas connecté, aucune application n'est affichée.

| Action | Description |
| --- | --- |
| Arrêter l'application qui ne répond pas | Choisissez l'application qui ne répond pas et cliquez sur Fermer l'application. Lorsque l'application est arrêtée, demandez à l'utilisateur de la démarrer à nouveau. |
| Arrêter les processus qui ne répondent pas | Si vous avez les permissions requises, cliquez sur l'onglet Processus. Sélectionnez un processus lié à l'application ou qui utilise une quantité importante de ressources UC ou de mémoire, et cliquez sur Mettre fin au processus. Toutefois, si vous ne possédez pas les permissions nécessaires pour mettre fin au processus, une tentative d'arrêt d'un processus échoue. |

| Action | Description |
| --- | --- |
| Redémarrer la machine de l'utilisateur | Pour les machines avec OS mono-session uniquement, pour la session sélectionnée, cliquez sur Redémarrer. Éventuellement, à partir de la vue de Détails de machine, utilisez la puissance des contrôles pour arrêter ou redémarrer la machine. Demandez aux utilisateurs de rouvrir une session afin que vous puissiez vérifier de nouveau l'application. Pour les machines avec OS multi-session, l'option de redémarrage n'est pas disponible. Au lieu de cela, fermez la session de l'utilisateur et laissez l'utilisateur rouvrir une session. |
| Placer la machine en mode de maintenance | Si l'image de la machine nécessite une maintenance, telle que l'installation d'un correctif ou d'autres mises à jour, placez la machine en mode de maintenance. Dans la vue Détails de machine, cliquez sur Détails et activez l'option du mode de maintenance. Informez l'administrateur du problème. |

## Restaurer les connexions aux bureaux

June 27, 2024

Dans Director, vérifiez le statut de connexion de l'utilisateur pour la machine courante dans la barre de titre utilisateur.

Si la connexion au bureau a échoué, l'erreur qui est la cause de l'échec est affichée et peut vous aider à résoudre le problème.

| Action | Description |
| --- | --- |
| Assurez-vous que la machine n'est pas en mode de maintenance. | Sur la page Détails de l'utilisateur, assurez-vous que le mode maintenance est désactivé. |

| Action | Description |
| --- | --- |
| Redémarrer la machine de l'utilisateur | Sélectionnez la machine et cliquez sur **Redémarrer**. Utilisez cette option si la machine de l'utilisateur ne répond pas ou ne peut pas se connecter. Par exemple, lorsque la machine utilise une quantité inhabituellement élevée de ressources CPU, ce qui peut rendre le CPU inutilisable. |

## Restaurer les sessions

June 27, 2024

Si une session devient déconnectée, elle reste active et ses applications continuent d'être exécutées, mais la machine cliente ne communique plus avec le serveur.

Dans la vue Détails de l'utilisateur, résolvez les échecs de session dans le panneau **Détails de la session**. Vous pouvez afficher les détails de la session en cours, indiquée par l'ID de session.

| Action | Description |
| --- | --- |
| Arrêter les applications ou processus qui ne répondent pas | Cliquez sur l'onglet **Applications**. Sélectionnez toute application qui ne répond pas et cliquez sur **Arrêter l'application**. Sélectionnez également un processus correspondant qui ne répond pas et cliquez sur **Arrêter le processus**. Mettez également fin aux processus qui consomment une quantité de mémoire ou de ressources UC anormalement élevée, ce qui peut rendre le processeur inutilisable. |
| Déconnecter la session Windows | Cliquez sur **Contrôle de la session**, puis sélectionnez **Déconnecter**. Cette option est uniquement disponible pour les machines avec OS multi-session avec broker. Pour les sessions sans broker, l'option est désactivée. |
| Déconnexion de la session de l'utilisateur | Cliquez sur **Contrôle de la session**, puis sélectionnez **Fermer la session**. |

Pour tester la session, l'utilisateur peut essayer de la rouvrir. Vous pouvez également observer l'utilisateur pour surveiller plus étroitement cette session.

## Exécuter des rapports système sur le canal HDX

June 27, 2024

Dans la vue **Détails de l'utilisateur**, vérifiez le statut des canaux HDX sur la machine de l'utilisateur dans le panneau **HDX**. Ce panneau est disponible uniquement si la machine utilisateur est connectée à l'aide de HDX.

Si un message s'affiche indiquant que les informations ne sont pas disponibles actuellement, patientez une minute afin que la page s'actualise, ou sélectionnez le bouton **Actualiser**. Les données HDX nécessitent un peu plus de temps pour être mises à jour que d'autres données.

Cliquez sur une icône d'erreur ou d'avertissement pour plus d'informations.

> Conseil :
>
> Vous pouvez afficher des informations sur les autres canaux dans la même boîte de dialogue en cliquant sur les flèches gauche situées dans le coin gauche de la barre de titre.

Les rapports du système de canal HDX sont principalement utilisés par le support technique Citrix pour résoudre davantage de problèmes.

1. Dans le panneau HDX, cliquez sur Télécharger le rapport système.
2. Vous pouvez afficher ou enregistrer le fichier de rapport .xml.
    - Pour afficher le fichier .xml, cliquez sur Ouvrir. Le fichier .xml s'affiche dans la même fenêtre que l'application Director.
    - Pour enregistrer le fichier .xml, cliquez sur Enregistrer. La fenêtre Enregistrer sous s'affiche, vous invitant à entrer un emplacement sur la machine Director dans lequel télécharger le fichier.

## Réinitialiser un profil utilisateur

June 27, 2024

> **ATTENTION :**
>
> Lorsqu'un profil est réinitialisé, les dossiers et les fichiers de l'utilisateur sont enregistrés et copiés dans le nouveau profil. Toutefois, la plupart des données de profil utilisateur ne sont pas incluses (par exemple, le registre est réinitialisé et les paramètres d'application peuvent être supprimés).

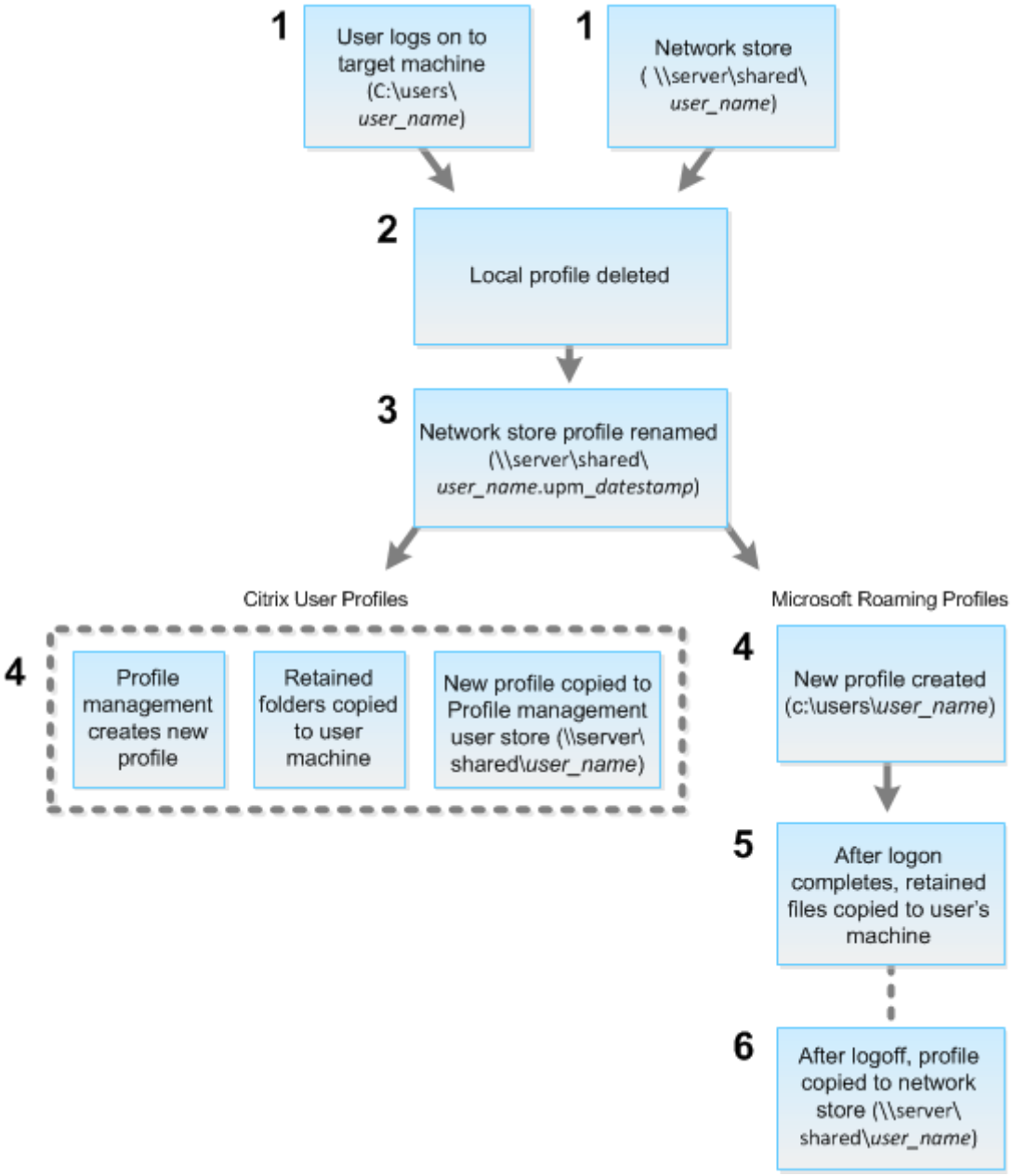
La fonction de réinitialisation s'applique à la fois aux solutions de profil basées sur des fichiers et basées sur des conteneurs.

### Comment les profils réinitialisés sont traités

Tout profil utilisateur Citrix ou profil itinérant Microsoft peut être réinitialisé. Lorsque l'utilisateur ferme sa session et que vous sélectionnez la commande de réinitialisation (dans Director ou en utilisant le kit de développement PowerShell), Director identifie d'abord le profil utilisateur en cours d'utilisation et délivre une commande de réinitialisation appropriée. Director reçoit les informations au travers de Profile Management, y compris les informations sur la taille, le type et la durée d'ouverture de session du profil.

Ce diagramme illustre le processus qui suit la connexion de l'utilisateur, lorsqu'un profil utilisateur est réinitialisé.




La commande de réinitialisation émise par Director spécifie le type de profil. Le service Profile Management, tente ensuite de réinitialiser un profil de ce type et recherche le partage réseau approprié (magasin de l'utilisateur). Si l'utilisateur est traité par Profile Management, mais reçoit une commande de profil itinérant, elle est rejetée (et vice versa).

1. Si un profil local est présent, il est supprimé.
2. Le profil réseau est renommé.
3. L'action suivante dépend du fait que le profil en cours de réinitialisation est un profil utilisateur Citrix ou un profil itinérant Microsoft.

Pour les profils utilisateur Citrix, le nouveau profil est créé à l'aide des règles d'importation Profile Management. Les dossiers sont de nouveau copiés dans le profil réseau et l'utilisateur peut se connecter normalement. Si un profil itinérant est utilisé pour la réinitialisation, tous les paramètres de registre du profil itinérant sont conservés dans le profil de réinitialisation. Vous pouvez configurer Profile Management de manière à ce qu'un profil modèle remplace le profil itinérant, si nécessaire.

Pour les profils itinérants Microsoft, un profil est créé par Windows, et lorsque l'utilisateur ouvre une session, les dossiers sont copiés vers la machine utilisateur. Lorsque l'utilisateur ferme une session, le profil est copié sur le magasin réseau.

### Pour réinitialiser un profil utilisateur dans Director

Si vous utilisez Citrix Virtual Desktops (VDA de bureau), procédez comme suit :

1. À partir de **Director**, recherchez l'utilisateur dont vous voulez réinitialiser le profil et sélectionnez la session de cet utilisateur.
2. Cliquez sur **Réinitialiser le profil**.
3. Demandez à l'utilisateur de fermer toutes ses sessions.
4. Demandez à l'utilisateur de rouvrir une session.
   Les dossiers et fichiers qui ont été enregistrés depuis le profil de l'utilisateur sont copiés dans le nouveau profil.

Si vous utilisez Citrix Virtual Desktops (VDA de serveur), vous devez être connecté pour réinitialiser le profil. L'utilisateur doit ensuite se déconnecter et se reconnecter pour terminer la réinitialisation du profil.

> **Important :**
>
> Si l'utilisateur possède des profils sur des plates-formes multiples (telles que Windows 8 et Windows 7), demandez à l'utilisateur de rouvrir une session tout d'abord sur le même bureau ou application que l'utilisateur a signalé comme un problème. Cette opération d'ouverture de session garantit que le profil approprié est réinitialisé. Si le profil est un profil utilisateur Citrix, le profil est déjà réinitialisé lorsque le bureau de l'utilisateur s'affiche. Si le profil est un profil itinérant Microsoft, la restauration du dossier est peut-être toujours en cours d'exécution pendant un court instant. L'utilisateur doit rester connecté jusqu'à ce que la restauration soit terminée.

Si le profil n'est pas correctement réinitialisé (par exemple, l'utilisateur ne peut pas correctement ouvrir une session à nouveau sur la machine ou certains fichiers sont manquants), vous devez manuellement restaurer le profil d'origine.

Notez les points suivants :

- Si le magasin de l'utilisateur est activé en tant que solution de gestion des profils utilisateur, le nouveau profil contient les dossiers personnels suivants provenant du profil utilisateur d'origine :
  - Bureau
  - Cookies
  - Favoris
  - Mes documents
  - Mes images
  - Ma musique
  - Mes vidéos
- Si le conteneur de profils Citrix Management est activé en tant que solution de gestion des profils utilisateur complète, le nouveau profil ne contient pas les dossiers personnels précédents.
- Dans Windows 8 ou version ultérieure, les cookies ne sont pas copiés sur le nouveau profil lorsque les profils sont réinitialisés.

### Pour restaurer un profil manuellement après un échec de réinitialisation

1. Demandez à l'utilisateur de fermer toutes ses sessions.
2. Supprimez le profil local s'il en existe un.
3. Recherchez le dossier archivé sur le partage réseau contenant la date et l'heure ajoutées au nom du dossier, le dossier avec une extension .upm_horodatage.
4. Supprimez le nom du profil actuel. Autrement dit, celui sans l'extension upm_horodatage.
5. Renommez le dossier archivé en utilisant le nom du profil d'origine. Autrement dit, supprimez l'extension avec la date et l'heure. Vous avez retourné le profil à son état d'origine, pré-réinitialisation.

### Pour réinitialiser un profil à l'aide du SDK PowerShell

Vous pouvez réinitialiser un profil à l'aide du SDK Broker PowerShell.

#### New-BrokerMachineCommand

Crée une commande de mise en file d'attente pour la mise à disposition à un utilisateur, une session ou une machine spécifique. Pour plus d'informations sur cette applet de commande, voir https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/.

#### Exemples

Consultez les exemples suivants pour plus de détails sur l'utilisation des applets de commande PowerShell pour réinitialiser un profil :

Réinitialiser un profil Profile Management

- Supposons que vous souhaitiez réinitialiser le profil pour user1. Utilisez la commande PowerShell New-BrokerMachineCommand. Par exemple :

  ```
  - New-BrokerMachineCommand -Category UserProfileManager -CommandName
    "ResetUpmProfile"-DesktopGroups 1 -CommandData $byteArray -
    SendTrigger logon -user domain1\user1
  ```

> **Important :**
>
> L'élément `CommandData $byteArray` doit être au format suivant : `<SID>[,<backup path>]`. Si vous ne fournissez pas le chemin de sauvegarde, Profile Management génère un dossier de sauvegarde nommé avec la date et l'heure actuelles.

Réinitialiser un profil itinérant Windows

- Supposons que vous souhaitiez réinitialiser le profil itinérant pour user1. Utilisez la commande PowerShell New-BrokerMachineCommand. Par exemple :

  ```
  - New-BrokerMachineCommand -Category UserProfileManager -CommandName
    "ResetRoamingProfile"-DesktopGroups 1 -CommandData $byteArray
    -SendTrigger logon -user domain1\user1
  ```

## Enregistrer les sessions

June 27, 2024

Vous pouvez enregistrer les sessions ICA à l'aide des contrôles d'enregistrement de session sur l'écran **Détails de l'utilisateur** et **Détails de la machine** dans Director. Cette fonctionnalité est disponible pour les clients de sites **Premium**.

### Enregistrement de session dynamique

Vous pouvez enregistrer la session active en cours à l'aide des commandes d'enregistrement de session de l'écran **Détails de l'utilisateur**. Pour en savoir plus sur l'enregistrement dynamique de session, consultez l'article sur le service d'enregistrement de session.

## Enregistrement de session basé sur des stratégies

Pour configurer l'enregistrement de session sur Director selon la stratégie à l'aide de l'outil DirectorConfig, consultez la section **Configurer Director pour utiliser le serveur d'enregistrement de session** dans Configurer des stratégies d'enregistrement de session.
Les contrôles d'enregistrement de session sont disponibles dans Director uniquement si l'utilisateur connecté dispose du droit de modifier les stratégies d'enregistrement de session. Ce droit peut être défini sur la Console d'autorisation d'enregistrement de session, comme décrit dans Autoriser les utilisateurs.

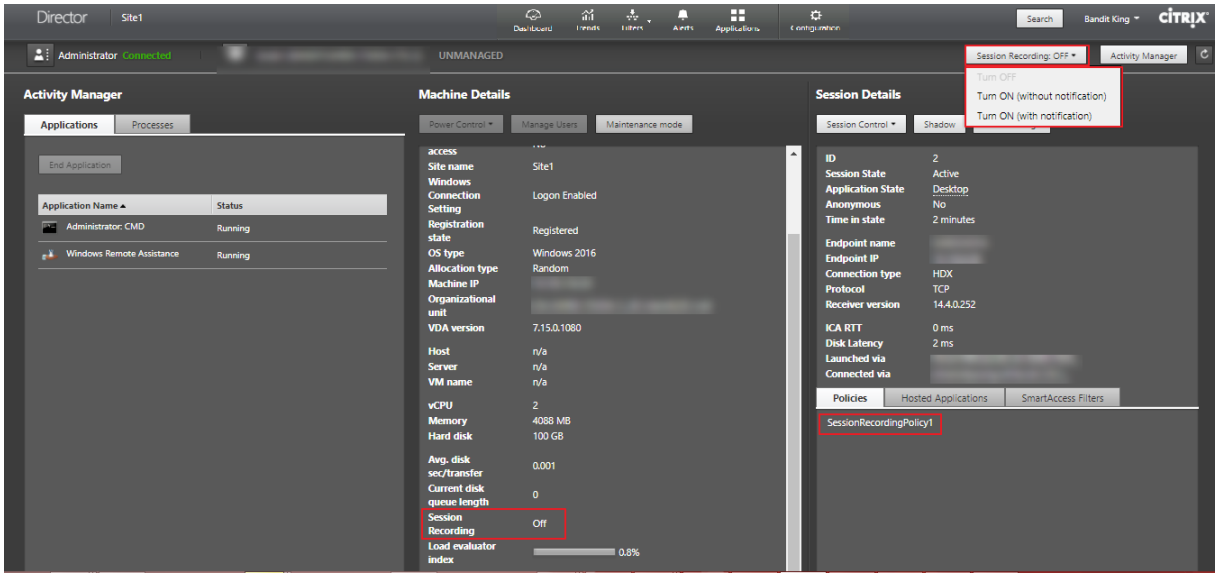
> **Remarque :**
> Les modifications apportées aux paramètres d'enregistrement de session depuis Director ou la Console de stratégie d'enregistrement de session prennent effet à partir de la session ICA suivante.

## Contrôles d'enregistrement de session dans Director

Vous pouvez utiliser les actions **Détails utilisateur** > **Enregistrement de session** pour enregistrer les sessions en cours ou suivantes.

- Activez l'enregistrement dynamique des sessions : la session en cours est enregistrée.
- Activer (avec notification) : les sessions suivantes sont enregistrées et l'utilisateur est averti de l'enregistrement de la session lorsqu'il ouvre une session ICA.
- Activer (sans notification) : les sessions suivantes sont enregistrées et la session est enregistrée de façon silencieuse sans avertir l'utilisateur.
- Désactiver : désactive l'enregistrement des sessions pour l'utilisateur.

Le panneau **Stratégies** affiche le nom de la stratégie d'enregistrement de session active.



Le panneau **Détails de la machine** affiche l'état de la stratégie d'enregistrement de session pour la machine.

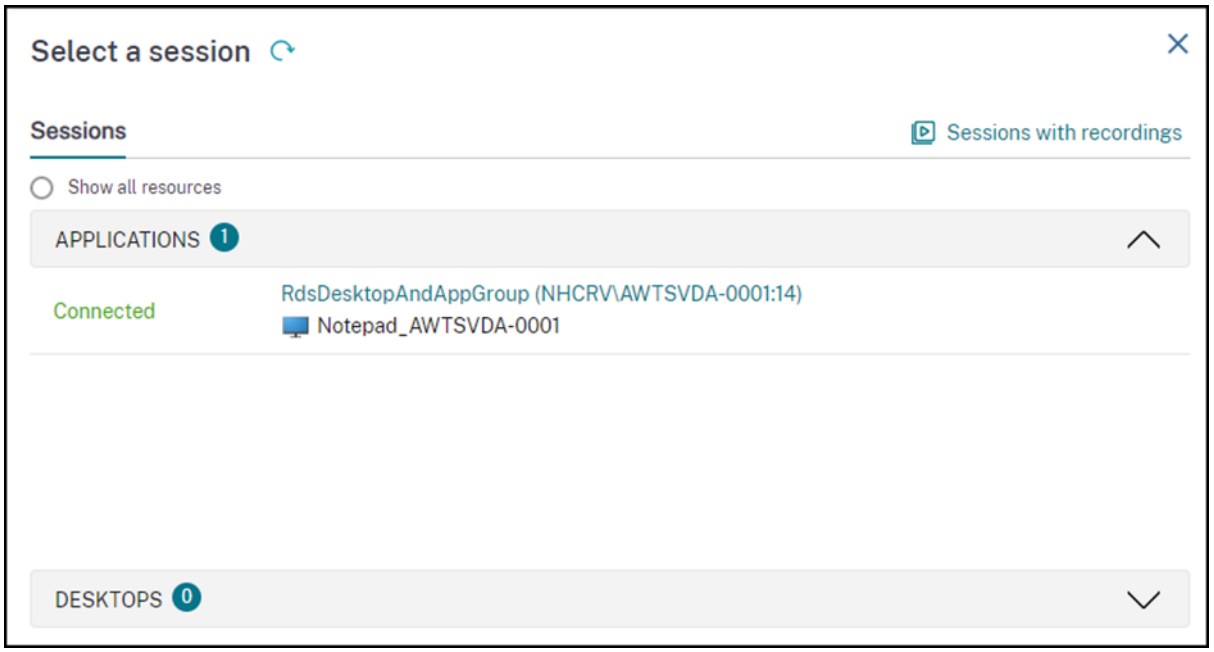
### Visionnez les sessions en direct et enregistrées

Vous pouvez visionner des sessions utilisateur enregistrées et en direct pour comprendre les problèmes rencontrés par l'utilisateur. Avec l'accès rapide aux enregistrements et aux mesures relatives aux sessions dans la console Director, vous n'avez plus besoin de rechercher les enregistrements sur plusieurs serveurs d'enregistrement de session ou de rechercher des applications tierces pour les visualiser. Il permet de relier les problèmes découverts dans les enregistrements avec les mesures de performance.

Cette fonctionnalité nécessite les éléments suivants :

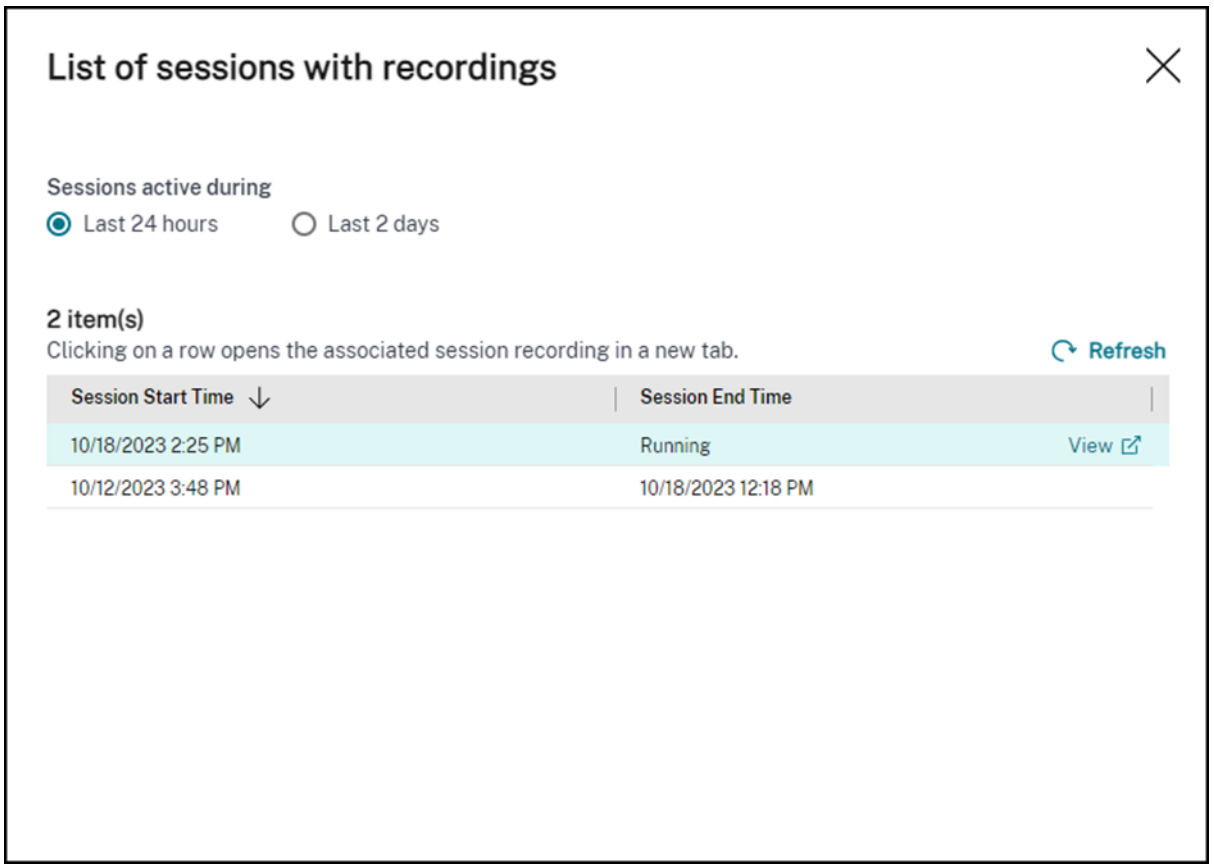
- Le VDA et les serveurs d'enregistrement de session sont sur la version 2308 ou ultérieure.
- Delivery Controller et Director utilisent la version 2311 ou ultérieure.

Director stocke les enregistrements de session dans un référentiel centralisé. La liste des enregistrements appartenant à l'utilisateur s'affiche en cliquant sur le lien modal **Sélecteur de session** > **Sessions avec enregistrements**.




Vous pouvez choisir d'afficher les enregistrements des sessions qui ont été actives au cours des dernières 24 heures ou des 2 derniers jours. Les enregistrements en direct des sessions actuellement actives sont marqués avec **l'heure de fin de session** comme étant **en cours**.




Cliquez sur le lien **Afficher** pour visionner l'enregistrement dans un nouvel onglet à l'aide du serveur de lecture Citrix Session Recording.

## Tableau de compatibilité des fonctionnalités

June 27, 2024

Citrix Director 7 2203 est compatible avec :

- Citrix Virtual Apps and Desktops 7 2112 et versions ultérieures
- Citrix Virtual Apps and Desktops 7 1912 LTSR

Dans chaque site, bien que vous puissiez utiliser Director avec des versions antérieures de Delivery Controller, certaines fonctionnalités de la version la plus récente de Director risquent de ne pas être disponibles. Citrix vous recommande d'installer les mêmes versions pour Director, Delivery Controller et VDA.

> **Remarque :**
>
> Après avoir mis à niveau un Delivery Controller, vous êtes invité à mettre à niveau le site lorsque

> vous ouvrez Studio. Pour plus d'informations, veuillez consulter la section **Séquence de mise à niveau** dans Mettre un déploiement à niveau.

La première fois que vous ouvrez une session après une mise à niveau de Director, une vérification de version est effectuée sur les sites configurés. Si un site exécute une version du Controller antérieure à celle de Director, un message apparaît sur la console Director, recommandant une mise à niveau du site. En outre, tant que la version du site est antérieure à celle de Director, une note continue à s'afficher dans le tableau de bord de Director indiquant cette incompatibilité.

> **Remarque :**
>
> Les versions antérieures de Citrix Director n'affichent pas les stratégies appliquées aux sessions utilisateur exécutées sur des versions récentes de VDA. Citrix Director 1912 et versions antérieures n'affichent pas les stratégies appliquées aux sessions utilisateur exécutées sur les versions VDA 2003 et ultérieures. Utilisez Citrix Director versions 2003 et ultérieures pour afficher ces stratégies.

Le tableau ci-dessous dresse la liste des fonctionnalités spécifiques de Director et de la version minimale de Delivery Controller (DC), VDA et autres composants dépendants requis ainsi que l'édition de la licence.

| Version de Director | Fonctionnalité | Dépendances - version min requise | Édition |
|---|---|---|---|
| 2311 | Visionnez les sessions en direct et enregistrées | VDA 2308 et DDC 2311 | Tous |
| 2311 | Topologie de session | Aucun | Tous |
| 2311 | Résolution d'écran optimale | Aucun | Tous |
| 2311 | Optimisation de MS Teams | VDA 2311 et dernière version de DDC | Tous |
| 2311 | Améliorations de la présentation des analyses | Aucun | Tous |
| 2311 | Affichage de la durée d'ouverture de session mis à jour | Aucun | Tous |
| 2308 | Résumé et détails des analyses | Aucun | Tous |

| Version de Director | Fonctionnalité | Dépendances - version min requise | Édition |
|---|---|---|---|
| 2308 | Prise en charge de Citrix Probe Agent pour l'authentification multifacteur Citrix Gateway | Citrix Gateway | Tous |
| 2308 | Désactiver les alertes d'hyperviseur | Aucun | Tous |
| 2308 | Tendances des mesures Expérience de session | Aucun | Tous |
| 2305 | Prise en charge de l' authentification via Citrix Gateway | Aucun | Tous |
| 2305 | Gestion de Autoscale dans Director | Aucun | Tous |
| 2303 | Alerte Machines défectueuses | DC 7 2303 | Premium |
| 2203 | Prise en charge de TLS 1.3 | - | Tous |
| 2212 | Utilisation du GPU en temps réel disponible pour les GPU AMD | DC 7.14 et VDA 7.14 exécutant Windows 64 bits et HDX 3D Pro activés | Tous |
| 2212 | Planification avancée des analyses | DC 7 1906 et Citrix Probe Agent 2209 | Premium |
| 1909 | Configurer des sites locaux avec Citrix Analytics for Performance | DC 7 1906 et VDA 1906 | Tous |
| 1906 | Reconnexion automatique de session | DC 7 1906 et VDA 1906 | Tous |
| 1906 | Durée du démarrage de session | DC 7 1906 et VDA 1903 | Tous |

| Version de Director | Fonctionnalité | Dépendances - version min requise | Édition |
|---|---|---|---|
| 1906 | Analyse de bureaux | DC 7 1906 et Citrix Probe Agent 1903 | Premium |
| 7.9 et versions ultérieures | Durée Citrix Profile Management dans Chargement du profil | VDA 1903 | Tous |
| 1811 | Détails du profil | DC 7 1811 et VDA 1811 | Tous |
| 1811 | Surveillance des alertes d'hyperviseur | DC 7 1811 | Premium |
| 1811 | Analyse d'application | DC 7 1811 et Citrix Application Probe Agent 1811 | Premium |
| 1811 | Intégrité des licences Microsoft RDS | DC 7 1811 et VDA 7.16 | Tous |
| 1811 | Affichage des données RTOP clés | DC 7 1811 et VDA 1808 | Premium |
| 1808 | Exportation de données de filtres | DC 7 1808 | Tous |
| 1808 | Détails de la session interactive | DC 7 1808 et VDA 1808 | Tous |
| 1808 | Détails GPO | DC 7 1808 et VDA 1808 | Tous |
| 1808 | Données historiques de machine disponibles à l'aide de l'API OData | DC 7 1808 | Tous |
| 7.18 | Analyse d'application | DC 7.18 | Premium (anciennement Platinum) |
| 7.18 | Stratégies d'alertes intelligentes | DC 7.18 | Premium (anciennement Platinum) |
| 7.18 | Lien Health Assistant | Aucun | Tous |
| 7.18 | Détails de la session interactive | Aucun | Tous |

| Version de Director | Fonctionnalité | Dépendances - version min requise | Édition |
|---|---|---|---|
| 7.17 | Authentification par carte à puce PIV | Aucun | Tous |
| 7.16 | Analyse des applications | DC 7.16 et VDA 7.15 | Tous |
| 7.16 | OData API V.4 | DC 7.16 | Tous |
| 7.16 | Observation des utilisateurs VDA Linux | VDA 7.16 | Tous |
| 7.16 | Prise en charge des groupes locaux de domaine | Aucun | Tous |
| 7.16 | Accès à la console machine | DC 7.16 | Tous |
| 7.15 | Détection des défaillances applicatives | DC 7.15 et VDA 7.15 | Tous |
| 7.14 | Résolution des problèmes centrée sur les applications | DC 7.13 et VDA 7.13 | Tous |
| 7.14 | Contrôle des disques | DC 7.14 et VDA 7.14 | Tous |
| 7.14 | Suivi GPU | DC 7.14 et VDA 7.14 | Tous |
| 7.13 | Protocole de transport sur le panneau Détails de la session | DC 7.x et VDA 7.13 | Tous |
| 7.12 | Descriptions claires des échecs de connexion et de machine | DC 7.12 et VDA 7.x | Tous |
| 7.12 | Optimisation des données historiques disponibles dans l'édition Enterprise | DC 7.12 et VDA 7.x | Entreprise |

| Version de Director | Fonctionnalité | Dépendances - version min requise | Édition |
|---|---|---|---|
| 7.12 | Rapports personnalisés | DC 7.12 et VDA 7.x | Premium (anciennement Platinum) |
| 7.11 | Rapports d'utilisation des ressources | DC 7.11 et VDA 7.11 | Tous |
| 7.11 | Alertes étendues pour les conditions CPU, mémoire et RTT ICA | DC 7.11 et VDA 7.11 | Premium (anciennement Platinum) |
| 7.11 | Amélioration de l'exportation des rapports | DC 7.11 et VDA 7.x | Tous |
| 7.11 | Intégration avec Citrix ADM | DC 7.11, VDA 7.x et MAS version 11.1 Build 49.16 | Premium (anciennement Platinum) |
| 7.9 | Répartition de la durée d'ouverture de session | DC 7.9 et VDA 7.x | Tous |
| 7.7 | Analyse et alertes proactives | DC 7.7 et VDA 7.x | Premium (anciennement Platinum) |
| 7.7 | Intégration de l'authentification Windows | DC 7.x et VDA 7.x | Tous |
| 7.7 | Utilisation des OS mono-session et multi-session | DC 7.7 et VDA 7.x | Premium (anciennement Platinum) |
| 7.6.300 | Prise en charge du canal virtuel Framehawk | DC 7.6 et VDA 7.6 | Tous |
| 7.6.200 | Intégration d'enregistrement de session | DC 7.6 et VDA 7.x | Premium (anciennement Platinum) |
| 7 | Intégration de HDX Insight | DC 7.6, VDA 7.x et Citrix ADM | Premium (anciennement Platinum) |

# Granularité de données et rétention

June 27, 2024

## Agrégation des valeurs de données

Monitor Service collecte les données, notamment l'utilisation de la session utilisateur, les détails des performances de l'ouverture de session utilisateur, les détails de l'équilibrage de charge de la session, et les informations de connexion et d'échec de machine. Les données sont agrégées différemment en fonction de leur catégorie. La compréhension de l'agrégation des valeurs de données présentées à l'aide de l'API OData Method est critique à l'interprétation des données. Par exemple :

- Les sessions connectées et les échecs de machine se produisent sur une période de temps. Ils sont donc exposés comme valeurs maximales sur une période de temps.
- La durée d'ouverture de session est une mesure de durée, par conséquent elle est exposée en tant que moyenne sur une période de temps.
- Le nombre d'ouvertures de session et les échecs de connexion représentent des nombres d'occurrences sur une période de temps, et par conséquent sont exposés en tant que sommes sur une période de temps.

## Évaluation des données simultanées

Les sessions doivent se chevaucher pour être considérées comme simultanées. Toutefois, lorsque l'intervalle de temps est de 1 minute, toutes les sessions de cette minute (qu'elles se chevauchent ou pas) sont considérées comme simultanées. La taille de l'intervalle est si petite que la surcharge de performance impliquée dans le calcul de la précision ne vaut pas la valeur ajoutée. Si les sessions se produisent dans la même heure, mais pas dans la même minute, elles ne sont pas considérées comme se chevauchant.

## Corrélation de tables de synthèse avec des données brutes

Le modèle de données représente des métriques de deux manières différentes :

- Les tables de synthèse représentent des vues des mesures détaillées de l'agrégation par minute, heure et jour.
- Les données brutes représentent des événements individuels ou l'état actuel de l'objet suivi dans la session, la connexion, l'application et autres objets.

Lorsque vous tentez de corréler les données dans les appels API ou dans le modèle de données lui-même, il est important de bien comprendre les concepts et les limitations suivantes :

- **Aucune données de synthèse pour les intervalles partiels.** Des résumés de métriques sont conçus pour répondre aux besoins de tendances historiques sur de longues périodes. Les métriques sont agrégées dans la table de synthèse pour effectuer des intervalles. Il n'y a pas de données de synthèse pour un intervalle partiel au début (les plus anciennes données disponibles) de la collection de données ni à la fin. Lorsque vous affichez les agrégations d'une journée (intervalle = 1 440), ceci signifie que la premier et le dernier jour incomplet ne possède pas de données. Bien que des données brutes puissent exister pour des intervalles partiels, elles ne sont jamais synthétisées. Vous pouvez déterminer le premier et le dernier intervalle d'agrégation pour une granularité de données particulière en extrayant les valeurs minimales et maximales de SummaryDate pour une table de synthèse particulière. La colonne SummaryDate représente le début de l'intervalle. La colonne Granularité représente la durée de l'intervalle pour les données agrégées.
- **Corrélation par heure.** Les métriques sont agrégées dans la table de synthèse pour terminer les intervalles comme décrit dans la section précédente. Ils peuvent être utilisés pour les tendances historiques, mais les événements bruts peuvent être plus actifs dans l'état de ce qui a été résumé pour l'analyse de tendances. Toute comparaison temporelle d'un résumé aux données brutes doit tenir compte du fait qu'il n'existe pas de données récapitulatives pour des intervalles partiels qui pourraient se produire ou pour le début et la fin de la période.
- **Événements manqués et latents.** Les mesures qui sont agrégées dans la table de synthèse peuvent être légèrement inexactes si les événements sont manqués ou latents pour la période d'agrégation. Bien que Monitor Service tente de conserver un état courant précis, il ne retourne pas dans le temps pour recalculer l'agrégation dans les tables de synthèse pour les événements manqués ou latents.
- **Haute disponibilité de connexion.** Lors de la haute disponibilité de connexion, il existera des espaces dans les données de synthèse du nombre de connexions actives, mais les instances de session seront toujours en cours d'exécution dans les données brutes.
- **Périodes de rétention des données.** Les données des tables de synthèse sont conservées sur un programme de nettoyage différent du programme des données brutes d'événement. Il se peut que les données soient manquantes, car elles ont été effacées depuis les tables de données de synthèse ou brutes. Les périodes de rétention peuvent également différer pour différentes granularités de données de synthèse. Les données de granularité inférieures (en minutes) sont nettoyées plus rapidement que les données de granularité supérieures (en jours). Si des données sont manquantes dans une granularité à cause du nettoyage, elles peuvent être détectées dans une meilleure granularité. Étant donné que les appels API retournent uniquement la granularité demandée, l'absence de réception de données pour un niveau de granularité ne signifie pas que les données n'existent pas pour une meilleure granularité pour la même période.
- **Fuseaux horaires.** Les métriques sont stockées avec des horodatages UTC. Les tables de syn-

thèse sont regroupées sur des limites de fuseau horaire. Pour les zones qui ne se trouvent pas dans les limites horaires, il se peut qu'il existe une différence pour laquelle les données sont agrégées.

### Granularité et rétention

La granularité des données agrégées récupérées par Director est une fonction de la période de temps (T) demandée. Les règles sont les suivantes :

- 0 < T <= 1 heure - utilise une granularité minute par minute
- 0 < T <= 30 jours - utilise une granularité heure par heure
- T > 31 jours - utilise une granularité jour par jour

Les données requises qui ne proviennent pas de données agrégées proviennent de la session brute et des informations de connexion. Ces données ont tendance à croître rapidement, et par conséquent, disposent de leur propre paramètre de nettoyage. Le nettoyage garantit que seules les données appropriées sont conservées à long terme. Le nettoyage garantit de meilleures performances tout en conservant la granularité nécessaire pour la création de rapports. Les clients sur sites avec licence Premium peuvent modifier la rétention de nettoyage sur leur nombre de jours de rétention désirés, sinon, la valeur par défaut est utilisée. En cas de perte de connectivité avec la base de données du site, Monitor Service utilisera les jours de rétention par défaut pour les droits Premium, comme indiqué dans le tableau ci-dessous.

Pour accéder aux paramètres, exécutez les commandes PowerShell suivantes sur le Delivery Controller :

```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>
<!--NeedCopy-->
```

| | Nom du paramètre | Nettoyage affecté | Jours de rétention pour Premium | Jours de rétention pour Advanced |
|---|---|---|---|---|
| 1 | GroomSessionsRetentionDays | Rétention des enregistrements de session et de connexion après la fermeture de session | 90 | 31 |
| 2 | GroomFailuresRetentionDays | Enregistrements MachineFailureLog et ConnectionFailureLog | 90 | 31 |
| 3 | GroomLoadIndexesRetentionDays | Enregistrements LoadIndex | 90 | 31 |
| 4 | GroomDeletedRetentionDays | Les enregistrements Machine, Catalog, DesktopGroup et Hypervisor qui possèdent un LifecycleState « Supprimé ». Ce paramètre supprime également tout enregistrement Session, SessionDetail, Summary, Failure ou LoadIndex. | 90 | 31 |

| | | Nom du paramètre | Nettoyage affecté | Jours de rétention pour Premium | Jours de rétention pour Advanced |
|---|---|---|---|---|---|
| | 5 | GroomSummariesRegistrationDays | Enregistrement Desktop-GroupSummary, FailureLogSummary et LoadIndexSummary. Données agrégées : granularité quotidienne. | 365 | 31 |
| | 6 | GroomMachineHotfixLogRetentionDays | Correctifs à chaud appliquées aux machines VDA et Controller | 90 | 31 |
| | 7 | GroomMinuteRetentionDays | Données agrégées : granularité par minute | 3 | 3 |
| | 8 | GroomHourlyRetentionDays | Données agrégées : granularité horaire | 32 | 31 |
| | 9 | GroomApplicationInstanceRetentionDays | Historique des instances d'application | 90 | Non applicable |
| | 10 | GroomNotificationLogRetentionDays | Enregistrement de journal de notification | 90 | Non applicable |

| | Nom du paramètre | Nettoyage affecté | Jours de rétention pour Premium | Jours de rétention pour Advanced |
|---|---|---|---|---|
| 11 | GroomResourceUsageRawDataRetentionDays | Daily Raw data | 3 | 3 |
| 12 | GroomResourceUsageMinuteDataRetentionDays | Daily Minute data | 7 | 7 |
| 13 | GroomResourceUsageHourDataRetentionDays | Daily Hour data | 30 | 30 |
| 14 | GroomResourceUsageDayDataRetentionDays | Daily Day data | 365 | 31 |
| 15 | GroomProcessUsageRawDataRetentionDays | Daily Raw data | 1 | 1 |
| 16 | GroomProcessUsageMinuteDataRetentionDays | Daily Minute data | 3 | 3 |

| | Nom du paramètre | Nettoyage affecté | Jours de rétention pour Premium | Jours de rétention pour Advanced |
|---|---|---|---|---|
| 17 | GroomProcessUsageHourDataRetentionDays | Données d'utilisation des processus : granularité par heure | 7 | 7 |
| 18 | GroomProcessUsageDayDataRetentionDays | Données d'utilisation des processus : granularité par jour | 30 | 30 |
| 19 | GroomSessionMetricsDataRetentionDays | Données de mesure de session | 1 | 1 |
| 20 | GroomMachineMetricsDataRetentionDays | Données de mesure de machine | 3 | 3 |
| 21 | GroomMachineMetricsSummaryDataRetentionDays | Données de synthèse de mesure de machine | 365 | 31 |
| 22 | GroomApplicationErrorDataRetentionDays | Données d'erreur d'application | 1 | 1 |
| 23 | GroomApplicationFailureDataRetentionDays | Données d'échec d'application | 1 | 1 |

> **Attention :**
>
> La modification des valeurs de la base de données de Monitor Service nécessite le redémarrage du service pour que les nouvelles valeurs prennent effet. Vous êtes invités à apporter des modifications à la base de données de Monitor Service uniquement avec l'assistance de Citrix.

Les paramètres GroomProcessusAgeRawDataRetentionDays, GroomResourceUsageRawDataRetentionDays et GroomSessionMetricsDataRetentionDays sont limités à leurs valeurs par défaut de 1, tandis que GroomProcessusAgeMinuteDataRetentionDays est limité à sa valeur par défaut de 3. Les commandes PowerShell permettant de définir ces valeurs ont été désactivées, car les données d'

utilisation du processus ont tendance à croître rapidement.
En outre, les paramètres de rétention basés sur les licences sont les suivants :

- **Sites sous licence Premium :** la rétention de nettoyage pour tous les paramètres est limitée à 1000 jours (Citrix recommande 365 jours).
- **Sites sous licence Advanced :** la rétention de nettoyage est limitée à 31 jours pour tous les paramètres.
- **Tous les autres sites :** la rétention de nettoyage est limitée à 7 jours pour tous les paramètres.

**Exceptions :**

- GroomApplicationInstanceRetentionDays ne peut être défini que dans les sites sous licence Premium.
- GroomApplicationErrorsRetentionDays et GroomApplicationFaultsRetentionDays sont limités à 31 jours dans les sites sous licence Premium.

La conservation de données pendant de longues périodes a les conséquences suivantes sur la taille des tables :

- **Données horaires.** Si les données horaires sont autorisées à rester dans la base de données pour un maximum de deux années, un site de 1 000 groupes de mise à disposition peut influencer la croissance de la base de données comme suit :

  1 000 groupes de mise à disposition x 24 heures/jour x 365 jours/an x 2 ans = 17 520 000 lignes de données. L'impact sur les performances d'une telle quantité importante de données dans les tables d'agrégation est significatif. Étant donné que les données du tableau de bord sont tirées de cette table, la configuration requise sur le serveur de base de données peut être importante. Il se peut que des quantités excessives de données aient un impact dramatique sur les performances.

- **Données de session et d'événement.** Données collectées chaque fois qu'une session est démarrée et qu'une connexion/reconnexion est effectuée. Pour un site important (100 000 utilisateurs), ces données s'accroissent très rapidement. Par exemple, l'équivalent de deux ans de tables rassemblerait plus d'un To de données nécessitant une base de données d'entreprise de haut au niveau.

## Dépannage et raison des échecs de Citrix Director

June 27, 2024

Les tableaux suivants décrivent les différentes catégories d'échec, les raisons et les mesures à prendre pour résoudre les problèmes. Pour plus d'informations, voir Valeurs d'énumération, codes d'erreur

et descriptions.

### Erreurs liées aux échecs de connexion

| Catégorie | Raison | Problème | Action |
|---|---|---|---|
| S/O | [0] Unknown. Ce code d'erreur n'est pas mappé. | Le Monitoring Service ne peut pas déterminer la raison de l'échec de lancement ou de connexion signalé à partir des informations partagées par le Broker Service. | Collectez les journaux CDF sur le Delivery Controller et contactez le support Citrix. |
| [0] None | [1] None | Aucun | S/O |
| [2] MachineFailure | [2] SessionPreparation | Échec de la demande de préparation d'une session envoyée par le Delivery Controller au VDA. Causes possibles : problèmes de communication entre le Delivery Controller et le VDA ; problèmes rencontrés par le Broker Service lors de la création d'une demande de préparation ; problèmes réseau entraînant le refus de la demande par le VDA. | Reportez-vous aux instructions de dépannage indiquées dans l'article du centre de connaissances, Dépannage de l'enregistrement de VDA auprès de Delivery Controller dans Virtual Apps and Desktops, pour plus d'informations sur les problèmes courants de communication entre le Delivery Controller et le VDA. |

| Catégorie | Raison | Problème | Action |
| --- | --- | --- | --- |
| [2] MachineFailure | [3] RegistrationTimeout | Le VDA a été lancé, mais un délai a été dépassé lors de sa tentative d'enregistrement auprès du Delivery Controller. | Vérifiez que le Citrix Broker Service est exécuté sur le Delivery Controller et que le Desktop Service est exécuté sur le VDA. Si ces services sont arrêtés, démarrez-les. |
| [1] ClientConnection-Failure | [4] ConnectionTimeout | Le client ne s'est pas connecté au VDA après que ce dernier ait été préparé pour le lancement de la session. La session a été négociée avec succès, mais un délai d'attente a été dépassé lors la connexion du client au VDA. Causes possibles : paramètres de pare-feu ; interruptions réseau ; paramètres qui empêchent les connexions à distance. | Consultez la console Director pour vérifier que le client dispose d'une connexion active, ce qui signifie qu'aucun utilisateur n'est affecté. Si aucune session n'existe, vérifiez les journaux d'événements sur le client et sur le VDA pour détecter toute erreur. Résolvez tous les problèmes de connectivité réseau entre le client et le VDA. |

| Catégorie | Raison | Problème | Action |
| --- | --- | --- | --- |
| [4] NoLicensesAvailable | [5] Licensing | La demande de licences a échoué. Causes possibles : nombre insuffisant de licences ; serveur de licences en panne depuis plus de 30 jours. | Vérifiez que le serveur de licences est en ligne et accessible. Réglez les problèmes de connectivité réseau éventuels avec le serveur de licences ou redémarrez le serveur de licences s'il semble ne pas fonctionner correctement. Vérifiez qu'il existe suffisamment de licences dans l'environnement et allouez-en davantage si nécessaire. |

| Catégorie | Raison | Problème | Action |
| --- | --- | --- | --- |
| [1] ClientConnection-Failure | [6] Ticketing | Une erreur s'est produite lors de la création de tickets. Elle indique que la connexion du client au VDA ne correspond pas à la demande négociée. Un ticket de demande de lancement est préparé par le broker et délivré dans le fichier ICA. Lorsqu'un utilisateur tente de lancer une session, le VDA valide le ticket de lancement dans le fichier ICA auprès du broker. Causes possibles : le fichier ICA est endommagé ; l'utilisateur tente d'établir une connexion non autorisée. | Vérifiez que l'utilisateur a accès à l'application ou au bureau en fonction des groupes d'utilisateurs définis dans les groupes de mise à disposition. Demandez à l'utilisateur de relancer l'application ou le bureau de manière à déterminer s'il s'agit d'un problème isolé. Si le problème persiste, recherchez la présence d'erreurs dans les journaux d'événements de la machine cliente. Vérifiez que le VDA auquel l'utilisateur essaye de se connecter est enregistré. S'il n'est pas enregistré, consultez les journaux d'événements sur le VDA et corrigez les problèmes liés à l'enregistrement. |

| Catégorie | Raison | Problème | Action |
| --- | --- | --- | --- |
| [1] ClientConnection-Failure | [7] Other | Le VDA a signalé la fermeture d'une session après que le client ait initialement contacté le VDA, mais avant qu'il ne puisse compléter la séquence de connexion. | Vérifiez que la session n'a pas été fermée par l'utilisateur avant le lancement. Essayez de relancer la session. Si le problème persiste, collectez les journaux CDF et contactez le support Citrix. |
| [1] ClientConnection-Failure | [8] GeneralFail | Impossible de lancer la session. Causes possibles : un lancement de session avec broker a été demandé alors que le broker était toujours en phase de démarrage ou d'initialisation ; une erreur interne s'est produite lors de la phase de négociation d'un lancement. | Vérifiez que le Citrix Broker Service est exécuté et essayez de relancer la session. |
| [5] Configuration | [9] MaintenanceMode | Le VDA ou le groupe de mise à disposition auquel le VDA appartient est en mode de maintenance. | Déterminez si le mode de maintenance est requis. Désactivez le mode de maintenance sur le groupe de mise à disposition ou la machine en question s'il n'est pas requis et demandez à l'utilisateur d'essayer de se reconnecter. |

| Catégorie | Raison | Problème | Action |
| --- | --- | --- | --- |
| [5] Configuration | [10] ApplicationDisabled | L'application a été désactivée par l'administrateur, par conséquent les utilisateurs ne peuvent pas y accéder. | Si l'application est destinée à être utilisée dans un environnement de production, activez l'application et demandez à l'utilisateur de se reconnecter. |
| [4] NoLicensesAvailable | [11] LicenseFeature Refused | La fonctionnalité utilisée n'est pas couverte par les licences existantes. | Contactez un représentant commercial Citrix pour vérifier les fonctionnalités qui sont couvertes par le type et l'édition de la licence de Citrix Virtual Apps and Desktops. |

| Catégorie | Raison | Problème | Action |
| --- | --- | --- | --- |
| [3] NoCapacityAvailable | [13] SessionLimitReached | Tous les VDA sont utilisés et la capacité actuelle ne permet pas d'héberger des sessions supplémentaires. Causes possibles : tous les VDA sont utilisés (pour les VDA avec OS mono-session) ; tous les VDA ont atteint le nombre maximal de sessions simultanées autorisées (pour les VDA avec OS multi-session). | Vérifiez s'il existe des VDA en mode de maintenance. Désactivez le mode de maintenance s'il n'est pas requis pour libérer de la capacité supplémentaire. Envisagez d'augmenter le paramètre de stratégie Citrix **Nombre maximum de sessions**, ce qui permettra d'accommoder plus de sessions par VDA de serveur. Envisagez d'ajouter des VDA avec OS multi-session supplémentaires. Envisagez d'ajouter des VDA avec OS mono-session supplémentaires. |

| Catégorie | Raison | Problème | Action |
| --- | --- | --- | --- |
| [5] Configuration | [14] DisallowedProtocol | Les protocoles ICA et RDP ne sont pas autorisés. | Exécutez la commande PowerShell **Get-BrokerAccessPolicyRule** sur un Delivery Controller et vérifiez que les protocoles souhaités sont tous répertoriés dans la valeur **AllowedProtocols**. Ce problème se produit uniquement lorsqu'une configuration est incorrecte. |
| [5] Configuration | [15] ResourceUnavailable | L'application ou le bureau auquel l'utilisateur tente de se connecter n'est pas disponible. Il est possible que cette application ou ce bureau n'existe pas ou qu'aucun VDA ne soit disponible pour l'exécuter. Causes possibles : la publication de l'application ou du bureau a été annulée ; le VDA hébergeant l'application ou le bureau a atteint sa charge maximale ; l'application ou le bureau sont en mode de maintenance. | Vérifiez que l'application ou le bureau sont toujours publiés et que les VDA ne sont pas en mode de maintenance. Déterminez si les VDA avec OS multi-session ont atteint leur charge maximale. Si c'est le cas, provisionnez des VDA multi-session supplémentaires. Vérifiez que des VDA avec OS mono-session sont disponibles pour les connexions. Provisionnez des VDA avec OS mono-session supplémentaires au besoin. |

| Catégorie | Raison | Problème | Action |
|---|---|---|---|
| [5] Configuration | [16] ActiveSessionRe-connectDisabled | La session ICA est active et connectée à un point de terminaison différent. Toutefois la **reconnexion aux sessions actives** étant désactivée, le client ne peut pas se connecter à la session active. | Sur le Delivery Controller, vérifiez que la **reconnexion aux sessions actives** est activée. Sous **HKEY_LOCAL_MACHINE\Software** vérifiez que la valeur de registre **DisableActiveSes-sionReconnect** est définie sur 0. |
| [2] MachineFailure | [17] NoSessionToRe-connect | Le client a tenté de se reconnecter à une session spécifique, mais la session a été fermée. | Essayez de vous reconnecter au contrôle de l'espace de travail. |
| [2] MachineFailure | [18] SpinUpFailed | Impossible de mettre le VDA sous tension pour le lancement de la session. Il s'agit d'un problème signalé par l'hyperviseur. | Si la machine est toujours hors tension, essayez de la démarrer à partir de Citrix Studio. Si le démarrage échoue, vérifiez la connectivité à l'hyperviseur ainsi que vos autorisations d'accès. Si le VDA est une machine provisionnée par PVS, vérifiez que la machine est en marche dans la console PVS. Si ce n'est pas le cas, vérifiez qu'un Personal vDisk est attribué à la machine et connectez-vous à l'hyperviseur pour réinitialiser la VM. |

| Catégorie | Raison | Problème | Action |
| --- | --- | --- | --- |
| [2] MachineFailure | [19] Refused | Le Delivery Controller envoie une demande au VDA afin qu'il se prépare à une connexion d'un utilisateur, mais le VDA refuse cette demande. | À l'aide d'une requête ping, vérifiez que le Delivery Controller et le VDA peuvent communiquer entre eux. Si ce n'est pas le cas, réglez les problèmes de pare-feu ou de routage réseau. |
| [2] MachineFailure | [20] ConfigurationSet Failure | Le Delivery Controller n'a pas envoyé les données de configuration requises au VDA, telles que les paramètres de stratégie et les informations sur la session, durant le lancement de la session. Causes possibles : problèmes de communication entre le Delivery Controller et le VDA ; problèmes rencontrés par le Broker Service lors de la création d'une demande de jeu de configuration ; problèmes réseau entraînant le refus de la demande par le VDA. | - |

| Catégorie | Raison | Problème | Action |
| --- | --- | --- | --- |
| [3] NoCapacityAvailable | [21] MaxTotalInstance-sExceeded | La quantité maximale d'instances autorisées pour une application a été atteinte. Aucune autre instance de l'application ne peut être ouverte sur le VDA. Ce problème est généralement lié aux paramètres de limite de l'application. | Envisagez d'augmenter la valeur du paramètre d'application **Limiter le nombre d'instances exécutées en même temps à** si le système de licences le permet. |
| [3] NoCapacityAvailable | [22] MaxPerUserIn-stancesExceeded | L'utilisateur essaye d'ouvrir plus d'une instance de l'application, mais l'application est configurée pour n'autoriser qu'une seule instance de l'application par utilisateur. Ce problème est généralement lié aux paramètres de limite de l'application. | Par défaut, les utilisateurs ne sont autorisés à exécuter qu'une seule instance de l'application. Si vous souhaitez qu'ils puissent exécuter plusieurs instances, envisagez de désélectionner le paramètre **Limiter à une instance par utilisateur**. |

| Catégorie | Raison | Problème | Action |
| --- | --- | --- | --- |
| [1] ClientConnection-Failure | [23] Communication error | Le Delivery Controller a essayé d'envoyer des informations au VDA, telle qu'une demande de préparation à une connexion, mais une erreur s'est produite durant la tentative de communication. Cela peut être dû à des interruptions réseau. | S'il est déjà démarré, redémarrez le Desktop Service sur le VDA pour redémarrer le processus d'enregistrement et vérifiez que le VDA s'enregistre correctement. Confirmez que les Delivery Controller configurés pour le VDA sont corrects via les détails du journal d'événements de l'application. |
| [3] NoCapacityAvailable | [100] NoMachineAvailable Monitoring service converts [12] NoDesktopAvailable to this error code. | Le VDA responsable du lancement de la session n'est pas valide ou n'est pas disponible. Causes possibles : l'état d'alimentation du VDA est inconnu ou non disponible ; le VDA n'a pas redémarré depuis la dernière session de l'utilisateur ; le partage de session est désactivé, hors la session actuelle nécessite qu'il soit activé ; le VDA a été supprimé du groupe de mise à disposition ou du site. | Vérifiez que le VDA se trouve dans un groupe de mise à disposition. Si ce n'est pas le cas, ajoutez-le au groupe de mise à disposition approprié. Vérifiez qu'il existe suffisamment de VDA enregistrés et activés pour le lancement de l'application ou du bureau partagé publié sollicité par l'utilisateur. Vérifiez que l'hyperviseur hébergeant le VDA ne se trouve pas en mode de maintenance. |

| Catégorie | Raison | Problème | Action |
| --- | --- | --- | --- |
| [2] MachineFailure | [101] MachineNotFunctional. Monitoring service converts [12] NoDesktopAvailable to this error code. | Le VDA n'est pas opérationnel. Causes possibles : le VDA a été supprimé du groupe de mise à disposition ; le VDA n'est pas enregistré ; l'état d'alimentation du VDA n'est pas disponible ; le VDA rencontre des problèmes internes. | Vérifiez que le VDA se trouve dans un groupe de mise à disposition. Si ce n'est pas le cas, ajoutez-le au groupe de mise à disposition approprié. Vérifiez que le VDA s'affiche en tant que sous tension dans Citrix Studio. Si l'état d'alimentation est inconnu pour plusieurs machines, réglez les problèmes de connectivité avec l'hyperviseur ou les hôtes défectueux. Vérifiez que l'hyperviseur hébergeant le VDA ne se trouve pas en mode de maintenance. Redémarrez le VDA une fois que ces problèmes ont été résolus. |

### Type d'échecs de machine

| Code d'erreur | ID du code d'erreur | Problème | Action |
| --- | --- | --- | --- |
| Inconnu | - | - | - |
| Non enregistré | 3 | - | - |

| Code d'erreur | ID du code d'erreur | Problème | Action |
|---|---|---|---|
| MaxCapacity (représenté par Max Load dans Director) | 4 | La machine indique qu'elle fonctionne à sa capacité maximale, c'est-à-dire à son indice de charge maximal. | Assurez-vous que tous les hyperviseurs sont sous tension. Ajoutez d'autres machines aux groupes de mise à disposition concernés en augmentant la capacité de l'hyperviseur ou en ajoutant d'autres hyperviseurs. |
| StuckOnBoot | 2 | La VM n'a pas terminé sa séquence de démarrage et ne communique pas avec l'hyperviseur. | Assurez-vous que la machine a démarré correctement sur l'hyperviseur. Vérifiez la présence d'autres messages sur la VM, tels que des problèmes d'OS. Assurez-vous que les outils de l'hyperviseur sont installés sur la VM. Assurez-vous que le VDA est installé sur la VM. |
| FailedToStart | 1 | La VM a rencontré des problèmes lors de la tentative de démarrage sur l'hyperviseur. | Vérifiez les journaux de l'hyperviseur. |
| Aucun | 0 | - | - |

**Raison de l'annulation d'enregistrement de la machine (applicable lorsque le type d'échec est défini sur Non enregistré ou Inconnu)**

| Code d'erreur | ID du code d'erreur | Problème | Action |
|---|---|---|---|
| AgentShutdown | 0 | Le VDA s'est arrêté correctement. | Mettez sous tension le VDA si cela est requis par des stratégies de gestion de l'alimentation existantes. Examinez les erreurs dans les journaux d'événements. |
| AgentSuspended | 1 | Le VDA est en mode veille ou veille prolongée. | Sortez le VDA de la mise en veille prolongée. Envisagez de désactiver la mise en veille prolongée des VDA Citrix Virtual Apps and Desktops via les paramètres d'alimentation. |
| IncompatibleVersion | 100 | Le VDA ne peut pas communiquer avec le Delivery Controller car les versions du protocole Citrix ne correspondent pas. | Alignez les versions du VDA et du Delivery Controller. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
| --- | --- | --- | --- |
| AgentAddressResolutionFailed | 102 | Le Delivery Controller n'a pas pu résoudre l'adresse IP du VDA. | Vérifiez que le compte de la machine VDA existe dans AD. Si ce n'est pas le cas, créez-le. Vérifiez que le nom et l'adresse IP du VDA dans le DNS sont corrects. Modifiez-les le cas échéant. Si le problème est généralisé, vérifiez les paramètres DNS sur les Delivery Controller. Vérifiez la résolution DNS du Delivery Controller en exécutant la commande `nslookup`. |
| | 101 | Le Delivery Controller n'a pas pu résoudre l'adresse IP du VDA. | Vérifiez que le compte de la machine VDA existe dans AD. Si ce n'est pas le cas, créez-le. Vérifiez que le nom et l'adresse IP du VDA dans le DNS sont corrects. Modifiez-les le cas échéant. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
|---|---|---|---|
| AgentNotContactable | 102 | Un problème de communication s'est produit entre le Delivery Controller et le VDA. | À l'aide d'une requête ping, vérifiez que le Delivery Controller et le VDA peuvent communiquer entre eux. Si ce n'est pas le cas, réglez les problèmes de pare-feu ou de réseau. Reportez-vous aux instructions de dépannage indiquées dans l'article du centre de connaissances, Dépannage de l'enregistrement de VDA auprès de Delivery Controller dans Virtual Apps and Desktops (CTX136668), pour plus d'informations sur les problèmes courants de communication entre le Delivery Controller et le VDA. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
|---|---|---|---|
| | 102 | Un problème de communication s'est produit entre le Delivery Controller et le VDA. | Reportez-vous aux instructions de dépannage indiquées dans l'article du centre de connaissances, Dépannage de l'enregistrement de VDA auprès de Delivery Controller dans Virtual Apps and Desktops (CTX136668), pour plus d'informations sur les problèmes courants de communication entre le Delivery Controller et le VDA. Contactez le support Citrix. |
| AgentWrongActiveDirectoryOU | 103 | La découverte Active Directory n'a pas été configurée correctement. L'unité d'organisation spécifique au site (sur laquelle les informations du contrôleur de site sont stockées dans AD) configurée dans le registre du VDA est destinée à un site différent. | Assurez-vous que la configuration de Active Directory est correcte ou vérifiez les paramètres de registre. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
|---|---|---|---|
| EmptyRegistrationRequest | 104 | La demande d'enregistrement envoyée depuis le VDA au Delivery Controller était vide. Cela peut être dû au fait que l'installation du logiciel VDA est corrompue. | Redémarrez le Desktop Service sur le VDA pour redémarrer le processus d'enregistrement et vérifiez que le VDA s'est enregistré correctement via le journal d'événements d'applications. |
| MissingRegistrationCapabilities | 105 | La version du VDA n'est pas compatible avec le Delivery Controller. | Mettez à niveau le VDA ou supprimez le VDA et réinstallez-le. |
| MissingAgentVersion | 106 | La version du VDA n'est pas compatible avec le Delivery Controller. | Réinstallez le logiciel VDA si le problème affecte toutes les machines. |
| InconsistentRegistrationCapabilities | 107 | Le VDA ne peut pas communiquer ses capacités au broker. Ceci peut être dû à une incompatibilité entre la version du VDA et celle du Delivery Controller. Les capacités d'enregistrement, qui diffèrent pour chaque version, sont exprimées dans un format qui ne correspond pas à la demande d'enregistrement. | Alignez les versions du VDA et du Delivery Controller. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
|---|---|---|---|
| NotLicensedForFeature | 108 | L'utilisation de cette fonctionnalité n'est pas couverte par une licence. | Vérifiez l'édition de votre système de licences Citrix ou supprimez et réinstallez le VDA. |
| | 108 | L'utilisation de cette fonctionnalité n'est pas couverte par une licence. | Contactez le support Citrix. |
| UnsupportedCredentialSecurityversion | 109 | La VDA et le Delivery Controller n'utilisent pas le même mécanisme de cryptage. | Alignez les versions du VDA et du Delivery Controller. |
| InvalidRegistrationRequest | 110 | Le VDA a fait une demande d'enregistrement auprès du broker, mais le contenu de la demande est corrompu ou non valide. | Reportez-vous aux instructions de dépannage indiquées dans l'article du centre de connaissances, Dépannage de l'enregistrement de VDA auprès de Delivery Controller dans Virtual Apps and Desktops (CTX136668), pour plus d'informations sur les problèmes courants de communication entre le Delivery Controller et le VDA. |
| SingleMultiSessionMismatch | 111 | Le système d'exploitation du VDA n'est pas compatible avec le catalogue de machines ou le groupe de mise à disposition. | Ajoutez le VDA au type de catalogue de machines ou groupe de mise à disposition correct contenant des machines avec le même système d'exploitation. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
| --- | --- | --- | --- |
| FunctionalLevelTooLowForCatalog | 112 | Le catalogue de machines est défini avec un niveau fonctionnel de VDA plus élevé que celui de la version installée du VDA. | Vérifiez que le niveau fonctionnel du catalogue de machines du VDA correspond à celui du VDA. Mettez à niveau ou rétrogradez le catalogue de machines de façon à ce qu'il corresponde à celui du VDA. |
| FunctionalLevelTooLowForDesktopGroup | 113 | Le groupe de mise à disposition est défini avec un niveau fonctionnel de VDA plus élevé que celui de la version installée du VDA. | Vérifiez que le niveau fonctionnel du groupe de mise à disposition du VDA correspond à celui du VDA. Mettez à niveau ou rétrogradez le catalogue de machines de façon à ce qu'il corresponde à celui du VDA. |
| Mettre hors tension | 200 | La VDA ne s'est pas arrêté correctement. | En supposant que le VDA est sous tension, essayez de démarrer le VDA depuis Citrix Studio et vérifiez qu'il démarre et s'enregistre correctement. Réglez tout problème de démarrage ou d'enregistrement. Consultez les journaux d'événements du VDA une fois la sauvegarde terminée pour déterminer la cause de l'arrêt. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
| --- | --- | --- | --- |
| AgentRejectedSettingsUpdate | 203 | Des paramètres, tels que les stratégies Citrix, ont été modifiés ou mis à jour, mais une erreur s'est produite lors de l'envoi des mises à jour au VDA. Cela peut se produire si les mises à jour ne sont pas compatibles avec la version du VDA installé. | Mettez à niveau le VDA si nécessaire. Vérifiez que les mises à jour qui ont été appliquées sont prises en charge par la version du VDA. |
| SessionPrepareFailure | 206 | Le broker n'a pas effectué un audit des sessions exécutées sur le VDA. | En cas de problème généralisé, redémarrez le Citrix Broker Service sur le Delivery Controller. |
| | 206 | Le broker n'a pas effectué un audit des sessions exécutées sur le VDA. | Contactez le support Citrix. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
| --- | --- | --- | --- |
| ContactLost | 207 | Le Delivery Controller a perdu la connexion avec le VDA. Cela est probablement dû à des perturbations du réseau. | Vérifiez que le Citrix Broker Service est exécuté sur le Delivery Controller et que le Desktop Service est exécuté sur le VDA. Si ces services sont arrêtés, démarrez-les. S'il est déjà démarré, redémarrez le Desktop Service sur le VDA pour redémarrer le processus d'enregistrement et vérifiez que le VDA s'enregistre correctement. Confirmez que les Delivery Controller configurés pour le VDA sont corrects via les détails du journal d'événements de l'application. À l'aide d'une requête ping, vérifiez que le Delivery Controller et le VDA peuvent communiquer entre eux. Si ce n'est pas le cas, réglez les problèmes de pare-feu ou de réseau. |
| | 207 | Le Delivery Controller a perdu la connexion avec le VDA. Cela est probablement dû à des perturbations du réseau. | Vérifiez que le Desktop Service fonctionne sur le VDA. Démarrez-le s'il est arrêté. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
| --- | --- | --- | --- |
| BrokerRegistrationLimitReached | 301 | Le nombre maximal de VDA autorisés à s'enregistrer simultanément auprès du Delivery Controller a été atteint. Par défaut, le Delivery Controller autorise l'enregistrement simultané de 10 000 VDA. | Envisagez d'ajouter des Delivery Controller au site ou de créer un site. Vous pouvez également accroître le nombre de VDA autorisés à s'enregistrer simultanément auprès du Delivery Controller via la clé de registre **HKEY_LOCAL_MACHINE\Software** Pour plus d'informations, consultez l'article du centre de connaissances, Entrées de clé de registre utilisées par Citrix Virtual Apps and Desktops (CTX117446). L'augmentation de ce nombre peut exiger des ressources processeur et mémoire supplémentaires pour le Delivery Controller. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
| --- | --- | --- | --- |
| SettingsCreationFailure | 208 | Le broker n'a pas réussi à construire un ensemble de paramètres et de configurations à envoyer au VDA. Si le broker est incapable de recueillir ces données, l'enregistrement échoue et le VDA n'est plus enregistré. | Vérifiez la présence d'erreurs dans les journaux d'événements du Delivery Controller. Si un problème n'est pas clair dans les journaux, redémarrez le Broker Service. Une fois que le Broker Service est redémarré, redémarrez le Desktop Service sur les VDA affectés et vérifiez qu'ils s'enregistrent correctement. |
| | 208 | Le broker n'a pas réussi à construire un ensemble de paramètres et de configurations à envoyer au VDA. Si le broker est incapable de recueillir ces données, l'enregistrement échoue et le VDA n'est plus enregistré. | Redémarrez le Desktop Service sur les VDA affectés et vérifiez qu'ils s'enregistrent correctement. Contactez le support Citrix. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
|---|---|---|---|
| SendSettingsFailure | 204 | Le broker n'a pas envoyé de paramètres et de données de configuration au VDA. Si le broker est capable de rassembler les données mais qu'il ne peut pas les envoyer, l'enregistrement échoue. | Si vous êtes limité à un seul VDA, redémarrez le Desktop Service sur le VDA pour forcer le ré-enregistrement et vérifiez que le VDA s'enregistre correctement dans le journal d'événements d'applications. Corrigez toutes les erreurs. Reportez-vous aux instructions de dépannage indiquées dans l'article du centre de connaissances, Dépannage de l'enregistrement de VDA auprès de Delivery Controller dans Virtual Apps and Desktops (CTX136668), pour plus d'informations sur les problèmes courants de communication entre le Delivery Controller et le VDA. |
| AgentRequested | 2 | Une erreur indéterminée s'est produite. | Contactez le support Citrix. |
| DesktopRestart | 201 | Une erreur indéterminée s'est produite. | Contactez le support Citrix. |
| DesktopRemoved | 202 | Une erreur indéterminée s'est produite. | Contactez le support Citrix. |

| Code d'erreur | ID du code d'erreur | Problème | Action |
|---|---|---|---|
| SessionAuditFailure | 205 | Une erreur indéterminée s'est produite. | Contactez le support Citrix. |
| UnknownError | 300 | Une erreur indéterminée s'est produite. | Contactez le support Citrix. |
| RegistrationStateMismatch | 302 | Une erreur indéterminée s'est produite. | Contactez le support Citrix. |
| Inconnu | - | Une erreur indéterminée s'est produite. | Contactez le support Citrix. |

## Avis de tiers

June 27, 2024

Cette version de Citrix Virtual Apps and Desktops peut inclure un logiciel tiers distribué sous une licence selon les conditions définies dans les documents suivants :

- Avis de tiers pour Citrix Virtual Apps and Desktops (téléchargement PDF)
- Divulgations de logiciels non commerciaux pour FlexNet Publisher 2017 (11.15.0.0) (téléchargement PDF)
- Supplément à la documentation FLEXnet Publisher Logiciels tiers et Open Source utilisés dans FlexNet Publisher 11.15.0 (Télécharger PDF)

## SDK et API

June 27, 2024

Plusieurs kits de développement et API sont disponibles avec cette version. Pour accéder aux SDK et aux API, visitez Build anything with Citrix. À partir de là, sélectionnez **Citrix Workspace** pour accéder aux informations de programmation de Citrix Virtual Apps and Desktops et de ses composants associés.

> **Remarque :**
>
> Le SDK Citrix Virtual Apps and Desktops et le SDK Citrix Group Policy peuvent être installés en tant que module ou composant logiciel enfichable. Plusieurs SDK de composants (tels que Citrix Licensing, Citrix Provisioning et StoreFront) s'installent uniquement à l'aide d'un composant logiciel enfichable.

Ce produit prend en charge les versions 3 à 5 de PowerShell.

## SDK Citrix Virtual Apps and Desktops

Ce SDK s'installe automatiquement en tant que module PowerShell lorsque vous installez un Delivery Controller ou Studio. Cela vous permet d'utiliser les applets de commande de ce kit SDK sans avoir à ajouter de composants logiciels enfichables. (Des instructions sont fournies ci-dessous si vous choisissez d'installer ce SDK en tant que composant logiciel enfichable.)

### Autorisations

Vous devez exécuter le shell ou le script avec une identité disposant de droits d'administration Citrix. Bien que les membres du groupe d'administrateurs locaux du contrôleur disposent automatiquement de privilèges d'administration complets pour permettre l'installation de Citrix Virtual Apps ou Citrix Virtual Desktops, Citrix vous recommande, pour un fonctionnement normal, de créer des administrateurs Citrix avec les droits appropriés, plutôt que d'utiliser le compte des administrateurs locaux.

### Accéder aux applets de commande et les exécuter

1. Démarrez un shell dans PowerShell : ouvrez Studio, sélectionnez l'onglet **PowerShell** et cliquez sur **Lancer PowerShell**.
2. Pour utiliser les applets de commande du kit de développement dans des scripts, définissez la stratégie d'exécution dans PowerShell. Pour plus d'informations sur la stratégie d'exécution PowerShell, veuillez consulter votre documentation Microsoft.
3. Si vous souhaitez utiliser le composant logiciel enfichable (plutôt que le module), ajoutez-le à l'aide de l'applet de commande `Add-PSSnapin` (ou `asnp`).

   V1 et V2 indiquent la version du composant logiciel enfichable. Les composants logiciels enfichables XenDesktop 5 correspondent à la version 1. Les composants logiciels enfichables de Citrix Virtual Apps and Desktops et de XenDesktop 7 correspondent à la version 2. Par exemple,

pour installer le composant logiciel enfichable de Citrix Virtual Apps and Desktops, tapez `Add-PSSnapin Citrix.ADIdentity.Admin.V2`. Pour importer tous les applets de commande, entrez : `Add-PSSnapin Citrix.*.Admin.V*`

Vous pouvez maintenant utiliser les applets de commande et les fichiers d'aide.

- Pour accéder aux fichiers d'aide de ce SDK, sélectionnez le produit ou le composant dans la liste Catégories, puis **Citrix Virtual Apps and Desktops SDK**.
- Pour obtenir des conseils sur PowerShell, consultez Windows PowerShell ISE.

### Kit de développement de stratégie de groupe

Le kit de développement (SDK) de stratégie de groupe Citrix vous permet d'afficher et de configurer les paramètres et les filtres de stratégie de groupe. Ce SDK utilise un fournisseur PowerShell pour créer un lecteur virtuel qui correspond aux paramètres et filtres de la machine et de l'utilisateur. Le fournisseur apparaît sous la forme d'une extension de `New-PSDrive`.

Pour utiliser le kit de développement de stratégie de groupe, soit Studio soit le kit de développement Citrix Virtual Apps and Desktops doit être installé.

Le fournisseur PowerShell de stratégie de groupe Citrix est disponible en tant que module ou composant logiciel enfichable.

- Pour utiliser le module, aucune action supplémentaire n'est nécessaire.
- Pour ajouter le composant logiciel enfichable, tapez `Add-PSSnapin citrix.common.grouppolicy`.

Pour accéder à l'aide, tapez : `help New-PSDrive -path localgpo:/`.

Pour créer un lecteur virtuel et le charger de paramètres, tapez `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>` où la chaîne de Controller correspond au nom de domaine complet d'un Controller du site auquel vous voulez vous connecter et à partir duquel vous voulez charger les paramètres.

### API REST Citrix Virtual Apps and Desktops

Avec les API REST Citrix Virtual Apps and Desktops, vous pouvez automatiser la gestion des ressources dans le cadre d'un déploiement Citrix Virtual Apps and Desktops.

Les API REST Citrix Virtual Apps and Desktops sont disponibles sur https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis. Les API qui ne s'appliquent pas à Citrix Virtual Apps and Desktops sont marquées comme telles. Suivez les instructions qui s'y trouvent pour configurer l'accès au service d'API et utiliser les API pour gérer et optimiser vos ressources.

### Monitor Service OData

L'API Monitor permet d'accéder aux données de Monitor Service à l'aide de la version 3 ou 4 de l'API OData. Vous pouvez créer des tableaux de bord de surveillance et de création de rapports personnalisés en fonction des données interrogées à partir des données de Monitor Service. OData V.4 est basé sur l'API Web ASP.NET et prend en charge les requêtes d'agrégation.

Pour plus d'informations, consultez la section API Monitor Service OData.