Citrix DaaS

Contents

Vue d'ensemble

March 30, 2024

Introduction

Citrix DaaS est un service qui fournit la virtualisation des applications et des bureaux, permettant au service informatique de contrôler les machines virtuelles, les applications et la sécurité sur site ou hébergées dans le cloud, tout en fournissant un accès en tout lieu et à n'importe quel appareil. Les utilisateurs peuvent utiliser des applications et des bureaux indépendamment du système d'exploitation et de l'interface de l'appareil.

Citrix DaaS vous permet de mettre à disposition de manière sécurisée des applications et bureaux virtuels sur n'importe quel appareil tout en laissant le gros de l'installation et les mises à jour à la charge de Citrix. Vous conservez un contrôle total sur les applications, les stratégies et les utilisateurs tout en offrant la meilleure expérience possible sur n'importe quel appareil.

Citrix DaaS vous permet de gérer ensemble les charges de travail des datacenters locaux et du cloud public dans un déploiement hybride. Vous pouvez vous connecter à des clouds publics Microsoft Azure, Amazon Web Services (AWS) et Google Cloud, ainsi qu'à des hyperviseurs locaux tels que XenServer, Microsoft Hyper-V, Nutanix AHV et VMware vSphere. L'approche hybride multicloud vous offre la flexibilité nécessaire pour déployer différentes applications dans différents emplacements de ressources dans le monde entier.

Citrix DaaS propose plusieurs méthodes pour mettre à disposition des applications et des bureaux.

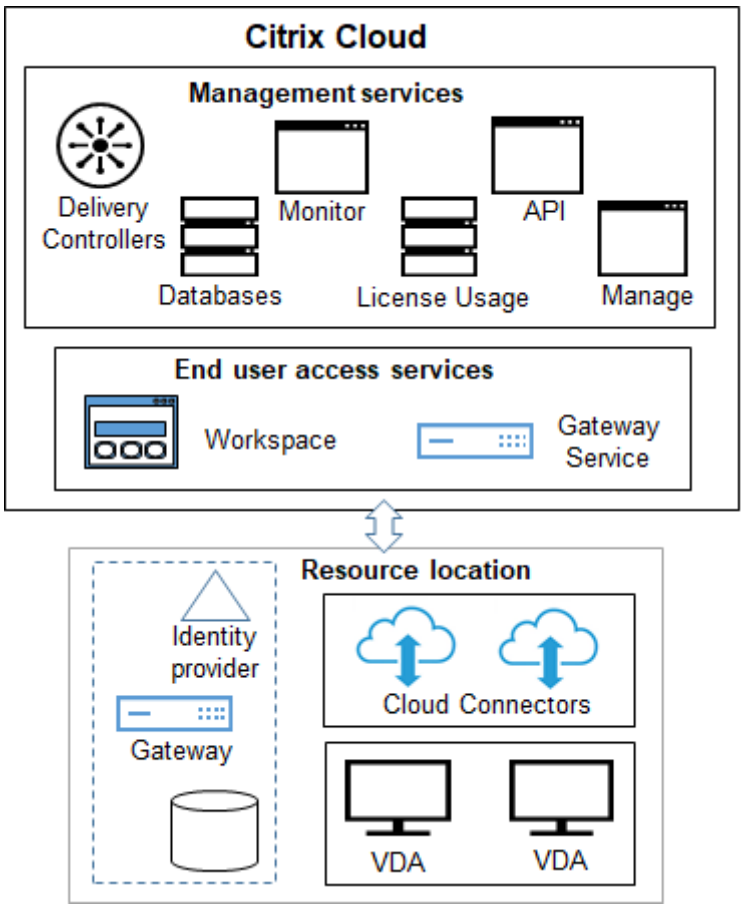
- Méthodes de mise à disposition décrit les méthodes principales, avec des cas d'utilisation et les avantages/inconvénients.
- Modèles de mise à disposition présente plus d'options et offre également des comparaisons de modèles VDI.

Azure géré par Citrix simplifie davantage le déploiement des applications et des bureaux virtuels. Avec Azure géré par Citrix, Citrix gère également l'hébergement des charges de travail Azure.

En savoir plus sur les avantages de l'utilisation de ce service.

Présentation du site

Le graphique suivant illustre les services et composants avec lesquels les administrateurs Citrix travaillent dans un déploiement de production Citrix DaaS (également appelé site).



Comme illustré dans le graphique, Citrix gère les services et composants d'accès utilisateur et de gestion dans Citrix Cloud. Les applications et bureaux que vous mettez à disposition des utilisateurs résident sur des machines dans un ou plusieurs emplacements de ressources. Dans un déploiement Citrix DaaS, un emplacement de ressources contient des composants provenant de la couche d'accès et des couches de ressources : Chaque emplacement de ressources est considéré comme une zone.

Si vous avez récemment migré à partir d'un site Citrix Virtual Apps and Desktops, vous verrez que Citrix DaaS élimine la majeure partie du travail de configuration des composants requis dans un déploiement local.

Composants et services gérés par Citrix

- **Delivery Controller :** Citrix DaaS permet d'équilibrer la charge des applications et des bureaux, d'authentifier les utilisateurs et de négocier ou de hiérarchiser les connexions directement depuis le cloud, sans avoir à gérer les Delivery Controller, comme avec Citrix Virtual Apps and Desktops.
- **Bases de données :** les données de configuration, de surveillance et de journalisation de la configuration du site sont stockées par le service cloud, éliminant ainsi le besoin d'utiliser une

base de données SQL pour le produit Citrix Virtual Apps and Desktops local.

- **Système de licences :** gère les licences et fournit des statistiques d'utilisation.
- **Interfaces de gestion :** voir Interfaces de gestion. De nombreuses tâches sont également disponibles dans les API de service.
- **Interface de surveillance :** l'interface Surveillance 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. Les affichages incluent :
  - Données de session en temps réel à partir du Broker Service dans le Controller, qui comprennent des données de l'agent broker dans le VDA.
  - Données historiques provenant de Monitor Service dans le Controller.
  - Données sur le trafic HDX (également appelé trafic ICA).
- **Cloud Connector :** un Cloud Connector est le canal de communication entre les composants dans le Citrix Cloud et les composants dans l'emplacement de ressources. Dans l'emplacement de ressources, le Cloud Connector sert de proxy pour le Delivery Controller dans Citrix Cloud.

  Chaque emplacement de ressources contient au moins un Cloud Connector. Deux ou plusieurs Cloud Connector sont recommandés pour la redondance.

  - Lorsque vous utilisez Configuration complète pour provisionner des machines, vous installez d'abord Cloud Connector à partir de la console Citrix Cloud. Pour plus d'informations, consultez Cloud Connector.
  - Lorsque vous utilisez le déploiement rapide pour provisionner des machines Azure, Citrix crée l'emplacement des ressources et Cloud Connector pour vous lorsque vous créez un catalogue.

  Une fois les Cloud Connector installés, Citrix les gère et les met à jour. Les seules tâches gérées par le client sont l'application de correctifs et les mises à jour Windows de Cloud Connector.

Interfaces de gestion

Dans l'onglet **Gérer** de Citrix DaaS, vous pouvez sélectionner les interfaces suivantes.

Configuration complète

Dans l'interface **Gérer > Configuration complète**, vous pouvez effectuer les opérations suivantes :

- Obtenez une vue d'ensemble de votre déploiement Citrix DaaS et des dernières fonctionnalités sur la page d'accueil.

- Créer et gérer des connexions aux hôtes.
- Créer et gérer des catalogues de machines contenant les applications et les bureaux que vous fournissez à vos utilisateurs.
- Créer et gérer des groupes de mise à disposition (et éventuellement des groupes d'applications).
- Créer et gérer des stratégies Citrix qui affectent l'utilisation et le comportement des technologies et fonctionnalités HDX, ainsi qu'une gestion au niveau du site. Cela inclut les paramètres de stratégie pour les sessions, le transport adaptatif, les périphériques, les graphiques, le contenu multimédia, la redirection de contenu et les VDA.
- Personnaliser l'administration déléguée pour créer des administrateurs basés sur des rôles ayant des étendues d'autorité spécifiques.
- Gérer la fonctionnalité Autoscale pour gérer de manière proactive les machines qui fournissent des applications et des bureaux.
- Équilibrer la charge des machines
- Exécuter des vérifications de l'état sur vos VDA pour identifier les problèmes potentiels et connaître les suggestions de correction.
- Afficher le contenu du journal de configuration pour vérifier quand les modifications de configuration et d'autres activités administratives ont eu lieu, et qui les a initiées.

Déploiement rapide

À partir de l'interface **Gérer > Déploiement rapide**, vous pouvez facilement déployer et gérer des charges de travail Microsoft Azure qui utilisent un abonnement Azure géré par Citrix ou votre propre abonnement Azure. Pour plus d'informations, consultez Déploiement rapide et Azure géré par Citrix. À partir du déploiement rapide, vous pouvez :

- Créer et gérer des catalogues.
- Créer et personnaliser des images, soit à partir de différentes images préparées par Citrix, soit à partir d'images que vous importez depuis votre abonnement Azure.

Pour plus d'informations, consultez Déploiement rapide.

Gestion de l'environnement

À partir de l'interface **Gestion de l'environnement**, vous pouvez utiliser les technologies de gestion intelligente des ressources et de Profile Management afin d'offrir les meilleures performances, durées de connexion aux bureaux et temps de réponses des applications. Pour plus d'informations, consultez Workspace Environment Management.

Composants et technologies gérés par le client

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

  Citrix installe et gère le service Citrix Gateway dans Citrix Cloud. Vous pouvez également installer Citrix Gateway dans des emplacements de ressources.

- **Active Directory :** Active Directory est utilisé pour l'authentification et l'autorisation. Il authentifie les utilisateurs et garantit qu'ils ont accès aux ressources appropriées. L'identité d'un abonné définit les services auxquels il a accès dans Citrix Cloud. Cette identité provient de comptes de domaine Active Directory fournis à partir des domaines dans l'emplacement de ressources.

- **Fournisseur d'identité (IdP) :** l'IdP est l'autorité finale pour l'identité de l'utilisateur. Les IDP pris en charge sont : Active Directory local, Active Directory plus jeton, Azure Active Directory, Citrix Gateway et Okta. Pour plus d'informations, consultez :

  - Identité d'espace de travail
  - Gestion des identités et des accès

- **Virtual Delivery Agents (VDA) :** un VDA Citrix doit être installé sur chaque machine physique ou virtuelle qui fournit des ressources (applications et bureaux). Les VDA établissent et gèrent la connexion entre la machine sur laquelle il est installé et l'appareil de l'utilisateur et appliquent toute stratégie qui a été configurée pour la session.

  Le VDA s'enregistre auprès d'un Delivery Controller, en utilisant un Cloud Connector dans l'emplacement des ressources en tant que proxy.

  Plusieurs types de VDA sont disponibles :

  - Les VDA pour les systèmes d'exploitation multi-session Windows autorisent plusieurs utilisateurs à se connecter à la machine à un moment donné. Ce type de VDA est généralement installé sur des serveurs Windows.
  - Les VDA pour les systèmes d'exploitation mono-session Windows ne permettent qu'à un seul utilisateur de se connecter à une machine à la fois. Ce type de VDA est généralement utilisé pour VDI.

    Une version principale de ce type de VDA est disponible pour une utilisation avec la fonctionnalité Remote PC Access. Il contient un sous-ensemble des fonctionnalités du VDA mono-session complet.

  - Les VDA Linux prennent en charge les applications et les bureaux virtuels Linux basés sur une distribution RHEL, CentOS, SUSE ou Ubuntu.

  Dans cette documentation, le mot « VDA » fait référence à l'agent ainsi qu'à la machine sur laquelle il est installé.

- **Hyperviseurs et services cloud :** dans la plupart des sites de production, les instances d'application et de bureau (charges de travail) que vous rendez disponibles (publiez) pour vos utilisateurs sont « hébergées » par un hyperviseur ou service de cloud pris en charge. (Généralement, la fonctionnalité Remote PC Access est utilisée avec des machines physiques. Par conséquent, elle n'utilise pas d'hyperviseurs ou de services de cloud pour le provisionnement des machines.)

  - Lorsque vous utilisez l'interface Configuration complète, vous créez une connexion à un hyperviseur hôte ou à un service cloud pris en charge. Ensuite, à partir de Configuration complète, vous utilisez une image (créée via cet hôte) pour créer un catalogue de machines contenant les instances d'application et de bureau. Ensuite, vous créez un groupe de mise à disposition. Citrix fournit de nombreux outils pour simplifier et faciliter la création et la maintenance de ces hôtes de session.
  - Lorsque vous utilisez le déploiement rapide pour fournir des charges de travail Azure, il vous suffit de créer le catalogue. Bien que vous puissiez utiliser votre propre abonnement Azure lors de la création du catalogue, l'utilisation d'un abonnement Azure géré par Citrix vous évite de devoir également gérer l'hôte.

  Les instances d'application et de bureau que vous publiez peuvent être locales, hébergées dans des clouds publics ou dans un mélange hybride des deux.

- **Citrix StoreFront :** Citrix StoreFront est le prédécesseur de Citrix Workspace hébergé dans le cloud. Il est utilisé comme interface Web pour accéder aux applications et aux bureaux.

  Vous pouvez éventuellement installer des serveurs StoreFront dans des emplacements de ressources. Le fait de disposer de magasins locaux peut aider à fournir des applications et des bureaux pendant les pannes de réseau. La fonctionnalité de cache d'hôte local nécessite un StoreFront géré par le client dans chaque emplacement de ressources.

  Pour plus d'informations sur l'utilisation de StoreFront dans un environnement de service, consultez la section Accès utilisateur.

Objets que vous configurez pour mettre à disposition les bureaux et les applications

Vous configurez les éléments suivants pour fournir des applications et des bureaux dans un environnement de production.

- **Connexion hôte :** une connexion hôte (mentionnée précédemment) permet d'activer la communication entre les composants du plan de contrôle (Citrix Cloud) et les VDA dans un emplacement de ressources. Spécifications relatives à la connexion :

  - Adresse et informations d'identification pour accéder à l'hôte
  - Méthode de stockage et machines à utiliser pour le stockage
  - Réseau que les VM peuvent utiliser

  N'oubliez pas : lorsque vous utilisez le déploiement rapide, vous n'avez pas besoin de créer de connexion. Et si vous utilisez Azure géré par Citrix, Citrix gère également l'hébergement.

- **Catalogue :** dans les interfaces Configuration complète et Surveiller, les catalogues sont appelés « catalogues de machines ».
  Un catalogue est un ensemble de machines virtuelles ou physiques ayant le même type de système d'exploitation (par exemple, multi-session Windows ou mono-session Ubuntu).

  When creating a catalog, you usually use an image, which is also known as a template. (Remote PC Access catalogs usually contain physical machines, so no image is needed.)

  - When using Quick Deploy, Citrix provides several Citrix prepared images you can use to create your own customized images. Or, you can import images from your own Azure subscription.
  - When using Full Configuration to create VMs using a supported host type, the image usually must be created and reside on a host machine. When creating the catalog, you provide the path to that image.

  Regardless of where the image resides, you can install applications on the image, if you want those apps on all machines created from that image (and don't want to virtualize those apps).

  After the image is ready, you create the catalog.

  - For VMs, MCS creates the machines and the catalog.
  - For Remote PC Access, MCS simply creates the catalog, because the physical machines already exist.

  For more information about MCS, see Image management.

- **Groupe de mise à disposition :** un groupe de mise à disposition spécifie :

  - Une ou plusieurs machines d'un catalogue.
  - Les utilisateurs qui sont autorisés à accéder à ces machines.
  - Les applications et bureaux auxquels les utilisateurs peuvent accéder via Workspace.

  Lors de l'utilisation du déploiement rapide, un groupe de mise à disposition est créé automatiquement. (Il apparaît uniquement dans l'interface Configuration complète.)

- **Groupe d'applications :** les groupes d'applications vous permettent de gérer des collections d'applications. Vous pouvez créer des groupes d'applications pour les applications partagées entre différents groupes de mise à disposition ou utilisées par un sous-ensemble d'utilisateurs dans des groupes de mise à disposition. Les groupes d'applications sont facultatifs.

Azure géré par Citrix

Azure géré par Citrix est une option disponible dans plusieurs éditions de Citrix DaaS. L'utilisation de Azure géré par Citrix simplifie le déploiement des applications et des bureaux virtuels à partir d'Azure. Citrix gère l'infrastructure d'hébergement des charges de travail Azure.

Avec Azure géré par Citrix, vous bénéficiez d'un abonnement Azure dédié et d'un emplacement de ressources Azure géré par Citrix. Dans cet abonnement Azure, vous créez un catalogue de machines virtuelles. Vous pouvez :

- Déployez des machines avec système d'exploitation Windows mono-session et multisession ou des machines sous OS Linux, à partir de différentes versions prises en charge.
- Choisissez parmi une liste organisée de types de calcul et d'options de stockage dans certaines régions.
- Provisionnez des charges de travail persistantes ou non persistantes sur ces machines.
- Choisissez parmi plusieurs images fournies par Citrix sur lesquelles le dernier VDA est installé. Ensuite, à partir de l'interface Citrix, créez votre propre image à partir de ce modèle et personnalisez-la. Vous pouvez également importer des images à partir de vos propres abonnements Azure.

Même si Citrix gère la capacité Azure, si vous souhaitez communiquer avec des ressources existantes sur votre propre abonnement Azure, vous pouvez utiliser l'appairage Azure VNet pour connecter des ressources. Vous pouvez également utiliser Citrix SD-WAN pour vous connecter directement à vos ressources locales.

Pour plus d'informations sur la sécurité et les responsabilités lors de l'utilisation d'Azure géré par Citrix, reportez-vous à Vue d'ensemble de la sécurité technique pour Azure géré par Citrix.

Commander Azure géré par Citrix

Pour obtenir un abonnement Azure géré par Citrix, vous devez vous abonner à une offre de service Citrix prise en charge, puis commander des fonds de consommation Azure géré par Citrix. Vous pouvez commander Citrix DaaS et les fonds de consommation via Citrix ou sur Azure Marketplace.
Azure géré par Citrix est pris en charge avec les offres de services suivantes :

- Citrix Workspace Premium Plus
- Éditions Citrix DaaS, Advanced, Advanced Plus et Premium

- Édition Citrix DaaS Standard pour Azure

Pour plus de détails, consultez la section S'inscrire à Citrix DaaS.

Résumé des avantages Azure géré par Citrix

L'utilisation de Azure géré par Citrix offre plusieurs avantages :

- La voie la plus rapide vers les avantages du cloud hybride.
- Décharge la gestion informatique de l'infrastructure. Facilite les tâches d'administration du service informatique.
- Permet de faire évoluer rapidement les solutions de travail.
- Fournit un abonnement Azure distinct qui est géré par Citrix. Les activités sont donc isolées de vos autres abonnements Azure.
- Vous conservez la possibilité de créer et de gérer des charges de travail à l'aide de vos propres abonnements Azure. Votre déploiement peut inclure des charges de travail qui utilisent l'abonnement Azure géré par Citrix et des charges de travail qui utilisent vos propres abonnements Azure (gérés par le client).
- Utilise un véritable modèle IaaS (Infrastructure as a Service) basé sur la consommation.
- Plusieurs technologies sont disponibles pour créer des connexions à vos propres réseaux locaux (tels que l'appairage Azure VNet et SD-WAN). Cela permet à vos utilisateurs d'accéder aux ressources de votre réseau, telles que les serveurs de fichiers.

Le déploiement et la gestion de Azure géré par Citrix à partir de ce service utilisent l'interface de gestion Déploiement rapide.

Pour plus d'informations, contactez votre représentant Citrix.

Mise à disposition d'applications et de bureaux pour les utilisateurs

Citrix Workspace

Les abonnés (utilisateurs) accèdent à leurs bureaux et applications via Citrix Workspace.

Après l'installation et la configuration de Citrix DaaS, un lien URL de l'espace de travail vous est fourni. L'URL de l'espace de travail est affichée à deux endroits :

- Dans la console Citrix Cloud, sélectionnez **Configuration de l'espace de travail** et cliquez sur le menu dans l'angle supérieur gauche. L'onglet **Accès** contient l'URL de l'espace de travail.
- Sur la page **Accueil** de Citrix DaaS, l'URL de l'espace de travail apparaît au bas de la page.

Testez et partagez le lien de l'URL de l'espace de travail avec vos abonnés (utilisateurs) pour leur donner accès à leurs applications et bureaux. Vos abonnés peuvent accéder à l'URL de l'espace de travail sans aucune configuration supplémentaire.

Vous configurez les espaces de travail à partir de Citrix Cloud.

- Spécifier les services intégrés à Citrix Workspace.
- Personnaliser l'URL que vos abonnés utilisent pour accéder à leur espace de travail.
- Personnaliser l'apparence des espaces de travail des abonnés, tels que les logos, la couleur et les préférences.
- Indiquer comment les abonnés s'authentifient auprès de leur espace de travail, par exemple en utilisant Active Directory ou Azure Active Directory.
- Spécifier la connectivité externe des emplacements de ressources utilisés par vos abonnés.

Pour plus d'informations, consultez Citrix Workspace.

Application Citrix Workspace

Du côté utilisateur, l'application Citrix Workspace est installée sur les machines utilisateur et d'autres points de terminaison, tels que des bureaux virtuels. L'application Citrix Workspace offre aux utilisateurs un accès sécurisé, rapide et en libre-service aux documents, applications et bureaux à partir de tout appareil, y compris les smartphones, tablettes et PC. 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, l'application Citrix Workspace pour HTML5 offre une connexion via un navigateur Web compatible HTML5.

L'application Citrix Workspace est disponible pour différents systèmes d'exploitation. Pour plus d'informations, consultez l'application Citrix Workspace.

Accord de niveau de service

Citrix DaaS a été développé à l'aide des meilleures pratiques de l'industrie afin de garantir la scalabilité du cloud et un haut degré de disponibilité du service.

Pour plus d'informations sur l'engagement de Citrix concernant la disponibilité des services Citrix Cloud, consultez le contrat de niveau de service.

Les performances par rapport à cet objectif peuvent être contrôlées de manière continue sur https://status.cloud.com.

Limitations

Le calcul de cet objectif de niveau de Service n'inclut pas la perte de disponibilité pour les raisons suivantes :

- Le client n'a pas respecté les exigences de configuration de Citrix DaaS documentées dans la documentation produit sur https://docs.citrix.com.
- Composant non géré par Citrix, y compris, mais sans s'y limiter, les composants suivants : machines physiques et virtuelles contrôlées par le client, systèmes d'exploitation installés et entretenus par le client, équipement réseau ou autre matériel installé et contrôlé par le client ; paramètres de sécurité, stratégies de groupe et autres stratégies de configuration définis et contrôlés par le client ; défaillances du fournisseur de cloud public, défaillances du fournisseur de services Internet ou autres défaillances externes au contrôle de Citrix.
- Interruption de service pour des raisons indépendantes de la volonté de Citrix, y compris une catastrophe naturelle, une guerre, des actes de terrorisme, action gouvernementale.

Informations supplémentaires

- Schémas Citrix DaaS
- Architecture de référence et méthodes de déploiement Citrix DaaS
- Vue d'ensemble de la sécurité technique
- Ports réseau
- Avis de tiers
- Configuration système requise
- Fonctionnalités
  - Une introduction aux technologies HDX, ainsi que des détails sur les périphériques, les graphiqueset le multimédia.
  - Remote PC Access : permet aux utilisateurs d'ouvrir une session à distance depuis n'importe quel emplacement sur un PC physique au bureau. Vous pouvez configurer Remote PC Access à partir de Configuration complète ou Déploiement rapide.
  - Publier du contenu : permet de publier une application qui est simplement une URL ou un chemin UNC vers une ressource.
  - Server VDI : permet de mettre à disposition un bureau depuis un système d'exploitation de serveur pour un utilisateur unique.
- Pour Citrix DaaS Standard pour Azure, consultez la documentation produit dédiée.
- Pour en savoir plus sur la disponibilité des fonctionnalités dans les produits et éditions de Citrix DaaS, consultez le tableau des fonctionnalités Citrix DaaS.

- Citrix Cloud Learning Series offre des cours éducatifs pour vous permettre de vous familiariser avec Citrix Cloud et ses services. Vous pouvez visualiser tous les modules de manière séquentielle, depuis les introductions jusqu'à la planification et la création de services. Vous pouvez également choisir des modules individuels ou des segments spécifiques à une tâche au sein d'un module. Consultez Cloud Learning Series.

Prise en main

Pour savoir comment configurer votre déploiement, commencez par Planifier et créer un déploiement. Ce résumé vous guide à travers les étapes principales du processus et offre des liens vers des informations supplémentaires et des procédures détaillées.

Nouveautés

June 13, 2024

L'un des objectifs de Citrix est d'offrir de nouvelles fonctionnalités et des mises à jour de produits aux clients de Citrix DaaS lorsqu'elles sont disponibles. Les nouvelles versions étant plus avantageuses, il est important que vous en profitiez le plus rapidement possible. Des mises à jour sont déployées sur Citrix DaaS environ toutes les 3 semaines.

Ce processus est transparent pour l'utilisateur. Les mises à jour initiales sont uniquement appliquées aux sites Citrix internes pour être ensuite graduellement appliquées aux environnements des clients. La mise à disposition des mises à jour de façon incrémentielle permet de garantir la qualité des produits et de maximiser la disponibilité.

Pour plus d'informations sur le contrat de niveau de service dans le cadre de la scalabilité et la disponibilité des services dans le cloud, consultez Contrat de niveau de service. Pour contrôler les interruptions de service et la maintenance planifiée, consultez le tableau de bord de l'état de service.

Virtual Delivery Agents (VDA)

Les VDA pour machines Windows sont généralement publiés en même temps que le produit Citrix Virtual Apps and Desktops.

- Pour plus d'informations sur les nouvelles fonctionnalités VDA et HDX, consultez les articles Nouveautés et Problèmes connus pour le produit Citrix Virtual Apps and Desktops actuel.
- Pour plus d'informations sur les plates-formes de VDA et les fonctionnalités qui ne sont plus prises en charge, consultez la section Fin de prise en charge. Cet article inclut également

les plates-formes et les fonctionnalités qui ne seront plus prises en charge dans une version ultérieure (par exemple, les systèmes d'exploitation prenant en charge l'installation de VDA).

> **Important :**
>
> 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 1912 LTSR 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 avez installé PvD mais ne l'avez jamais utilisé. Pour plus d'informations, voir Si Personal vDisk est installé sur le VDA.

Juin 2024

Fonctionnalités nouvelles et améliorées

Prise en charge de la création de groupes de ressources lors de la création de catalogues Azure (pour PVS). Auparavant, lors de la création de catalogues Azure à l'aide de l'interface Configuration complète, vous deviez créer les groupes de ressources à l'aide des commandes PowerShell. Grâce à cette fonctionnalité, vous pouvez désormais créer facilement un groupe de ressources lors de la création d'un catalogue dans Web Studio. Cette amélioration simplifie le workflow de création global. Pour plus d'informations, consultez Créer un catalogue Citrix Provisioning à l'aide de l'interface Configuration complète.

Mai 2024

Fonctionnalités nouvelles et améliorées

Secure HDX (version Technical Preview). Vous pouvez désormais utiliser cette fonctionnalité pour empêcher tout élément réseau du chemin de trafic de pouvoir inspecter le trafic HDX. Pour plus d'informations, consultez Secure HDX.

Prise en charge de la mise en veille prolongée de l'unité de traitement graphique Azure (version Technical Preview). Vous avez désormais la possibilité de prendre en charge la mise en veille prolongée des SKU de machines Azure compatibles avec l'unité de traitement graphique.
Pour plus d'informations sur les tailles de machines virtuelles prises en charge, consultez la documentation Microsoft.

La prise en charge des catalogues Citrix Provisioning pour la jointure hybride à Azure AD a été étendue à l'interface Configuration complète. Lorsque vous créez un catalogue Citrix Provisioning, le type d'identité **Joint à Azure Active Directory hybride** est désormais disponible sur la page **Configuration du catalogue de machines > Identités des machines**. Avec cette nouvelle option, vous

pouvez créer des machines hybrides associées à Azure AD via Citrix Provisioning. Pour de plus amples informations, consultez cet article sur Citrix Provisioning.

Améliorations apportées à l'aide contextuelle dans l'interface Configuration complète. Nous avons repensé le panneau d'aide pour offrir une expérience plus informative, en proposant des informations ciblées pour chaque nœud de l'interface Configuration complète. En cliquant sur l'icône d'aide de n'importe quel nœud, vous pouvez désormais accéder à un ensemble complet de ressources visant à fournir une expérience d'apprentissage unique, vous aidant à mieux comprendre les fonctionnalités associées :

- Accédez à des documents clés spécifiquement liés au nœud sélectionné.
- Restez informé des mises à jour de services, notamment de Citrix Roadmap, des problèmes connus, des limites, de la configuration système requise et des nouvelles fonctionnalités.
- Accédez à des ressources étendues telles que Citrix Blogs, Citrix Community, Citrix Feature Explained, la documentation produit Citrix, le support Citrix et la documentation pour les développeurs.

Amélioration de la journalisation de la configuration : suivi des modifications d'adhésion pour les groupes de mise à disposition. Grâce à cette amélioration, la journalisation de la configuration capture et affiche désormais les ID d'utilisateur et de groupe ajoutés ou supprimés des groupes de mise à disposition. Pour consulter les journaux de configuration, accédez à **Configuration complète > Journalisation > Événements**.

Personnalisation de l'ordre de tabulation dans le nœud de recherche. Vous pouvez désormais personnaliser l'ordre des onglets du nœud de **recherche** en fonction de vos habitudes d'utilisation, pour une expérience de navigation améliorée. Pour ce faire, cliquez sur l'icône à trois points située à côté des onglets, faites glisser ces derniers dans l'ordre de votre choix, puis cliquez sur **Appliquer**.

Mise en cache des données pour le nœud Catalogues de machines. Nous avons introduit la mise en cache des données pour le nœud **Catalogues de machines** Citrix DaaS. Cette amélioration réduit considérablement le temps de chargement des pages lorsque vous accédez au nœud **Catalogues de machines**, offrant ainsi une meilleure expérience utilisateur globale.

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.

Détection et atténuation des échecs du service de mise à niveau des VDA pendant le processus de mise à niveau des VDA (version Technical Preview). Notre service intègre désormais des mécanismes de détection avancés. Si des problèmes susceptibles d'entraîner un échec de l'IPU du VDA sont détectés, rendant ainsi le VDA inutilisable, le service prendra des mesures proactives. Il cessera de mettre à jour d'autres machines et quittera le workflow actuel de manière transparente. Cette approche proactive vise à minimiser l'impact et à garantir une expérience fluide, même en cas de problèmes inattendus, en réduisant le rayon d'action potentiel des problèmes rencontrés. Pour plus d'informations, consulter la section Détection et atténuation des échecs du service de mise à niveau des VDA

Prise en charge des mises à jour de VDA à partir d'un partage de fichiers local auquel les VDA ont accès (Technical Preview). Grâce au contrôle d'accès amélioré du programme d'installation du VDA, vous bénéficiez désormais d'une flexibilité et d'un contrôle accrus sur les VDA qui peuvent se connecter et récupérer les MSI de téléchargement nécessaires sans vous soucier d'accorder un accès réseau aux VDA pour récupérer les mises à jour depuis le CDN Azure géré par Citrix. Cela vous permet d'appliquer des règles réseau plus strictes tout en garantissant un accès fluide aux mises à jour essentielles. Pour plus d'informations, consulter la section Prise en charge des mises à jour des VDA à partir d'un partage de fichiers local auquel les VDA ont accès

Prise en charge de l'interface Configuration complète pour la mise à disposition d'applications packagées sur des bureaux statiques mono-session et des PC de bureau. Grâce à cette amélioration, vous pouvez désormais fournir des applications packagées à tous les types de bureau à l'aide de l'interface Configuration complète. Voici les avantages de la fourniture d'applications packagées sur des bureaux *mono-session statiques* :

- 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.

Pour fournir des applications packagées sur des bureaux, ajoutez ces applications aux groupes de mise à disposition de la manière suivante :

- Ajoutez des applications lors de la création du groupe de mise à disposition.
- Ajoutez des applications à un groupe de mise à disposition existant à l'aide de l'une des entrées suivantes : **Groupes de mise à disposition > Ajouter des applications > Applications**, **Applications > Propriétés > Groupes**, ou **Packages d'applications > Packages > Ajouter des groupes de mise à disposition**.

Pour plus d'informations, consultez Créer des groupes de mise à disposition, Gérer les groupes de mise à disposition et Ajouter des applications aux groupes de mise à disposition.

Prise en charge de l'interface Configuration complète pour la mise à disposition d'applications packagées au format FlexApp. Dans **Configuration complète > Packages d'applications**, vous pouvez désormais charger des applications packagées FlexApp vers Citrix Cloud et les mettre à la disposition de vos utilisateurs. Pour plus d'informations, consultez la section Packages d'applications.

Pagination OData. Monitor augmente la limite de pagination OData. Tous les points de terminaison OData v4 renvoient un maximum de 1 000 enregistrements par page, ainsi qu'un lien vers les 1 000 enregistrements suivants dans la réponse. Comme chaque page renvoie de grands ensembles de données, vous pouvez obtenir la même quantité totale de données avec moins de requêtes OData. Cette fonctionnalité réduit le temps nécessaire pour obtenir la quantité totale de données et améliore ainsi l'expérience utilisateur. Pour plus d'informations, consultez la section Accès aux données Monitor Service via le point de terminaison OData v4 dans la documentation Citrix Cloud.

Prise en charge de la création et de la gestion de machines virtuelles confidentielles Azure à l'aide de l'interface Configuration complète. Les machines virtuelles confidentielles Azure fournissent une limite renforcée par du matériel pour répondre à vos besoins de sécurité. Grâce à l'interface utilisateur Configuration complète, vous pouvez désormais créer et gérer des machines virtuelles confidentielles sur Azure. Pour plus d'informations, consultez la section Machines virtuelles confidentielles Azure (Technical Preview).

Prise en charge de l'affichage des adresses IP des clients dans les journaux de configuration. Dans **Configuration complète > Journalisation > Événements**, vous pouvez désormais afficher les détails des adresses IP dans les journaux, ce qui facilite le suivi de l'origine des actions. Pour afficher la colonne des adresses IP dans la vue principale, cliquez sur l'icône **Colonnes à afficher** en haut à droite des journaux, puis sélectionnez **IP du client**. Pour plus d'informations, consultez Afficher le contenu du journal de configuration.

Prise en charge de la capture de propriétés supplémentaires à l'aide de la source de profil de machine dans AWS. Dans les environnements AWS, grâce à cette amélioration, vous pouvez désormais créer ou mettre à jour un catalogue basé sur le profil de machine pour :

- Capturer les options d'unité centrale, le type de location et la capacité de mise en veille prolongée à partir de la source du profil de la machine lors de la création d'un catalogue de machines MCS.
- Modifier le type de location de la source du profil de machine lors de la modification d'un catalogue de machines MCS. Cette fonctionnalité ne s'applique qu'aux machines virtuelles nouvellement ajoutées au catalogue.
- Modifier la capacité de mise en veille prolongée de la source du profil de machine lors de la modification d'un catalogue de machines MCS. Cette fonctionnalité ne s'applique qu'aux machines virtuelles nouvellement ajoutées au catalogue.

La source du profil de machine peut être une machine virtuelle ou une version du modèle de lance-

ment. Cette fonctionnalité s'applique à la fois aux catalogues persistants et non persistants.

Pour plus d'informations, consultez Créer un catalogue de machines basé sur le profil de machine à l'aide de PowerShell.

Réparer les informations d'identité des comptes d'ordinateur actifs dans AWS. Dans les environnements AWs, vous pouvez désormais réinitialiser les informations d'identité des comptes d'ordinateur 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. Actuellement, cette fonctionnalité n'est prise en charge que pour les environnements de virtualisation AWS, Azure et VMware. Pour plus d'informations, voir Réparer les informations d'identité des comptes d'ordinateurs actifs.

Prise en charge du cryptage du disque d'identité d'un catalogue de machines virtuelles MCS dans AWS. Auparavant, dans les environnements AWS, MCS n'autorisait que le cryptage du disque du système d'exploitation des machines virtuelles provisionnées. Grâce à cette fonctionnalité, vous pouvez désormais crypter le disque d'identité et le disque du système d'exploitation. Cette fonctionnalité vous permet d'utiliser des clés AWS KMS (clé gérée par le client et clé gérée par AWS) pour effectuer des opérations cryptographiques sur les disques connectés à une machine virtuelle.

Pour crypter le disque du système d'exploitation et le disque d'identité, configurez l'une des options suivantes :

- Utiliser une image principale cryptée (par exemple, une AMI créée à partir d'une instance ou un instantané contenant un volume racine crypté avec une clé KMS)
- Utiliser une source de profil de machine (machine virtuelle ou modèle de lancement) contenant un volume racine crypté.

Pour plus d'informations, consultez Crypter le disque du système d'exploitation et le disque d'identité.

Configurer des groupes de sécurité par interface réseau dans AWS. Lorsque vous modifiez une connexion hôte pour les environnements AWS, vous pouvez désormais configurer le nombre maximum de groupes de sécurité autorisés par interface réseau élastique (ENI) à l'aide d'une commande PowerShell. Ainsi, si vous augmentez le quota de groupes de sécurité par interface réseau, vous pouvez configurer la même valeur pour la connexion hôte. Pour plus d'informations sur la configuration, consultez Configurer les groupes de sécurité par interface réseau.

Optimisation des coûts [Technical Preview]. La page **Optimisation des coûts** fournit une représentation visuelle des économies d'infrastructure réalisées au cours d'une période sélectionnée et prévoit les économies attendues pour les jours restants. En analysant l'utilisation des machines et les sessions, cette page vous aide à identifier les économies réalisées et les opportunités de réduction des coûts. Cette page propose :

- Des informations détaillées sur l'optimisation des coûts d'infrastructure
- Des informations sur les économies réalisées
- Des informations sur une série de scénarios susceptibles d'entraîner un dépassement des coûts prévus
- Des opportunités potentielles d'identification et de planification stratégique pour réaliser des économies sur les coûts d'infrastructure

La page **Optimisation des coûts** affiche les **Économies estimées** et le **Rapport sur les économies réalisées avec Autoscale**.

Les **Économies estimées** permettent d'évaluer l'utilisation efficace des ressources d'infrastructure. Les économies sont affichées en dollars américains ou en pourcentage des coûts encourus. Vous pouvez consulter les résultats pour les 3, 6 et 12 derniers mois. Le graphique **Économies estimées** affiche les éléments suivants :

- Économies estimées : affiche le montant des économies d'infrastructure réalisées pendant la durée sélectionnée.
- Machines à alimentation gérée : affiche le nombre total de machines à alimentation gérée.
- Économies prévues : affiche les économies d'infrastructure qui peuvent être réalisées pour la durée restante.

Le **Rapport sur les économies réalisées avec Autoscale** affiche des informations sur le groupe de mise à disposition pour lequel Autoscale est configuré et activé. Ce rapport s'applique uniquement aux machines à alimentation gérée. Pour plus d'informations, consultez la page Optimisation des coûts.

Inspecter les machines ayant fait récemment l'objet d'une action d'alimentation. Vous pouvez désormais inspecter les machines grâce à l'état des actions d'alimentation. Cette fonctionnalité vous permet d'analyser les éléments suivants :

- Échec de mise sous tension entraînant des problèmes pour l'utilisateur
- Échec de mise hors tension qui augmente les coûts

> **Remarque :**
>
> Les données ne sont disponibles que pour les machines à alimentation gérée. Les données ne sont pas disponibles pour les actions d'alimentation effectuées avant la prise en charge de la fonctionnalité.

Vous pouvez consulter l'état des actions d'alimentation des machines de la manière suivante :

- À partir de l'onglet **Filtres** > **Machines**. Dans ce cas, les colonnes **Durée de l'action d'alimentation** et **Résultat de l'action d'alimentation** sont visibles par défaut. Vous pouvez également sélectionner les colonnes que vous souhaitez afficher.

- À partir de l'onglet **Optimisation des coûts**. Dans ce cas, le filtre par défaut **Action d'alimentation déclenchée par** est défini sur *Autoscale* et **Résultat de l'action d'alimentation** est défini sur *Échec*.

Grâce à cette fonctionnalité, vous pouvez afficher les détails des contrôles d'action d'alimentation. Par exemple, vous pouvez voir qui a déclenché l'action, quelle action a modifié l'état de l'alimentation, la raison de l'échec et l'heure à laquelle l'action s'est terminée. Vous pouvez également exporter ces informations.

Pour plus d'informations, consultez Inspecter les machines ayant fait récemment l'objet d'une action d'alimentation.

Avril 2024

Fonctionnalités nouvelles et améliorées

Prise en charge de la nouvelle version de Microsoft Teams. Citrix Monitor prend désormais en charge Microsoft Teams version 2.1 ou antérieure.

Modifier le cryptage de disque dans Azure. Grâce à cette fonctionnalité, vous pouvez désormais modifier le cryptage des disques dans les environnements de virtualisation Azure. Vous pouvez effectuer les opérations suivantes :

- Créer un catalogue de machines MCS avec un jeu de cryptage de disque (DES) différent de celui de l'image principale.
- Modifier le type de cryptage de disque en remplaçant une clé DES par une autre clé DES d'un catalogue de machines MCS et de machines virtuelles existant.
- Mettre à jour un catalogue de machines MCS et une machine virtuelle qui n'étaient pas initialement compatibles avec l'utilisation de clés CMEK afin qu'ils disposent d'un cryptage par clé de cryptage gérée par le client (CMEK) (DES), d'un cryptage de disque sur l'hôte ou d'un cryptage double.
- Mettre à jour un catalogue de machines MCS et une machine virtuelle initialement cryptés afin de supprimer le cryptage.
- Activer le cryptage de disque avec un point de terminaison privé (un catalogue de machines MCS utilisant une connexion hôte pour laquelle `ProxyHypervisorTrafficThroughConnector` est activé).

Pour plus d'informations, consultez la section Modifier le cryptage de disque.

Prise en charge de la modification des paramètres du fichier de page. Grâce à cette fonctionnalité, vous pouvez modifier les paramètres du fichier de page des machines virtuelles récemment ajoutées à un catalogue sans mettre à jour l'image principale. Actuellement, cette fonctionnalité ne s'applique qu'aux environnements Azure.

Pour modifier les paramètres du fichier de page, vous avez besoin de la version 2311 ou ultérieure du VDA. Vous pouvez modifier les paramètres du fichier de page à l'aide des commandes PowerShell. Pour plus d'informations sur la modification des paramètres du fichier de page, consultez Modifier les paramètres du fichier de page.

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 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.

Fonctionnalités obsolètes dans l'interface Configuration complète. Les fonctionnalités et paramètres suivants sont désormais obsolètes dans l'interface Configuration complète :

Prise en charge de HDX Plus pour Windows 365 PC Cloud et Azure Virtual Desktop. Monitor est désormais compatible avec HDX Plus pour Windows 365 PC Cloud et Azure Virtual Desktop (AVD). Pour plus d'informations, consultez la section Dépanner les machines.

Modification du compte de service Cloud Build. GCP apporte des modifications au comportement par défaut des services Cloud Build et à l'utilisation des comptes de service dans les nouveaux projets créés après le 29 avril 2024. Pour plus d'informations, consultez la page Modification d'un compte de service Cloud Build. Cependant, vos projets Google et vos catalogues Citrix existants ne sont pas concernés par cette modification. Pour plus d'informations, consultez :

- Configuration et mise à jour des comptes de service
- Autorisations GCP requises

Prise en charge de HDX Plus pour Windows 365 PC Cloud et Azure Virtual Desktop. Monitor est désormais compatible avec HDX Plus pour Windows 365 PC Cloud et Azure Virtual Desktop (AVD). Pour plus d'informations, consultez la section Dépanner les machines.

Environnements VDA avec proxys pour Internet et filtrage d'URL (Technical Preview). Vous pouvez désormais utiliser le service de mise à niveau des VDA pour mettre à jour les VDA lorsque vous disposez de proxys pour la connectivité Internet et le filtrage Web. Le proxy configuré dans la stratégie a priorité sur le proxy configuré dans le registre. Pour plus d'informations, consultez la section Installer des VDA. Consultez également la liste des URL qui doivent figurer sur une liste blanche dans le proxy.

Modification du compte de service Cloud Build. GCP apporte des modifications au comportement par défaut des services Cloud Build et à l'utilisation des comptes de service dans les nouveaux projets créés après le 29 avril 2024. Pour plus d'informations, consultez la page Modification d'un compte de service Cloud Build. Cependant, vos projets Google et vos catalogues Citrix existants ne sont pas concernés par cette modification. Pour plus d'informations, consultez :

- Configuration et mise à jour des comptes de service
- Autorisations GCP requises

Mars 2024

Fonctionnalités nouvelles et améliorées

Enregistrement de session dynamique. Vous pouvez désormais enregistrer la session active en cours à l'aide des commandes d'enregistrement de session depuis l'écran **Détails de l'utilisateur** sans avoir à rétablir la session. Cette fonctionnalité permet de résoudre plus rapidement et efficacement les problèmes liés à l'expérience des sessions rencontrés par les utilisateurs. Ceci est utile pour résoudre les problèmes difficiles à reproduire.

Pour en savoir plus sur l'enregistrement dynamique de session, consultez l'article sur le service d'enregistrement de session.

Outil d'inscription pour enregistrer des VDA à l'aide de WebSockets pour les catalogues de machines. Vous pouvez désormais utiliser l'outil d'inscription pour enregistrer en toute sécurité vos VDA non associés à un domaine dans les catalogues de machines. Cette fonctionnalité offre l'avantage d'utiliser uniquement le port TLS 443 pour la communication entre le VDA et le Delivery Controller, et de supprimer le trafic du port 80. Pour plus d'informations, consultez la section Inscrire des machines à des catalogues à l'aide de l'outil d'inscription de VDA WebSocket.

Mises à jour des sous-réseaux simplifiées pour les catalogues de machines. Auparavant, pour modifier les paramètres de sous-réseau d'un catalogue de machines, vous deviez le supprimer, puis

le recréer. Grâce à cette fonctionnalité, vous pouvez désormais obtenir le même résultat en modifiant simplement le catalogue. Notez que seules les nouvelles machines virtuelles créées dans le catalogue figureront sur les nouveaux sous-réseaux associés. Cette amélioration réduit la nécessité de supprimer le catalogue et les tâches associées. Pour plus d'informations, consultez la section Modifier un catalogue.

Configuration complète : prise en charge de la mise à jour d'un plus grand nombre de paramètres de machine virtuelle Azure à l'aide de profils de machine. L'interface Configuration complète vous permet désormais de mettre à jour un plus large éventail de paramètres pour les machines virtuelles Azure provisionnées par MCS via des profils de machine, notamment :

- Taille de la machine
- Type de licence
- Zone de disponibilité
- ID de groupe d'hôtes dédié

Après avoir mis à jour le profil de la machine, l'interface Configuration complète compare les paramètres actuels avec les nouveaux paramètres. S'il existe des différences, vous êtes invité à confirmer lesquels appliquer. Ceci garantit des mises à jour transparentes et efficaces des paramètres des machines virtuelles.

Configuration complète : prise en charge de la modification des propriétés du cache en écriture différée pour les machines virtuelles Azure provisionnées par MCS. Pour les machines virtuelles Azure provisionnées à l'aide de MCS (Machine Creation Services), vous pouvez désormais modifier les propriétés de cache en écriture différée (WBC) à l'aide de l'interface Configuration complète, notamment : **Taille du cache disque**, **Taille du cache mémoire** et **Activer la réduction des coûts de stockage**. En outre, lorsque vous sélectionnez une nouvelle taille de machine ou un nouveau profil de machine pour ces machines virtuelles, l'interface Configuration complète valide les paramètres WBC afin d'éviter les conflits, tels que le dépassement de la limite de mémoire de la nouvelle sélection. En cas de conflit, vous serez invité à reconfigurer les paramètres WBC.

Février 2024

Fonctionnalités nouvelles et améliorées

Suspendre les machines virtuelles depuis l'interface Workspace. Vous pouvez désormais suspendre les machines virtuelles persistantes dont les sessions sont actives depuis l'interface utilisateur de Workspace. Cette amélioration offre les avantages suivants :

- Reprise du système là où vous vous étiez arrêté.
- Temps de lancement plus rapide par rapport à une machine désallouée arrêtée.
- Rentabilité et économies d'énergie.

- Allocation efficace des ressources à l'aide de la fonctionnalité Autoscale.

Nouvelle prise en charge de l'optimisation du stockage (MCSIO) de Machine Creation Services (MCS) : le service de portabilité des images permet désormais d'ajouter ou de supprimer l'option MCSIO lorsque vous préparez une image pour le provisioning MCS.
Pour plus d'informations, consultez Automatiser la configuration du VDA.

Amélioration de la présentation des analyses : un résumé des mesures d'analyse et des étapes de défaillance d'analyse est désormais disponible sur la page **Analyse** > **Présentation**. Les mesures d'analyse indiquent le nombre d'exécutions planifiées, échouées, ignorées et réussies. Le graphique des étapes de défaillance permet d'analyser les étapes au cours desquelles la plupart des défaillances se sont produites. Ces informations permettent de résoudre rapidement les problèmes liés aux résultats d'analyse. Pour en savoir plus, voir Analyse d'applications et de bureaux.

Informations sur les images de la page Catalogues de machines. Vous pouvez désormais afficher les informations d'image suivantes via les **Propriétés du modèle** du catalogue de machines :

- Système d'exploitation
- Machine Identity Service
- Stockage Machine Creation Service
- Chemin de fichier pour `pagefile.sys` pour les déploiements Azure

Ce changement améliore la clarté des informations sur les images et garantit que les administrateurs disposent de toutes les informations sur le catalogue de machines en un seul endroit.

Prise en charge de l'interface Configuration complète pour la gestion des jetons d'inscription du VDA. L'inscription d'un VDA basé sur des jetons réduit la charge sur les Cloud Connector et diminue les points de défaillance potentiels, ce qui est idéal pour les cas d'utilisation où vous préparez les machines à l'aide d'une technologie autre que Citrix Provisioning. L'interface Configuration complète vous permet désormais de générer et de gérer des jetons d'inscription pour les VDA non provisionnés par Citrix, rationalisant ainsi les déploiements basés sur des jetons d'inscription. Pour plus d'informations, consultez Générer et gérer des jetons d'inscription.

Journalisation PowerShell. Dans l'interface Configuration complète, vous pouvez désormais afficher les commandes PowerShell correspondant aux actions quotidiennes de votre interface utilisateur. Cette fonctionnalité vous permet de mieux comprendre les commandes PowerShell sous-jacentes à des fins d'apprentissage. Pour afficher les journaux PowerShell, cliquez sur **Logging > PowerShell**. Pour plus d'informations, consultez la section Journalisation de la configuration.

Activez le cache d'hôte local (LHC) pour les VDA regroupés à session unique à l'aide de l'interface Configuration complète. Par défaut, les VDA regroupés à session unique provisionnés à l'aide de MCS ou Citrix Provisioning ne sont pas disponibles en mode LHC. L'interface Configuration complète vous permet désormais de modifier ce comportement par défaut pour chaque groupe de mise à disposition, afin de rendre ces VDA disponibles pour les nouvelles connexions pendant le LHC. Pour

plus d'informations, consultez Créer des groupes de mise à disposition et Gérer des groupes de mise à disposition.

Citrix Hypervisor a été renommé XenServer dans l'interface Configuration complète. Conformément à notre stratégie de changement de nom, nous avons remplacé toutes les instances de Citrix Hypervisor dans l'interface Configuration complète par XenServer.

Vue des sauts réseau de bout en bout. La visualisation des sauts réseau de bout en bout constitue la prochaine étape vers l'amélioration des workflows de dépannage dans Citrix Monitor. 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. Le chemin de session permet de comprendre les composants impliqués dans le chemin de session avec leurs métadonnées, le lien entre les composants et les applications publiées sur le VDA. La topologie de session facilite les flux de données et permet d'identifier les sauts spécifiques susceptibles d'entraîner des problèmes de performances.

De plus, les indicateurs Latence ICA et RTT ICA sont affichés pour la session lorsqu'elle est connectée. Pour en savoir plus, voir Affichage des sauts de réseau de bout en bout.

Utilisez le Disk Encryption Set ID (DES ID) de l'image principale pour chiffrer tous les disques des machines virtuelles du catalogue. Auparavant, dans les environnements Azure, le Disk Encryption Set ID (DES ID) d'un catalogue de machines MCS était dérivé d'un profil de machine ou de propriétés personnalisées. Grâce à cette fonctionnalité, un catalogue de machines peut également dériver du DES ID à partir de l'image principale pour chiffrer tous les disques de machines virtuelles d'un catalogue.

Mettez à jour les balises MCS pour détecter les ressources orphelines après la migration. Lorsque vous faites migrer une configuration locale vers un site cloud ou une configuration cloud vers un autre site cloud, les ressources orphelines ne sont pas détectées correctement en raison de l'ancienne balise d'identification du site. Grâce à cette fonctionnalité, vous pouvez mettre à jour à l'aide d'une commande PowerShell les balises d'identification de site MCS d'un catalogue persistant après la migration, afin que les ressources orphelines puissent être détectées correctement. Actuellement, cette fonctionnalité est applicable à Azure. Pour plus d'informations, consultez Mettre à jour les balises MCS pour détecter les ressources orphelines après la migration.

Validez la configuration avant de créer un catalogue de machines MCS. Cette fonctionnalité vous permet désormais de valider les paramètres de configuration avant de créer un catalogue de machines MCS à l'aide du paramètre `-validate` dans la commande `New-ProvScheme`. Après avoir exécuté cette commande PowerShell avec le paramètre, un message d'erreur approprié s'affiche si un paramètre incorrect est utilisé ou si un paramètre est en conflit avec un autre paramètre. Vous pouvez ensuite utiliser le message d'erreur pour résoudre le problème, puis créer le catalogue de machines MCS à l'aide de PowerShell.

Actuellement, cette fonctionnalité est applicable aux environnements de virtualisation Azure, GCP et VMware. Pour plus d'informations, consultez Valider la configuration avant de créer un catalogue de

machines MCS.

Prise en charge de la copie de balises depuis une source de profil de machine vers une machine virtuelle dans AWS. Dans les environnements AWS, cette fonctionnalité vous permet de copier les balises des cartes réseau et des disques (disque d'identité, disque cache en écriture différée et disque du système d'exploitation) indiqués dans le profil de la machine vers des machines virtuelles nouvellement créées dans un catalogue de machines MCS. Vous pouvez indiquer ces balises dans n'importe quelle source de profil de machine (instance AWS EC2 ou version du modèle de lancement AWS). Cette fonctionnalité s'applique aux catalogues de machines et de machine virtuelle persistants et non persistants. Pour en savoir plus, voir Copier les balises sur les machines virtuelles.

Prise en charge de SCVMM pour le profil de la machine. Grâce à cette fonctionnalité, vous pouvez désormais 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. Pour en savoir plus, voir Créer un catalogue à l'aide d'un profil de machine.

Prise en charge d'Azure pour l'utilisation de machines virtuelles Spot avec MCS. Les machines virtuelles Azure Spot vous permettent d'exploiter la capacité de calcul inutilisée d'Azure tout en réalisant des économies importantes. En raison de leur stratégie d'éviction, les machines virtuelles Azure Spot ne sont toutefois adaptées qu'à certaines applications et bureaux non essentiels.

Grâce à cette fonctionnalité, vous pouvez créer un catalogue de machines MCS de machines virtuelles Azure Spot à l'aide d'un profil de machine (spécification de machine virtuelle ou de modèle). Vous pouvez mettre à jour un catalogue existant pour que les machines virtuelles Azure Spot soient les machines virtuelles nouvellement créées ou passer à des machines virtuelles Azure standard. Vous pouvez également mettre à jour les machines virtuelles existantes pour les transformer en machines virtuelles Azure Spot. Pour en savoir plus, voir Créer un catalogue à l'aide de machines virtuelles Azure Spot.

Prise en charge de la capture des paramètres de diagnostic à partir d'un profil de machine. Dans les environnements Azure, MCS prend désormais en charge la capture des paramètres de diagnostic sur les machines virtuelles et les cartes d'interface réseau à partir d'un profil de machine lors de la création ou de la mise à jour d'un catalogue de machines MCS ou de la mise à jour de machines virtuelles existantes. Grâce à cette fonction, les données de diagnostic peuvent donc être transmises de manière fluide à des points de terminaison Azure désignés, tels que les espaces de travail Log Analytics ou les Event Hubs, pour une analyse et une visualisation approfondies. Pour en savoir plus, voir Capturer des paramètres de diagnostic sur des machines virtuelles et des cartes d'interface réseau à partir d'un profil de machine.

Prise en charge de MCS pour gérer les différentes versions d'un catalogue de machines. Grâce à cette fonctionnalité, vous pouvez gérer les versions de configuration d'un catalogue de machines à l'aide des commandes PowerShell. Chaque modification de configuration utilise les résultats `Set-ProvScheme` dans une nouvelle version de configuration. Vous pouvez :

- Afficher la liste des versions.
- Utiliser n'importe quelle version précédente pour mettre à jour un catalogue de machines.
- Supprimer manuellement une version si elle n'est pas utilisée par une machine virtuelle.
- Modifier le nombre maximum de versions à conserver par un catalogue de machines.

Pour en savoir plus, voir Gérer les versions d'un catalogue de machines.

Publiez des applications App-V, MSIX et packagées via l'attachement d'application MSIX sur des VDA de bureau mono-session et partagés. Vous pouvez désormais accéder à des applications packagées, telles qu'App-V, MSIX et l'attachement d'application MSIX sur les VDA de bureau mono-session et partagés. Cette amélioration garantit que les applications packagées sont facilement disponibles lorsque vous vous connectez. Cette fonctionnalité accélère le lancement des applications packagées et améliore considérablement votre expérience en la rapprochant de l'accès à une application installée localement. Pour en savoir plus, voir Publier des applications packagées sur des VDA de bureau à session unique ou partagés.

Visionnez les sessions en direct et enregistrées : Citrix Monitor prend désormais en charge la lecture de sessions utilisateur en direct et enregistrées à l'aide du service d'enregistrement de session. Vous pouvez rapidement comprendre les problèmes liés à la session rencontrés par l'utilisateur dès la rediffusion. Cette fonctionnalité vous permet d'accéder facilement aux enregistrements ainsi qu'aux statistiques relatives aux sessions dans la console Monitor. Il permet de relier les problèmes découverts dans les enregistrements avec les mesures de performance. Il n'est plus nécessaire de rechercher des enregistrements sur plusieurs serveurs d'enregistrement de session ou de rechercher des applications tierces pour visualiser les enregistrements.

Cette fonctionnalité nécessite un VDA et le serveur d'enregistrement de session version 2308 ou ultérieure.

Monitor stocke les enregistrements dans un référentiel centralisé et les affiche dans la fenêtre modale **Sélecteur de session**. Le lien **Sessions avec enregistrements** affiche les enregistrements des sessions qui ont été actives au cours des dernières 24 heures ou des 2 derniers jours. L'enregistrement est lu dans un nouvel onglet à l'aide du serveur de lecture Citrix Session Recording.

Pour en savoir plus, voir Enregistrer des sessions.

Optimisation Microsoft Teams : Monitor affiche l'état de l'optimisation HDX disponible pour Microsoft Teams. La nouvelle **optimisation de Microsoft Teams** peut être consultée dans la page **Détails de l'utilisateur** > panneau **Détails de la session**. Monitor affiche le statut d'optimisation de Microsoft Teams uniquement si Microsoft Teams est exécuté en tant qu'application publiée ou sur un bureau publié. Cette amélioration fournit aux administrateurs une visibilité leur permettant de résoudre les problèmes de performances des sessions sur Microsoft Teams signalés par les utilisateurs. Pour de plus amples informations, consultez la section Résoudre les problèmes utilisateur.

Améliorations de l'interface utilisateur : l'interface utilisateur de Citrix Monitor est désormais actualisée avec une apparence moderne. La nouvelle interface utilisateur améliorée facilite la navigation

et améliore la représentation des données. L'expérience améliorée est intuitive et conçue pour inclure facilement les données requises afin de surveiller et dépanner une session Citrix.

Résolution d'écran optimale : la résolution d'écran optimale recommandée pour l'affichage de Citrix Monitor a été mise à jour sur 1440 x 1024.

Janvier 2024

Fonctionnalités nouvelles et améliorées

Amélioration de la configuration de redirection bidirectionnelle du contenu Auparavant, la configuration de la redirection bidirectionnelle du contenu 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 (configurées dans **DaaS > Configuration complète**) 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.

Prise en charge du redémarrage et de l'arrêt des machines mono-session à partir de l'onglet Sessions du nœud Rechercher. Dans l'onglet **Sessions** du nœud **Rechercher**, vous pouvez désormais rechercher les sessions utilisateur défaillantes et redémarrer ou arrêter facilement les machines mono-session associées dans le même onglet. Cette fonctionnalité améliore l'efficacité en permettant d'agir rapidement sur les problèmes de session identifiés au sein d'une interface unique.

Prise en charge de l'accès au service de configuration globale des applications à partir de Configuration complète. Nous avons fourni des actions dans l'interface Configuration complète pour vous associer au service de configuration globale des applications. Grâce à cette intégration, vous pouvez facilement accéder à la configuration globale des applications pour gérer les paramètres de l'utilisateur final via Configuration complète.

Pour accéder à ce service depuis Configuration complète, deux options s'offrent à vous :

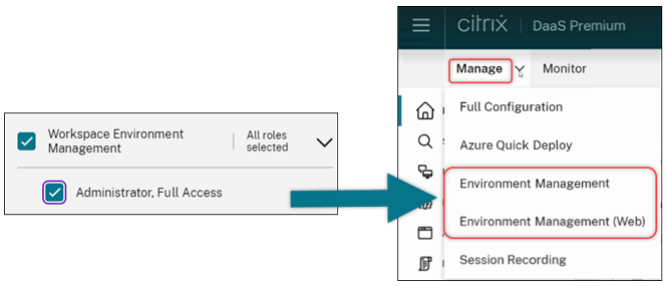
- Sélectionnez le nœud **StoreFront**, cliquez sur un enregistrement de serveur, puis sélectionnez **Configurer les paramètres du client** dans la barre d'action.
- Sélectionnez le nœud **Stratégies**, puis **Configurer les paramètres du client** dans la barre d'actions.

Prise en charge de la gestion des attributions d'utilisateur pour les groupes de mise à disposition gérés par Citrix Cloud à l'aide de Configuration complète. Dans le cadre de notre plan de migration de la gestion des attributions d'utilisateur de la bibliothèque cloud vers Configuration complète, vous pouvez désormais gérer les attributions d'utilisateur pour les groupes de mise à dispo-

sition gérés par Citrix Cloud via Configuration complète. Pour cela, modifiez un groupe de mise à disposition cible dans **Configuration complète > Groupes de mise à disposition** et désignez les utilisateurs autorisés à utiliser des bureaux ou des applications via l'un des menus suivants : **Bureaux** (ou **Règles d'attribution de bureau**) ou **Règle d'attribution d'application**. Pour de plus amples informations, consultez la section Gérer les groupes de mise à disposition.

Les mises à jour effectuées sur un portail sont parfaitement synchronisées avec l'autre, garantissant ainsi la cohérence des mises à jour sur les deux portails.

Limitation de l'accès à la console WEM au rôle d'administrateur WEM à accès complet. Nous avons activé le contrôle d'accès pour les consoles Workspace Environment Management (WEM) afin d'empêcher toute entrée non autorisée. Seuls les utilisateurs dotés du rôle d'**administrateur à accès complet à Workspace Environment Management** peuvent désormais utiliser **DaaS > Gérer** pour accéder aux consoles WEM.



Configuration complète : les catalogues Azure prennent en charge l'héritage des paramètres DES provenant des images principales. Auparavant, Configuration complète définissait les paramètres DES par défaut des catalogues Azure uniquement en fonction des profils de machine. Nous avons maintenant étendu cette capacité. Grâce à cette amélioration, dans les cas suivants, Configuration complète définit les paramètres DES par défaut d'un catalogue Azure directement en fonction de l'image principale :

- Si aucun profil de machine n'est sélectionné
- Si le profil spécifie une clé PMK (Platform Managed Key)

Pour plus d'informations, consultez la section Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans l'interface Configuration complète.

Recherche améliorée : davantage de filtres pour une plus grande précision. Nous avons amélioré la recherche sur le nœud Rechercher pour inclure deux nouveaux filtres, Zone et Type de provisioning, pour une plus grande précision et une facilité d'utilisation accrue.

Configuration complète : prise en charge de la sélection du type de machine Google Cloud pour les catalogues de machines GCP. Grâce à cette fonctionnalité, les administrateurs peuvent sélectionner les configurations de mémoire et de processeur requises pour les machines virtuelles GCP provisionnées, en les adaptant à des exigences opérationnelles spécifiques. Pour plus d'informations, consultez la section Créer un catalogue de machines à l'aide de l'interface Configuration complète.

Prise en charge des clés de cryptage, mondiales et régionales, gérées par le client (CMEK) pour le provisioning des machines virtuelles GCP. Vous pouvez désormais utiliser des clés CMEK mondiales et régionales pour provisionner des machines virtuelles à partir de n'importe quel projet de provisioning. Cette amélioration offre une plus grande flexibilité dans la sélection des clés pour le provisioning des machines virtuelles et l'amélioration de la sécurité des machines virtuelles.

Décembre 2023

Fonctionnalités nouvelles et améliorées

Progression de l'envoi de message. Vous pouvez désormais consulter la progression de l'opération d'**envoi de message** dans **Surveiller** > **Filtres**. Cette opération permet d'envoyer des messages en masse à toutes les sessions connectées à votre site. La progression de l'opération s'affiche en pourcentage. Une fois l'opération terminée, le système affiche le nombre de messages envoyés et le nombre d'échecs. L'état d'envoi des messages s'avère utile pour administrer des sites volumineux. Il vous permet de déterminer si le message doit être renvoyé à certains utilisateurs. L'envoi de messages peut échouer si les machines ne sont pas enregistrées ou si les sessions sont défectueuses. Pour plus d'informations sur l'envoi d'un message, consultez Envoyer des messages aux utilisateurs.

Prise en charge de l'authentification Citrix Probe Agent via Citrix Gateway avec des informations d'identification de domaine et de l'authentification multifacteur.

Citrix Probe Agent pour l'analyse d'applications et de bureaux prend désormais en charge l'authentification via Citrix Gateway avec des informations d'identification de domaine et l'authentification multifacteur. Cette prise en charge permet d'exécuter Probe Agent sur des machines connectées à StoreFront via Citrix Gateway. Les résultats d'analyse complets disponibles dans Director peuvent aider à résoudre les problèmes liés aux applications, à la machine d'hébergement ou à la connexion avant que les utilisateurs ne les rencontrent. La prise en charge de Citrix Gateway avec l'authentification multifacteur n'est disponible que pour Citrix Gateway configuré avec LDAP et OTP natif à l'aide d'un schéma de connexion unique. Pour plus d'informations, consultez Analyse d'applications et de bureaux

Remaniement de l'interface utilisateur des stratégies d'accès pour un contrôle d'accès aux ressources plus flexible. Nous avons repensé l'interface utilisateur **Modifier le groupe de mise à disposition > Stratégie d'accès** afin de vous donner plus de flexibilité dans la gestion de l'accès aux ressources pour les groupes de mise à disposition. Voici les principales fonctionnalités disponibles avec le nouveau design :

- **Prise en charge de l'ajout de stratégies.** Vous pouvez désormais ajouter des stratégies d'accès pour limiter l'accès aux ressources en fonction des attributs des connexions utilisateur. Une stratégie peut comprendre deux types de critères :

  - **Critères d'inclusion.** Vous permettent de spécifier les connexions utilisateur autorisées à accéder au groupe de mise à disposition.
  - **Critères d'exclusion.** Vous permettent de spécifier les connexions utilisateur qui ne sont pas autorisées à accéder au groupe de mise à disposition.

- **Prise en charge des filtres étendue.** Vous pouvez désormais définir des critères d'inclusion et d'exclusion à l'aide d'une gamme de filtres SmartAccess. Ces filtres incluent des filtres Workspace, comme `Citrix.Workspace.UsingDomain`et `Citrix-Via-Workspace`, ainsi que des filtres pour l'accès adaptatif en fonction de l'emplacement réseau.
- **La logique Correspondance exacte prend en charge les critères inclus.** La nouvelle logique vous permet d'atteindre un niveau de précision et de contrôle élevé lorsque vous spécifiez les connexions utilisateur autorisées pour les groupes de mise à disposition.

Pour plus d'informations, consultez la section Restreindre l'accès aux ressources dans un groupe de mise à disposition.

Novembre 2023

Fonctionnalités nouvelles et améliorées

Prise en charge de la création de catalogues Citrix Provisioning à l'aide de l'interface Configuration complète. Pour créer un catalogue Citrix Provisioning, vous deviez utiliser l'assistant d'installation Citrix Virtual Apps and Desktops. Grâce à cette fonctionnalité, vous pouvez désormais 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. Pour plus d'informations, consultez la section Créer des catalogues Citrix Provisioning dans Citrix Studio.

Présentation de la recherche de groupes d'applications. Nous avons introduit la fonctionnalité de recherche pour les groupes d'applications dans le nœud **Applications**. Grâce à cette amélioration, vous pouvez désormais rechercher directement un groupe d'applications dans n'importe quel dossier d'applications. Pour plus d'informations, consultez la section Rechercher des groupes d'applications.

Limites de configuration modifiées. Le tableau suivant décrit les modifications apportées aux limites de configuration de DaaS afin d'améliorer les performances et de garantir un meilleur rapport coût-efficacité.

Ressource	Ancienne limite	Nouvelle limite
Domaines Active Directory	85	100
Catalogues	1 000	2 000
Groupes de mise à disposition	1 000	2 000
Emplacement de ressources	85	100
Emplacement des ressources -> Nombre total de sessions	20 000	25 000

Pour plus d'informations, consultez la section Limites.

Une option unique pour conserver la machine virtuelle et le disque système pendant les cycles d'alimentation. Le démarrage d'une machine virtuelle existante sur Azure est désormais plus rapide que le lancement d'une nouvelle machine virtuelle, ce qui en fait un choix plus efficace pour conserver les machines virtuelles pendant tous les cycles d'alimentation. En réponse à ce changement, nous avons combiné les options **Conserver les machine virtuelle durant les cycles d'alimentation** et **Conserver le disque système pendant les cycles d'alimentation** en une seule option **Conserver la machine virtuelle et le disque système pendant les cycles d'alimentation**. Cela signifie que lorsque vous sélectionnez cette option pour réduire les temps de redémarrage des machines virtuelles en conservant les disques système, vos machines virtuelles sont également conservées.

Nouvelle fonctionnalité de l'interface Configuration complète permettant de filtrer les tailles des machines en fonction de la *propriété de cryptage sur l'hôte* définie dans les profils de machine (spécifique aux machines virtuelles Azure). Une fois que vous avez choisi un profil de machine avec *Chiffrement sur l'hôte* activé lors de la création ou de la gestion du catalogue de machines Azure, seules les tailles de machines prenant en charge cette fonctionnalité sont affichées.

Limiter les actions de sauvegarde et de restauration au rôle d'administrateur complet. Nous avons amélioré le contrôle d'accès pour les actions de sauvegarde et de restauration. Seuls les utilisateurs dotés du rôle d'administrateur complet peuvent désormais accéder au nœud **Sauvegarde + Restauration**, empêchant ainsi les actions non autorisées.

Mise en cache des données pour le nœud Recherche. Nous avons introduit la mise en cache des données pour le nœud **Recherche** de Citrix DaaS. Ce changement améliore les performances de la recherche et la liste suivante répertorie les cas d'utilisation qui facilitent vos tâches habituelles :

- Affichage rapide des résultats de recherche une fois qu'ils ont été récupérés pour la première fois.
- Conserve les résultats de pagination après avoir navigué depuis le nœud **Recherche** et y être retourné.

Informations sur les images de la page Catalogues de machines. Vous pouvez désormais afficher les informations d'image suivantes via les **Propriétés du modèle** du catalogue de machines :

- Système d'exploitation
- Machine Identity Service
- Stockage Machine Creation Service
- Chemin de fichier pour `pagefile.sys` pour les déploiements Azure.

Ce changement améliore la clarté des informations sur les images et garantit que les administrateurs disposent de toutes les informations sur le catalogue de machines en un seul endroit.

Prise en charge de l'épinglage des filtres de recherche. Pour fournir une expérience de recherche rapide, Configuration complète permet d'épingler vos filtres de recherche. Les épingles de filtre vous permettent de garder les filtres de recherche fréquemment utilisés accessibles sur la page. Cette amélioration est disponible dans les panneaux de recherche des nœuds suivants :

- **Rechercher**
- **Catalogues de machines**
- **Groupes de mise à disposition**
- **Applications**

Pour plus d'informations, voir Utiliser la recherche dans l'interface de gestion Configuration complète.

Prise en charge de l'association de métadonnées aux journaux de configuration. Grâce à cette amélioration, vous pouvez désormais associer des métadonnées aux journaux de configuration en associant une paire `name-value` sur les opérations de haut niveau. Pour plus d'informations, voir Associer des métadonnées aux journaux de configuration.

Ignorer les ressources orphelines avec une balise spécifique. Dans les environnements Azure, une ressource gérée par le client balisée avec toutes les balises Citrix est détectée comme ressource orpheline. Avec cette fonctionnalité, si vous ajoutez une autre balise `CitrixDetectIgnore` dont la valeur est true pour cette ressource, la ressource est ignorée lors de la détection des ressources orphelines.

Solution au problème de duplication du GUID SCCM. Après avoir créé plusieurs machines virtuelles à l'aide de MCS, System Center Configuration Manager (SCCM) n'affichait qu'une seule machine virtuelle sur sa console en raison de la duplication des GUID. Ce problème est désormais résolu en ajoutant une étape dans la préparation de l'image. Cette étape supprime les certificats existants et les informations GUID dans l'image principale. L'étape est activée par défaut.

Réparer les informations d'identité des comptes d'ordinateur actifs. Cette fonctionnalité vous permet de 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 persistants et non persistants. Actuellement, cette fonctionnalité n'est prise en charge que pour les environnements de virtualisation Azure et VMware. Pour plus d'informations, voir Réparer les informations d'identité des comptes d'ordinateurs actifs.

Associer des informations de chiffrement sur l'hôte à un profil de machine. Dans les environnements Azure, grâce à cette fonctionnalité, vous pouvez désormais savoir si le chiffrement sur l'hôte est activé pour une entrée de profil de machine (machine virtuelle ou spécification de modèle) à l'aide des commandes PowerShell. Pour plus d'informations, voir Récupérer les informations de chiffrement sur l'hôte à partir d'un profil de machine.

Réparer les certificats utilisateur des identités de machines jointes à Azure AD hybride. Grâce à cette fonctionnalité, vous pouvez utiliser une commande Powershell pour réparer les certificats utilisateur des identités de machines jointes à Azure AD hybride s'ils sont corrompus ou ont expiré. Pour plus d'informations, consultez la section Créer des catalogues joints à Azure Active Directory hybride.

Prise en charge des avertissements d'expiration de certificats pour les catalogues de machines joints à Hybrid Azure AD. Configuration complète fournit désormais des avertissements un mois à l'avance en cas d'expiration des certificats utilisateur sur les catalogues de machines joints à Hybrid Azure AD. Cette amélioration vise à réduire le risque d'interruptions de service résultant de l'expiration du certificat. Pour afficher les détails et les actions recommandées, accédez au nœud **Catalogues de machines**, sélectionnez le catalogue de machines, puis cliquez sur l'onglet **Dépannage**.

Vous pouvez exécuter la commande `Get-ProvScheme` pour obtenir des informations sur la date d'expiration du certificat utilisateur d'un catalogue hybride de machines jointes à Azure AD.

Prise en charge des machines virtuelles confidentielles Azure (Technical Preview). Les machines virtuelles informatiques confidentielles Azure garantissent que votre bureau virtuel est chiffré en mémoire et protégé lors de son utilisation. Grâce à cette fonctionnalité, vous pouvez désormais 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 (Technical Preview).

Prise en charge de la conversion d'un catalogue de machines non basé sur un profil de machine vers un catalogue de machines basé sur un profil de machine dans l'environnement AWS. Dans un environnement AWS, vous pouvez désormais utiliser une machine virtuelle ou un modèle de lancement 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 prennent les valeurs de propriété du profil de la machine. Pour plus d'informations, voir Convertir un catalogue de machines non basé sur un profil de machine vers un catalogue de machines basé sur un profil de machine.

Prise en charge du plug-in HPE Moonshot géré par Citrix (Technical Preview). Auparavant, vous utilisiez le plug-in Moonshot géré par HPE (HPE Moonshot Machine Manager) géré par Hewlett Packard Enterprise (HPE) pour effectuer les actions de gestion de l'alimentation sur le châssis HPE Moonshot. Le plug-in était basé sur des API existantes qui compliquaient les projets d'infrastructure MCS. Avec cette fonctionnalité, un plug-in HPE Moonshot géré par Citrix (HPE Moonshot) est disponible. 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 à l'aide de l'interface Configuration complète et des commandes PowerShell. Pour plus d'informations, consultez :

- Environnements de virtualisation HPE Moonshot (Technical Preview)
- Connexion à HPE Moonshot (Technical Preview)
- Créer un catalogue de machines HPE Moonshot (Technical Preview)
- Gérer un catalogue HPE Moonshot (Technical Preview)

Possibilité de modifier la taille du cache du disque et de la mémoire. Grâce à cette fonctionnalité, vous pouvez désormais modifier la mémoire et la taille du cache disque du cache à écriture différée (lorsque MCSIO est activé) à l'aide d'une commande PowerShell sans créer de nouveau catalogue de machines. Cette implémentation vous permet de disposer d'une configuration de cache optimisée adaptée aux besoins de votre entreprise. Cette fonctionnalité s'applique aux éléments suivants :

- des environnements GCP et Microsoft Azure, et
- un catalogue non persistant avec MCSIO activé

Pour plus d'informations, voir Modifier la configuration du cache sur un catalogue de machines existant.

Prise en charge de la création d'un catalogue activé par clé de chiffrement géré par le client. Dans les environnements Azure, vous pouvez désormais créer un catalogue Citrix Provisioning activé avec une clé de chiffrement gérée par le client (CMEK) à l'aide de l'interface Configuration complète et des commandes PowerShell. Pour plus d'informations, voir Créer un catalogue activé par une clé de chiffrement gérée par le client.

Possibilité de copier des balises sur toutes les ressources dans Azure. Avec cette fonctionnalité, dans un environnement Azure, 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. Pour plus d'informations, voir Copier les balises sur toutes les ressources.

État de la session réglé sur déconnectée après la suspension de la machine. Auparavant, après la suspension d'une machine virtuelle, la session était toujours affichée comme **active**. Grâce à cette

amélioration, une fois que vous avez suspendu une machine virtuelle, l'état de la session associée est désormais affiché comme **Déconnecté**.

Prise en charge de la création de machines virtuelles AWS compatibles avec la mise en veille prolongée. Vous pouvez désormais créer des catalogues de machines compatibles avec la mise en veille prolongée des machines virtuelles dans vos environnements AWS, améliorant ainsi la rentabilité globale de votre déploiement. Vous pouvez également modifier un catalogue pour inclure des machines virtuelles compatibles avec la mise en veille prolongée si le profil de machine associé prend en charge cette fonctionnalité. Pour plus d'informations, consultez Gérer l'alimentation des machines virtuelles AWS.

Prise en charge de la configuration des méthodes d'équilibrage de charge au niveau du groupe de mise à disposition (Technical Preview). Cette fonctionnalité vous permet de choisir la méthode d'**Équilibrage de charge vertical** au niveau du groupe de mise à disposition. Grâce à cette fonctionnalité, chaque machine est alignée sur l'indice de charge maximal avant que la machine suivante ne soit mise sous tension. Autoscale et l'équilibrage de charge vertical déterminent le moment où la prochaine machine sera mise sous tension. Cette fonctionnalité permet une utilisation maximale de chaque machine et des économies de coûts dans les clouds publics. Cette fonctionnalité offre une plus grande flexibilité dans la gestion des stratégies d'équilibrage de charge pour les machines.

Vous pouvez configurer un groupe de mise à disposition pour hériter de la méthode d'équilibrage de charge à partir des paramètres au niveau du site ou remplacer la méthode d'équilibrage de charge au niveau du site et choisir à la place l'une des méthodes d'équilibrage de charge vertical ou horizontal. Pour plus d'informations, reportez-vous à l'étape 2. Équilibrage de charge.

Prise en charge des machines virtuelles compatibles avec la mise en veille prolongée dans Azure (Technical Preview). 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. Pour plus d'informations, voir Créer des machines virtuelles compatibles avec la mise en veille prolongée dans Azure (Technical Preview).

Guide de démarrage DaaS. Nous avons publié un nouveau guide pour rationaliser et simplifier le déploiement et la configuration de DaaS pour les administrateurs débutants et expérimentés. Il offre les principaux avantages suivants :

- **Démarrage facile.** En utilisant une approche étape par étape basée sur des questionnaires, ce guide aide les nouveaux administrateurs à configurer rapidement leurs déploiements. Des informations d'aide contextuelles tout au long du guide aident à comprendre les concepts et la terminologie essentiels.
- **Simplification des configurations complexes.** Ce guide inclut des paramètres préconfigurés, le cas échéant, et donne accès à l'interface utilisateur Configuration complète pour une configuration avancée. Les administrateurs expérimentés peuvent l'utiliser comme base pour des

configurations plus complexes.

Pour plus d'informations, consultez le guide de démarrage de l'utilisation de DaaS.

Attribuer des lettres de lecteur aux disques de cache en écriture différée dans Configuration complète. Auparavant, vous pouviez attribuer une lettre de lecteur spécifique au disque de cache en écriture différée uniquement à l'aide d'une applet de commande PowerShell. Vous pouvez désormais accomplir la même tâche à l'aide de Configuration complète. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.

Prise en charge de la modification de différentes propriétés de machine Azure dans Configuration complète. Pour les machines Azure provisionnées par Machine Creation Services, vous pouvez désormais modifier les paramètres de propriété suivants à l'aide de Configuration complète :

- Type de stockage
- Groupe d'hôtes dédié
- Paramètres d'Azure Compute Gallery

Lorsque vous modifiez l'un de ces paramètres, Configuration complète identifie automatiquement les paramètres associés et fournit une synchronisation automatique ou des messages vous demandant de resélectionner les paramètres associés. Cette fonctionnalité garantit des modifications cohérentes entre les paramètres associés, évitant ainsi les erreurs de configuration potentielles. Pour plus d'informations, consultez la section Modifier un catalogue.

Utiliser les pools d'identités existants pour créer des identités pour les machines provisionnées par MCS. Lorsque vous créez des catalogues joints à AD ou que vous y ajoutez des machines à l'aide de Configuration complète, vous pouvez désormais utiliser un pool d'identités existant pour attribuer les identités des machines. Cette fonctionnalité vous permet d'appliquer un schéma de dénomination des comptes de machine cohérent dans plusieurs catalogues. Pour plus d'informations, consultez la section Identités des machines.

Topologie de session. La vue Topologie de session est la prochaine étape vers l'amélioration des flux de résolution des problèmes dans Monitor (Surveiller). La vue Topologie de session fournit une représentation visuelle du parcours en session pour les sessions HDX connectées. Vous pouvez accéder à la vue topologique depuis **Détails utilisateur > Performances des sessions**.

La vue Topologie de session pour une session connectée à HDX montre les composants impliqués dans le parcours de session avec leurs métadonnées, le lien entre les composants et les applications publiées sur le VDA. De plus, les indicateurs Latence ICA et RTT ICA sont affichés pour la session lorsqu'elle est connectée.

Utilisez la vue Topologie de session pour comprendre les composants par lesquels les données de session circulent et pour identifier le saut spécifique susceptible d'entraîner des problèmes de performances. Pour plus d'informations, voir Topologie de session.

Octobre 2023

Fonctionnalités nouvelles et améliorées

Affiner vos paramètres Autoscale à l'aide de l'historique d'utilisation. Un nouvel onglet des paramètres Autoscale, appelé **Insights sur Autoscale**, propose un graphique complet qui compare visuellement vos paramètres Autoscale et les données d'utilisation de la machine de la semaine précédente. Ce graphique vous permet de mieux comprendre l'efficacité des paramètres Autoscale :

- **Pas rentable**. Le gaspillage financier existe en raison d'un provisioning excessif des capacités.
- **Mauvaise expérience utilisateur**. L'expérience utilisateur est affectée négativement en raison d'un provisioning insuffisant des capacités.
- **Bon équilibre entre expérience utilisateur et coût**. La capacité provisionnée est alignée sur l'utilisation historique.

Pour plus d'informations, voir Analyser l'efficacité des paramètres Autoscale.

Prise en charge de plusieurs cartes réseau pour les machines virtuelles Azure. Avec Configuration complète, vous pouvez désormais créer des machines virtuelles Azure avec plusieurs cartes réseau. Le nombre maximal de cartes réseau d'une machine virtuelle est déterminé par le paramètre de taille de la machine, tandis que le nombre de cartes réseau réel autorisé est défini par le paramètre du profil de la machine. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.

Pour créer ou mettre à jour un catalogue avec plusieurs cartes réseau par machine virtuelle à l'aide des commandes PowerShell, voir Créer ou mettre à jour un catalogue avec plusieurs cartes réseau par machine virtuelle.

Tendances des mesures Performances des sessions Monitor introduit un nouvel onglet, **Détails utilisateur > Performances des sessions**, avec des 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. L'expérience de session contient désormais les tendances des mesures 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. Cette fonctionnalité permet de réduire le délai moyen de résolution en vous permettant de corréler plusieurs indicateurs de performance dans une seule vue. Pour plus d'informations, consultez l'article Problèmes utilisateur.

Version VDA sur la page des paramètres pour la création/modification de stratégie. Lors de la création d'une stratégie, lorsque vous configurez les 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 pour toutes les versions de VDA

- Paramètres actuels uniquement - Afficher les paramètres uniquement pour les versions actuelles de VDA
- Anciens paramètres uniquement - Afficher les paramètres uniquement pour les versions de VDA obsolètes

Pour de plus amples informations, consultez la section Créer des stratégies.

Limite de visibilité des applications uniquement prise en charge pour les comptes Active Directory. La capacité de limiter la visibilité des applications n'est disponible que pour les comptes utilisateur Active Directory, et non pour les comptes Azure Active Directory et Okta. Notez que pour faciliter cette fonctionnalité, dans le flux de travail de configuration de l'application, sur la page Sélectionner des utilisateurs ou des groupes, les options **Azure Active Directory** et **Okta** dans le champ **Sélectionnez le type d'identité** sont désactivées.

Nouvelle option d'interface utilisateur permettant de supprimer les enregistrements de machine virtuelle uniquement de la base de données du site Citrix. Lorsque la suppression du catalogue et des machines virtuelles échoue en raison d'un hyperviseur inaccessible, vous pouvez désormais choisir de supprimer uniquement les enregistrements de machines virtuelles de la base de données du site Citrix, en laissant les machines virtuelles intactes sur l'hôte. Pour plus d'informations, voir Supprimer un catalogue.

Prise en charge de la création de catalogues de machines vides pour les machines non provisionnées par MCS. La création de catalogues de machines vides s'étend désormais aux machines non provisionnées par MCS, notamment :

- Machines virtuelles ou lames provisionnées à l'aide de technologies autres que Machine Creation Services.
- Machines physiques non gérées par Citrix DaaS
- Machines Remote PC Access

Grâce à cette fonctionnalité, vous pouvez désormais créer des catalogues de machines sans avoir à y ajouter de machines lors de la création de catalogue.

Améliorations apportées à l'actualisation des images. Auparavant, lors de l'actualisation des images, toutes les images de l'arborescence d'images étaient mises à jour, qu'un nœud spécifique de l'arborescence ait été sélectionné ou non. Avec la dernière amélioration, si vous avez sélectionné un nœud, seules les images de ce nœud sont actualisées. Cette amélioration garantit un processus d'actualisation plus ciblé, ce qui améliore considérablement la vitesse d'actualisation des images. En outre, vous pouvez désormais effacer un nœud sélectionné dans l'arborescence d'images en maintenant la touche CTRL enfoncée et en cliquant sur le nœud. Pour plus d'informations, veuillez consulter la section Image principale.

Mise sous tension des machines attribuées par Autoscale pendant les heures de pointe. Lorsque des bureaux persistants sont allumés mais restent inutilisés ou si aucun utilisateur ne se connecte, les

administrateurs peuvent définir le temps d'attente pour effectuer des actions telles que l'absence d'action, la suspension ou l'arrêt.

Pour les machines attribuées, si une machine est allumée mais qu'aucune session n'y a été connectée dans le délai défini après le début de l'heure de pointe, vous pouvez ajouter une stratégie au niveau du groupe de mise à disposition pour éteindre la machine.

Pour les machines attribuées, si une machine est en état de reprise mais qu'aucune session n'y a été connectée dans le délai défini après le début de l'heure de pointe, vous pouvez ajouter une stratégie au niveau du groupe de mise à disposition pour suspendre la machine.

Cette fonctionnalité est utile si un utilisateur final est en congé ou ne s'est pas connecté, ou si une entreprise a un long week-end, vous pouvez définir le temps d'attente et les mesures de déconnexion de la machine à prendre afin de réduire le coût de consommation d'Azure. Pour plus d'informations, voir Groupes de mise à disposition aléatoires d'OS mono-session et Groupes de mise à disposition statiques d'OS mono-session.

Surveiller plusieurs instances Citrix DaaS (Technical Preview). Vous pouvez désormais utiliser Citrix Monitor pour surveiller et résoudre les problèmes rencontrés sur plusieurs instances Citrix DaaS. Citrix DaaS permet aux clients d'agréger plusieurs instances de leur service à l'aide d'un modèle hub and spoke. Grâce à cette configuration, les administrateurs peuvent effectuer des recherches de support technique sur toutes les instances DaaS configurées à partir d'une seule console Monitor. Pour plus d'informations concernant la configuration requise pour agréger les instances de service spoke sur un hub, voir Agréger plusieurs instances du service Citrix Virtual Apps and Desktops. Monitor prend en charge l'agrégation d'un maximum de quatre locataires DaaS (spokes) sous un même tenant DaaS (hub).
Pour bénéficier d'une surveillance unifiée entre tous les locataires DaaS, utilisez l'énumération bidirectionnelle des instances hub et spoke. Pour plus d'informations, consultez la section Recherche agrégée sur plusieurs instances DaaS (Technical Preview).

Prise en charge de vSAN 8.0. Vous pouvez désormais utiliser MCS pour provisionner des machines virtuelles dans l'environnement vSAN 8.0.

Préserver les paramètres de la carte d'interface réseau sur les machines virtuelles provisionnées. Auparavant, les paramètres de la carte d'interface réseau de l'image principale n'étaient pas conservés dans les machines virtuelles provisionnées. Par exemple, si vous avez configuré les paramètres DNS sur l'image principale, les machines virtuelles provisionnées ne conservaient pas les paramètres DNS configurés de l'image principale. Grâce à cette fonctionnalité, les machines virtuelles provisionnées peuvent désormais conserver les paramètres de la carte d'interface réseau de l'image principale. Les paramètres sont conservés même après la mise à jour de Windows. Le pilote de filtre est automatiquement installé si vous effectuez une nouvelle installation du VDA version 2308 ou ultérieure sur une machine déployée par Hyper-V via les installations de l'image principale MCS. Toutefois, actuellement, si vous effectuez une mise à niveau depuis une ancienne version du VDA (version inférieure à 2308) et que vous souhaitez installer le pilote de filtre, vous devez

cocher la case **Citrix HyperV Filter Driver** sur la page **Composants supplémentaires** lors de la mise à niveau du VDA. Pour plus d'informations, voir Installer des composants supplémentaires.

Cette fonctionnalité s'applique aux éléments suivants :

- Machines virtuelles Hyper-V (y compris Azure et SCVMM)
- Catalogues de machines MCS persistants et non persistants
- Catalogues de machines MCS non persistants avec MCSIO
- Image principale avec plusieurs cartes d'interface réseau

Détecter les ressources Azure orphelines. Grâce à cette fonctionnalité, vous pouvez désormais détecter les ressources orphelines dans votre déploiement Azure, ce qui permet une gestion efficace des ressources. Une fois les ressources orphelines identifiées, vous pouvez prendre d'autres mesures pour améliorer la productivité et réduire les coûts. Pour plus d'informations, consultez la section Détecter les ressources Azure orphelines dans votre déploiement.

Nouvel état de mise à jour de l'image. Lorsque vous surveillez l'état de mise à jour des images pour les catalogues dans Configuration complète, vous pouvez désormais afficher un nouvel état **Préparation de l'image**, en plus des états existants : **Entièrement mise à jour**, **Partiellement mise à jour** et **En attente de la mise à jour**. Pour plus d'informations, veuillez consulter la section Modifier l'image principale.

Commandes PowerShell pour créer des balises automatiques (Technical Preview). Grâce à cette fonctionnalité, vous pouvez désormais créer des balises automatiquement à l'aide de la commande PowerShell. Pour plus d'informations, veuillez consulter la section Balises automatiques.

Un signe de notification s'affiche pour l'utilisateur ou le groupe de mise à disposition. Lors de la création ou de la modification d'une stratégie et de la configuration des paramètres, si tous les groupes de mise à disposition sont désactivés, le système affiche un avertissement indiquant qu'aucun des éléments de ce filtre n'est activé. Si au moins un groupe de mise à disposition est activé, le système n'affiche pas le signe d'avertissement. Pour plus d'informations, veuillez consulter la section Paramètres de stratégie.

Septembre 2023

Fonctionnalités nouvelles et améliorées

Commandes PowerShell pour gérer le cache d'hôte local (LHC). Vous pouvez désormais utiliser les commandes PowerShell pour gérer le LHC sur les Citrix Cloud Connector. Pour plus d'informations, consultez la section Commandes PowerShell du cache d'hôte local.

Prise en charge de la création de catalogues de machines vides. Dans Configuration complète, vous pouvez désormais créer un catalogue de machines sans créer immédiatement de machine virtuelle. Grâce à cette fonctionnalité, vous pouvez reporter la création de machines virtuelles jusqu'

à ce que les hôtes principaux soient entièrement préparés ou que le provisioning des machines virtuelles soit terminé, afin de gagner en flexibilité dans la création de catalogues. Actuellement, cette fonctionnalité s'applique uniquement aux catalogues fournis par Machine Creation Services. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.

Mise en cache des données pour le nœud Accueil. Nous avons introduit la mise en cache des données pour le nœud **Accueil** de Citrix DaaS. Cela améliore l'expérience utilisateur en réduisant le temps de chargement des pages lorsque vous naviguez vers le nœud **Accueil**.

Améliorations de la recherche pour les applications. Nous avons réorganisé la fonctionnalité de recherche dans le nœud **Applications** afin de l'aligner sur le nouveau design introduit dans le nœud **Recherche**. Cette nouvelle fonctionnalité améliore votre expérience de recherche dans les applications et garantit une expérience de recherche cohérente dans l'ensemble de DaaS. Le mot clé **Nom de l'application** dans l'expression du filtre est renommé **Nom**, tout en conservant sa signification d'origine. Pour plus d'informations, voir Utiliser la recherche dans l'interface de gestion Configuration complète.

Gestion améliorée des étendues : affichage des objets sous forme de dossiers. Sur les pages de création et de gestion des étendues, les catalogues de machines, les groupes de mise à disposition et les groupes d'applications sont désormais affichés dans des structures de dossiers conformes à leur gestion dans DaaS. Cette vue par dossiers simplifie le processus de sélection des objets pour la création et la gestion des étendues, rendant vos choix plus intuitifs et plus directs. Pour plus d'informations, consultez Créer et gérer des étendues.

Suppression de l'option Laissez Citrix Cloud se charger de la gestion des utilisateurs. Lors de la création d'un groupe de mise à disposition dans Gérer > Configuration complète, sur la page Utilisateurs, cette option est supprimée. Pour les groupes de mise à disposition où les attributions d'utilisateurs étaient gérées via Citrix Cloud, continuez à gérer les attributions d'utilisateurs au sein de la bibliothèque Citrix Cloud.

Suppression de l'option Azure Allemagne. Suite à la fermeture de Microsoft Cloud Deutschland le 29 octobre 2021, nous avons supprimé l'option **Azure Allemagne** de la page de création de connexion hôte.

Alertes de service proactives dans Configuration complète. Les alertes se répartissent en deux niveaux : les alertes à l'échelle du site affichées dans la page d'accueil (icône représentant un drapeau) et les alertes relatives aux zones affichées dans l'onglet Dépannage de chaque zone. Actuellement, cette fonctionnalité vous envoie des avertissements et des alertes proactifs pour vous assurer que votre cache d'hôte local et vos zones sont correctement configurés afin qu'en cas de panne, le cache d'hôte local fonctionne et que vos utilisateurs ne soient pas affectés. Pour plus d'informations, consultez Alertes d'état du service et Zones.

Août 2023

Fonctionnalités nouvelles et améliorées

Configuration complète : provisioning de machines virtuelles AWS et GCP à l'aide de profils de machine. Lorsque vous provisionnez des machines virtuelles AWS ou GCP à l'aide de Machine Creation Services (MCS), vous pouvez désormais sélectionner une machine virtuelle existante comme profil de machine, afin que les machines virtuelles du catalogue héritent des paramètres de la machine virtuelle sélectionnée.

- Pour les machines virtuelles GCP, les paramètres hérités incluent l'ID du jeu de chiffrement de disque, la taille de la machine, le type de stockage et la zone.
- Pour les machines virtuelles AWS, les paramètres hérités varient en fonction de l'étape :
  - Lors de la création du catalogue : taille de la machine, type de location, groupe de sécurité et nombre de cartes réseau.
  - Lors de la modification du catalogue : taille de la machine et groupe de sécurité.

Pour de plus amples informations, consultez l'article Créer un catalogue de machines.

Nouvelle fonctionnalité de recherche dans les nœuds Catalogues de machines et Groupes de mise à disposition. Vous pouvez désormais rechercher et localiser directement des catalogues de machines et des groupes de mise à disposition dans les nœuds **Catalogues de machines** et **Groupes de mise à disposition**. La fonctionnalité de recherche de ces nœuds fournit la même interface que le nœud **Recherche**, offrant ainsi une expérience de recherche fluide dans DaaS. Pour plus d'informations, voir Utiliser la recherche dans l'interface de gestion Configuration complète.

Consultez l'état de la machine de point de terminaison dans les diagnostics de lancement de session à l'aide de l'option État de l'appareil. Dans l'onglet Surveiller, la fonction de diagnostic du lancement de session permet de déterminer le composant et le stade exacts où l'échec de session s'est produit. Cela permet d'identifier la raison exacte d'un échec de lancement de session et de prendre les mesures recommandées.

Afin que cette vérification soit complète sur tous les composants impliqués dans la séquence de lancement de session, vous pouvez désormais consulter les résultats de l'analyse de la machine de point de terminaison. Lorsque vous cliquez sur **Machine de point de terminaison** dans la liste des composants, l'état de l'analyse de l'état de l'appareil s'affiche. Le service de détermination de l'état de l'appareil analyse la machine de point de terminaison à des fins de vérification de conformité en fonction des stratégies définies par l'administrateur.

Assurez-vous que le service de détermination de l'état de l'appareil est configuré avec DaaS, comme le décrit l'article sur les états de l'appareil. Les erreurs enregistrées par l'état de l'appareil sont décrites dans les journaux des erreurs enregistrées au niveau de l'état de l'appareil.

Pour plus d'informations, consultez Étapes pour diagnostiquer l'échec du lancement de session.

Nouvelles options de configuration complète pour acheminer les requêtes d'API vers Azure et GCP via des Citrix Cloud Connector. Auparavant, les requêtes d'API adressées à Azure et à GCP ne pouvaient être acheminées que via des points de terminaison publics. Avec une nouvelle option dans **Configuration complète > Ajouter une connexion et des ressources**, vous pouvez désormais opter pour une approche plus sécurisée en les acheminant via des Citrix Cloud Connector. Pour plus d'informations, consultez Créer un principal de service et une connexion à l'aide de Configuration complète.

Améliorations de la recherche et du filtrage. Nous avons apporté les améliorations suivantes pour améliorer votre expérience de recherche :

- **Recherche simplifiée** : l'exécution d'une recherche sans filtres supprime désormais les recommandations de recherche, offrant ainsi une expérience de recherche claire et directe.
- **Mise à jour de l'opérateur ET/OU** : les options « Correspondance exacte (opérateur ET) » ou « Correspondance partielle (opérateur OU) » sont désormais disponibles dans le panneau des filtres, accessibles en un seul clic sur l'icône des filtres.
- **Configuration des filtres simplifiée** : vous pouvez désormais spécifier et appliquer plusieurs filtres en toute simplicité à l'aide du panneau des filtres.
- **Interface plus épurée :** la fonctionnalité d'« épinglage des filtres » a été supprimée, ce qui permet de réduire l'encombrement de l'interface utilisateur et de rendre votre expérience de recherche plus intuitive.
- **Ajout rapide de filtres** : Après avoir appliqué des filtres, vous pouvez désormais utiliser le signe plus pour ajouter rapidement un filtre supplémentaire.
- **Supprimer des ensembles de filtres enregistrés** : vous pouvez désormais supprimer facilement les ensembles de filtres enregistrés directement dans le menu de recherche, sans devoir accéder à **Gérer les ensembles de filtres**.

Pour plus d'informations, voir Utiliser la recherche dans l'interface de gestion Configuration complète.

Prise en charge de la mise à niveau de VDA pour les catalogues de machines créés par Déploiement rapide d'Azure. Avec Configuration complète, vous pouvez désormais activer la **mise à niveau de VDA** pour les catalogues de machines créés via Déploiement rapide d'Azure, puis effectuer une **mise à niveau de VDA** sur ceux-ci, pour des mises à niveau immédiates ou planifiées. Pour plus d'informations, consultez Mettre à niveau les VDA à l'aide de l'interface Configuration complète.

Possibilité de réinitialiser le disque d'OS d'une MV persistante dans un catalogue de machines créé par MCS dans SCVMM. Vous pouvez désormais utiliser la commande PowerShell `Reset-ProvVMDisk` pour réinitialiser le disque d'OS d'une machine virtuelle persistante dans un catalogue de machines créé par MCS. La fonctionnalité automatise le processus de réinitialisation du disque d'OS. Par exemple, elle permet de réinitialiser la machine virtuelle à son état initial dans

un catalogue de bureau de développement persistant créé à l'aide de MCS. Actuellement, cette fonctionnalité est applicable aux environnements de virtualisation Azure, Citrix Hypervisor, SCVMM et VMware. Pour plus d'informations sur la réinitialisation du disque d'OS à l'aide de la commande PowerShell, consultez Réinitialiser le disque d'OS.

Mettez à jour les propriétés des machines virtuelles individuelles. Vous pouvez désormais mettre à jour les propriétés de machines virtuelles individuelles dans un catalogue de machines MCS persistant à l'aide d'une commande PowerShell. 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. Pour plus d'informations, consultez Mettre à jour les propriétés des machines virtuelles individuelles.

Limitez le chargement et le téléchargement des disques gérés. Conformément à la stratégie d'Azure, vous ne pouvez pas charger ni télécharger plus de cinq disques ou instantanés en même temps avec le même objet d'accès au disque. Grâce à cette fonctionnalité, la limite de cinq chargements ou téléchargements simultanés n'est pas appliquée si vous :

- configurez `ProxyHypervisorTrafficThroughConnector` dans `CustomProperties` ; et
- ne configurez pas la stratégie Azure pour créer automatiquement des accès au disque pour chaque nouveau disque afin d'utiliser des points de terminaison privés.

Prise en charge de l'attribution d'une lettre de lecteur spécifique au disque de cache en écriture différée des E/S de MCS. Auparavant, le système d'exploitation Windows attribuait automatiquement une lettre de lecteur au disque de cache en écriture différée des E/S de MCS. Grâce à cette fonctionnalité, vous pouvez désormais attribuer une lettre de lecteur spécifique à un 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. Cette fonctionnalité s'applique uniquement au système d'exploitation Windows. Pour plus d'informations, consultez Attribuer une lettre de lecteur spécifique au disque de cache en écriture différée des E/S de MCS.

Prise en charge du profil de machine dans Citrix Hypervisor. Dans Citrix Hypervisor, vous pouvez désormais créer un catalogue de machines MCS à l'aide d'un profil de machine. La source de l'entrée de profil de machine est une machine virtuelle. Le profil de machine capture les propriétés matérielles à partir d'un modèle de machine virtuelle et les applique aux machines virtuelles qui viennent d'être provisionnées dans le catalogue. Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'un profil de machine.

Réessayer de créer le catalogue après un échec. Lorsque la création du catalogue échoue, vous pouvez désormais réessayer de créer le catalogue. Pour garantir la réussite de la création, consultez les informations de dépannage et résolvez les problèmes. Les informations décrivent les problèmes détectés et fournissent des recommandations pour les résoudre. Les catalogues ayant échoué sont

marqués d'une icône d'erreur. Pour en savoir plus, accédez à l'onglet **Dépannage** de chaque catalogue. Pour de plus amples informations, consultez l'article Gérer des catalogues de machines.

Autorisation de gestion des jeux de configuration. Pour un contrôle plus précis de la gestion des jeux de configuration WEM, nous avons introduit une nouvelle autorisation appelée **Gérer les jeux de configuration** dans le jeu d'autorisations **des catalogues de machines**. Cette autorisation accorde un accès exclusif aux utilisateurs qui peuvent effectuer des tâches telles que lier ou dissocier un jeu de configuration et passer à un autre jeu de configuration pour les catalogues. Pour plus d'informations, consultez Gérer un jeu de configuration pour un catalogue.

Nouvelle option dans Configuration complète permettant le nettoyage des appareils joints à Azure AD obsolètes. Nous avons introduit une option dans la configuration complète afin de simplifier le nettoyage des appareils joints à Azure AD obsolètes dans Citrix DaaS. Auparavant, vous deviez exécuter un script PowerShell personnalisé pour effectuer cette tâche. L'activation de cette option accorde aux connexions hôtes l'autorisation de nettoyer automatiquement les appareils joints à Azure AD obsolètes. Pour plus d'informations, consultez Connexions hôtes Azure.

Surveiller l'état de mise à jour des images pour les catalogues à l'aide de la configuration complète. Vous pouvez désormais surveiller l'état des mises à jour des images pour les catalogues de machines non persistants à l'aide d'une nouvelle colonne, **Mise à jour des images**. Cette colonne indique si les images d'un catalogue sont **entièrement mises à jour**, **partiellement mises à jour** ou **en attente de mise à jour**.

Pour afficher la colonne dans le tableau **Catalogues de machines**, procédez comme suit :

1. Dans le nœud **Catalogues de machines**, sélectionnez l'icône **Colonnes à afficher** dans la barre d'actions.
2. Sélectionnez **Catalogue de machines > État de l'image**.
3. Cliquez sur **Enregistrer**.

L'affichage de la colonne **Mise à jour de l'image** peut dégrader les performances de la console. Nous vous recommandons de ne l'afficher que lorsque cela est nécessaire.

Environnement sécurisé pour le trafic géré par GCP. Grâce à cette fonctionnalité, vous pouvez désormais autoriser uniquement 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 cela, ajoutez `ProxyHypervisorTrafficThroughConnector` dans `CustomProperties` en cas de déploiement de Citrix Cloud. Si vous utilisez un pool de travailleurs privés, ajoutez `UsePrivateWorkerPool` dans `CustomProperties`. Pour plus d'informations, consultez la section Créer un environnement sécurisé pour le trafic géré par GCP.

Juillet 2023

Fonctionnalités nouvelles et améliorées

Aide à l'obtention d'une liste de ressources orphelines sur Azure. Dans les environnements Azure, vous pouvez désormais obtenir une liste des ressources orphelines créées par MCS mais qui ne sont plus utilisées par MCS. Cette fonctionnalité permet d'éviter des coûts supplémentaires. Pour plus d'informations, reportez-vous à la section Récupérer une liste de ressources orphelines.

Prise en charge de la création de machines multi-sessions persistantes à l'aide de Configuration complète. Lorsque vous créez un catalogue de machines multisessions, vous pouvez désormais spécifier si vous souhaitez les rendre persistantes. Pour les machines multi-sessions persistantes, gardez à l'esprit que les modifications apportées par les utilisateurs aux bureaux sont enregistrées et accessibles à tous les utilisateurs autorisés. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.

Nouvelle fonctionnalité dans Configuration complète pour filtrer l'inventaire AWS AMI. Lorsque vous sélectionnez des modèles de machines lors de la création d'un catalogue AWS, vous pouvez désormais filtrer l'inventaire AWS AMI pour un modèle cible à l'aide des critères de recherche suivants :

- Nom de l'image
- Identifiant de l'image
- Balises d'image

La liste des modèles de machines se charge dynamiquement lorsque vous faites défiler la liste. 25 éléments sont initialement chargés et d'autres sont chargés au fur et à mesure que vous faites défiler la liste.

Prise en charge de la suppression d'appareils Azure AD. Grâce à cette fonctionnalité, les appareils Azure AD obsolètes peuvent être systématiquement supprimés en attribuant le rôle d'administrateur de machine cloud au principal du service et en modifiant la propriété personnalisée de la connexion d'hébergement. Si vous ne supprimez pas les machines Azure AD obsolètes, la machine virtuelle non persistante correspondante reste dans l'état d'initialisation jusqu'à ce que vous la supprimiez manuellement du portail Azure AD. Pour plus d'informations, consultez la section Créer des catalogues joints à Azure Active Directory.

Prise en charge du profil de machine dans l'environnement AWS. 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 modifi-

cation du catalogue, le profil des machines provisionnées peut être modifié en fournissant une machine virtuelle ou un modèle de lancement différent. Pour plus d'informations, consultez Créer un catalogue à l'aide d'un profil de machine.

La limite d'exportation des résultats de recherche a été étendue de 10 000 à 30 000. Nous avons étendu la limite d'exportation des résultats de recherche. Auparavant limité à 10 000 éléments, vous pouvez désormais exporter jusqu'à 30 000 éléments vers un fichier CSV. Pour plus d'informations, voir Exporter les résultats de la recherche vers un fichier CSV.

Option d'actualisation de l'image. Lorsque vous sélectionnez des images principales pour les catalogues de machines, vous pouvez désormais obtenir rapidement la liste d'images principales les plus récentes à l'aide de l'option **Actualiser** en haut à droite. Notez que l'option **Actualiser** n'est pas disponible pour les catalogues AWS. En outre, une option d'**actualisation** est disponible pour les profils de machines et les groupes d'hôtes dans les catalogues Azure.

Juin 2023

Fonctionnalités nouvelles et améliorées

Prise en charge de l'obtention de propriétés personnalisées à partir de l'entrée de profil de machine dans GCP. Auparavant, dans les environnements GCP, lors de la création d'un catalogue de machines MCS à l'aide d'une entrée de profil de machine, vous deviez spécifier explicitement les propriétés personnalisées. L'action nécessitait un effort supplémentaire. Grâce à cette fonctionnalité, vous pouvez désormais déterminer les propriétés personnalisées suivantes sans les définir explicitement :

- `ServiceOffering`
- `CryptoKeyId`
- `CatalogZones`
- `Storage`

Lorsque vous exécutez les commandes `New-ProvScheme` et `Set-ProvScheme` sans spécifier explicitement les propriétés personnalisées, les valeurs des propriétés sont déterminées en fonction de l'entrée de profil de la machine.

Par exemple, `New-ProvScheme -MachineProfile` écrit le type de machine du profil de machine dans la propriété `ServiceOffering` du schéma de provisioning, sauf si vous spécifiez `ServiceOffering` dans la commande `New-ProvScheme`. Si vous exécutez `Set-ProvVMScheme` deux fois, la commande la plus récente prend effet.

Suppression des balises dans les environnements AWS. Auparavant, les commandes PowerShell `Remove-ProvVM` et `Remove-ProvScheme` avec le paramètre `ForgetVM` supprimaient les machines virtuelles et les catalogues de machines de la base de données Citrix. Toutefois, les comman-

des ne supprimaient pas les balises. Vous deviez gérer individuellement les machines virtuelles et les catalogues de machines qui n'étaient pas complètement supprimés de toutes les ressources. Grâce à cette fonctionnalité, vous pouvez utiliser :

- `Remove-ProvVM` avec le paramètre `ForgetVM` pour supprimer les machines virtuelles et les balises d'une seule machine virtuelle ou d'une liste de machines virtuelles d'un catalogue de machines virtuelles.
- `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 implémentation permet de :

- Identifier les ressources divulguées
- Éliminer les coûts supplémentaires liés à la gestion des ressources inutiles

Cette fonctionnalité s'applique uniquement aux machines virtuelles persistantes. Pour plus d'informations, veuillez consulter la section Supprimer les balises.

Possibilité d'obtenir les données historiques des erreurs et des avertissements associés à un catalogue de machines MCS. Auparavant, vous ne receviez que les derniers avertissements et erreurs associés à un catalogue de machines. Grâce à cette fonctionnalité, vous pouvez désormais obtenir une liste historique des avertissements et erreurs d'un catalogue de machines MCS. Cette liste vous aide à comprendre les problèmes liés à votre catalogue de machines MCS et à les résoudre.

Pour plus d'informations, voir Récupérer les erreurs et les avertissements associés à un catalogue.

Capacité accrue et performances améliorées pour Citrix dans Google Cloud. Citrix peut désormais prendre en charge des catalogues contenant jusqu'à 3 000 VDA dans un seul projet Google Cloud. Cette mise à jour améliore les performances des opérations de provisioning et de gestion de l'alimentation.

Possibilité de réinitialiser le disque d'OS d'une VM persistante dans un catalogue de machines créé par MCS dans un environnement Google Cloud et AWS. Vous pouvez désormais utiliser la commande PowerShell `Reset-ProvVMDisk` pour réinitialiser le disque d'OS d'une machine virtuelle persistante dans un catalogue de machines créé par MCS. La fonctionnalité automatise le processus de réinitialisation du disque d'OS. Par exemple, elle permet de réinitialiser la machine virtuelle à son état initial dans un catalogue de bureau de développement persistant créé à l'aide de MCS. Actuellement, cette fonctionnalité est applicable aux environnements de virtualisation AWS, Azure, Citrix Hypervisor, Google Cloud et VMware. Pour plus d'informations sur la réinitialisation du disque d'OS à l'aide de la commande PowerShell, consultez Réinitialiser le disque d'OS.

Prise en charge de la modification des propriétés personnalisées liées au disque d'un catalogue existant et de machines virtuelles existantes dans GCP. Auparavant, dans les environnements GCP, vous pouviez ajouter les propriétés personnalisées uniquement lorsque vous créiez le catalogue de

machines MCS. Grâce à cette fonctionnalité, vous pouvez désormais modifier les propriétés personnalisées suivantes liées au disque d'un catalogue existant et des machines virtuelles existantes du catalogue.

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

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 plus d'informations, consultez Modifier les propriétés personnalisées liées au disque d'un catalogue existant.

La prise en charge du délai d'expiration dynamique des sessions a été étendue au VDA version 2203 LTSR CU3 ou ultérieure. Pour les groupes de mise à disposition d'OS mono-session, cette fonctionnalité s'applique désormais aux VDA de version 2206 CR ou ultérieure, ou 2203 LTSR CU3 ou ultérieure. Pour plus d'informations, consultez la section Délai d'expiration de session dynamique.

Amélioration apportée à l'expérience de création de connexion hôte dans Configuration complète Une fois que vous avez sélectionné un emplacement de ressources, la liste déroulante **Type de connexion** affiche désormais tous les hyperviseurs et services cloud pris en charge par Citrix, et leur disponibilité dépend :

- Pour un emplacement de ressources dépourvu de connecteurs cloud accessibles, seuls les hyperviseurs et les services cloud prenant en charge les déploiements sans connecteur sont disponibles.
- Pour un emplacement de ressources doté de connecteurs cloud accessibles, seuls les hyperviseurs et les services cloud dont les plug-ins sont correctement installés sur ces connecteurs sont disponibles.

Pour plus d'informations, consultez la section Créer et gérer des connexions.

Sélection de composants supplémentaires lors de la mise à niveau du VDA. Vous pouvez désormais sélectionner les composants supplémentaires à mettre à niveau ou à installer lors de la mise à niveau d'un VDA. Pour plus d'informations, voir Configurer la mise à niveau automatique pour les VDA.

> **Important :**
>
> Pour utiliser la fonctionnalité des composants supplémentaires, assurez-vous que votre agent de mise à niveau VDA est à la version 7.34 ou ultérieure, incluse dans le programme d'installation du VDA version 2206 ou ultérieure.

La configuration complète préconfigure désormais certains paramètres pour les machines Azure en fonction des profils de machine. Lorsque vous provisionnez des machines virtuelles Azure, la configuration complète préconfigure désormais les paramètres suivants en fonction du profil de machine sélectionné :

- Groupe d'hôtes
- Jeu de chiffrement de disque
- Zone de disponibilité
- Type de licence

Prise en charge de la mise en veille prolongée des instances AWS. Vous pouvez désormais lancer des instances AWS, les configurer comme vous le souhaitez et les mettre en veille prolongée. 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. Pour plus d'informations sur la création de machines virtuelles compatibles avec la mise en veille prolongée, consultez la section Mise en veille prolongée d'instance.

Prise en charge de l'optimisation de la limitation d'AWS. Vous pouvez désormais allumer et éteindre un grand nombre de machines dans un catalogue AWS sans rencontrer de problèmes de limitation. Des problèmes de limitation se produisent lorsque le nombre de demandes envoyées à AWS dépasse le nombre de demandes que le serveur peut gérer. Cette fonctionnalité augmente l'efficacité en réduisant le nombre d'appels AWS nécessaires pour allumer et éteindre des machines en masse. Elle réduit également de manière significative le temps nécessaire pour allumer et éteindre les machines dans les catalogues permanents.

Environnement sécurisé pour le trafic géré par Azure. Auparavant, vous utilisiez l'Internet public pour permettre à vos points de terminaison Azure d'interagir avec les ressources de votre environnement. En conséquence, des problèmes de sécurité ont été soulevés en raison de l'accès à l'Internet public. Grâce à cette fonctionnalité, MCS permet d'acheminer le trafic réseau via des Citrix Cloud Connector dans votre environnement. Cela garantit la sécurité de l'environnement car tout le trafic géré par Azure provient désormais de votre propre environnement. Pour ce faire, ajoutez `ProxyHypervisorTrafficThroughConnector` dans `CustomProperties`. Pour plus d'informations, consultez la section Créer un environnement sécurisé pour le trafic géré par Azure.

Après avoir défini les propriétés personnalisées, vous pouvez configurer des stratégies Azure pour avoir un accès privé aux disques gérés par Azure.

Prise en charge du provisioning des machines virtuelles du catalogue avec Azure Monitor Agent. L'agent Azure Monitor (AMA) collecte les données de surveillance et les transmet à Azure Monitor. Cette fonctionnalité vous permet de provisionner des machines virtuelles du catalogue de machines MCS (persistantes et non persistantes) avec l'agent AMA installé en tant qu'extension. Cette implémentation permet de surveiller en identifiant de manière unique les machines virtuelles dans les données de surveillance. Pour plus d'informations sur l'agent AMA, consultez la section Vue d'ensemble

de l'agent Azure Monitor.

Actuellement, MCS prend uniquement en charge le workflow de profil de machine pour cette fonctionnalité. Pour plus d'informations sur le provisioning des machines virtuelles du catalogue de machines avec l'option AMA activée, voir Provisionner des machines virtuelles de catalogue avec l'agent Azure Monitor installé.

Activer un programme de redémarrage pour un catalogue MCS. Auparavant, vous pouviez planifier les mises à jour des images en attendant le prochain redémarrage ou en déclenchant un redémarrage immédiat de toutes les machines virtuelles. Grâce à cette fonctionnalité, vous pouvez désormais créer un programme de redémarrage unique pour qu'un catalogue soit déclenché à la date et à l'heure souhaitées afin de faciliter la mise à jour des images MCS. Pour créer un programme de redémarrage, utilisez la commande `BrokerCatalogRebootSchedule`. Pour plus d'informations, veuillez consulter la section Modifier l'image principale.

Gérez les clés secrètes client expirées dans Déploiement rapide d'Azure. Dans Déploiement rapide d'Azure, vous pouvez désormais rester informé grâce à des alertes lors de l'expiration des clés secrètes client et les mettre à jour facilement pour garantir un accès continu aux ressources Azure. Pour plus d'informations, consultez la section Mettre à jour les clés secrètes client expirées.

Mai 2023

Fonctionnalités nouvelles et améliorées

Améliorations apportées à la recherche. Cette fonctionnalité améliore les éléments visuels et les interactions des filtres, vous offrant ainsi une meilleure expérience de recherche. Pour plus d'informations, voir Utiliser la recherche dans l'interface de gestion Configuration complète.

Nouvelle stratégie d'exclusion des utilisateurs avec laquelle vous pouvez définir des chemins de répertoire qui ne sont pas redirigés vers la couche utilisateur. Les exclusions d'utilisateurs s'appliquent à la couche de personnalisation utilisateur (UPL), mais pas à l'hôte de la session. Logoff.txt contient désormais toutes les exclusions d'utilisateurs actives. Pour plus d'informations, voir Couche de personnalisation de l'utilisateur.

Prise en charge de la mise à jour de la version matérielle des nouvelles machines virtuelles ajoutées à un catalogue de machines MCS. Dans les environnements VMware, vous pouvez désormais mettre à jour la version matérielle des machines virtuelles récemment ajoutées dans un catalogue de machines MCS existant à l'aide d'une source de profil de machine. Il n'est pas nécessaire de créer un catalogue de machines pour mettre à jour la version matérielle des machines virtuelles ajoutées à un catalogue. Vous devez appliquer le workflow de profil de machine pour utiliser cette fonctionnalité.

Prise en charge du filtrage des instances de machines virtuelles AWS. Auparavant, lorsque vous utilisiez une instance de machine virtuelle AWS comme entrée de profil de machine pour créer un

catalogue de machines MCS, le catalogue ne se créait pas ou ne fonctionnait pas correctement en raison d'une entrée de profil de machine non valide. Grâce à cette fonctionnalité, vous pouvez désormais répertorier les instances de machines virtuelles AWS qui peuvent être utilisées comme des machines virtuelles de profil de machine valides. Pour ce faire, utilisez la commande `Get-HypInventoryItem`. Pour plus d'informations, consultez la section Filtrage des instances de machines virtuelles.

Prise en charge de la conversion d'un catalogue de machines non basé sur un profil de machine vers un catalogue de machines basé sur un profil de machine dans l'environnement Azure. Dans l'environnement Azure, vous pouvez désormais utiliser une machine virtuelle ou une spécification de modèle 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 machines virtuelles existantes et 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. Pour plus d'informations, voir Convertir un catalogue de machines non basé sur un profil de machine vers un catalogue de machines basé sur un profil de machine.

Prise en charge du chiffrement double sur disque géré dans l'environnement Azure. Dans l'environnement Azure, vous pouvez désormais créer un catalogue de machines MCS à l'aide du chiffrement double. 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.

Prise en charge du profil de machine dans VMware. Dans les environnements VMware, vous pouvez désormais 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. Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'un profil de machine.

Possibilité de réinitialiser le disque du système d'exploitation d'une machine virtuelle persistante dans un catalogue de machines créé par MCS dans Azure et Citrix Hypervisor. Vous pouvez désormais utiliser la commande PowerShell `Reset-ProvVMDisk` pour réinitialiser le disque d'OS d'une machine virtuelle persistante dans un catalogue de machines créé par MCS. La fonctionnalité automatise le processus de réinitialisation du disque d'OS. Par exemple, elle permet de réinitialiser la machine virtuelle à son état initial dans un catalogue de bureau de développement persistant créé à l'aide de MCS. Actuellement, cette fonctionnalité est applicable aux environnements de virtualisation Azure, Citrix Hypervisor et VMware. Pour plus d'informations sur la réinitialisation du disque d'OS à

l'aide de la commande PowerShell, consultez Réinitialiser le disque d'OS.

Amélioration apportée à l'expérience de création de connexion hôte. Vous pouvez désormais obtenir les informations suivantes lors de la création d'une connexion hôte :

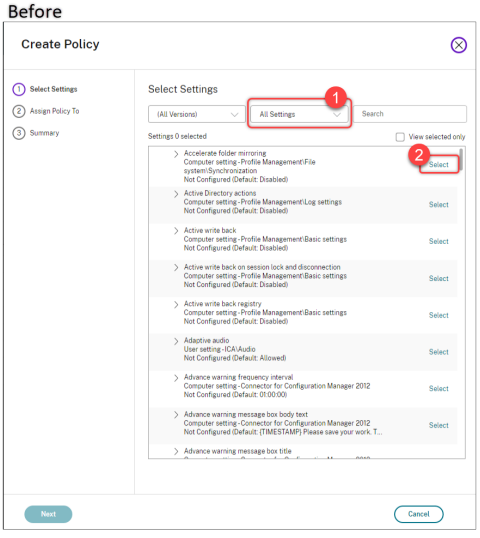
- Liste de tous les plug-ins d'hyperviseur pris en charge par Citrix, y compris les plug-ins tiers
- Disponibilité du plug-in d'hyperviseur. Si l'état de disponibilité est défini sur « false », cela peut être dû au fait que Cloud Connector n'est pas installé.

Cette fonctionnalité vous aide à configurer correctement un emplacement de ressources et à créer ainsi une connexion hôte. Pour plus d'informations, consultez Étape 1. Connexion.

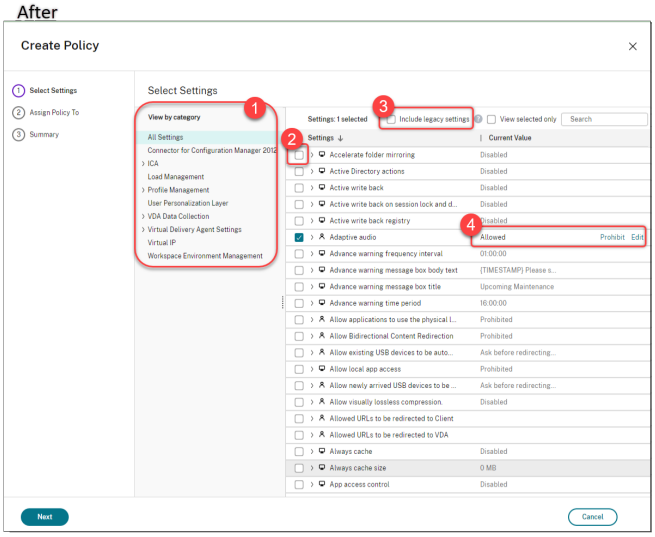
Améliorations apportées à l'expérience utilisateur dans le nœud Stratégies. Pour améliorer l'expérience utilisateur et rendre la gestion des stratégies plus efficace, nous avons apporté les améliorations suivantes dans le nœud **Configuration complète > Stratégies** :

- Nouvelle apparence de l'interface utilisateur pour les actions **Créer une stratégie** et **Créer un modèle** :
  - Affichage des dossiers développés dans les paramètres de stratégie. Sur la page **Sélectionner les paramètres**, tous les paramètres sont affichés par catégorie dans une arborescence développée, ce qui facilite la recherche d'un paramètre.
  - Pour sélectionner un paramètre, il vous suffit de cocher une case au lieu d'utiliser le bouton **Sélectionner**.
  - Les anciens paramètres ont été masqués par défaut afin que seuls les paramètres les plus pertinents soient affichés. Si des anciens paramètres sont nécessaires, sélectionnez **Inclure les anciens paramètres**.
  - Un bouton d'action a été ajouté à côté d'un paramètre booléen, vous permettant de modifier sa valeur directement dans la liste des paramètres.

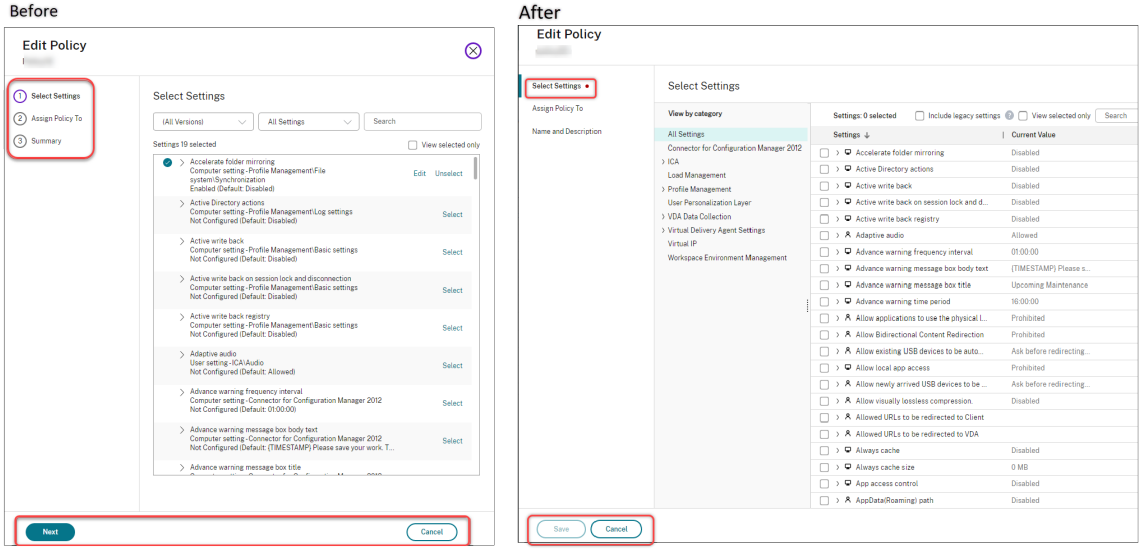
Before



After



- Nouvelle apparence de l'interface utilisateur pour l'action **Modifier la stratégie** :
  - Le menu de navigation a été mis à jour et est désormais affiché dans une liste non ordonnée. Chaque élément de la liste inclut désormais un bouton **Enregistrer** sur sa page. Grâce à cette nouvelle apparence, vous pouvez enregistrer les modifications apportées à un élément sans avoir à parcourir tous les éléments du menu de navigation. Ces améliorations rendent la gestion des stratégies plus efficace et simple.
  - Des points rouges apparaissent à côté des éléments de navigation pour indiquer des erreurs de réglage.



- Faites glisser le pointeur pour redéfinir les priorités des stratégies. Dans la liste des priorités, vous pouvez désormais modifier la priorité d'une stratégie en la faisant glisser vers la position souhaitée.

Nouvelle option pour désactiver la fermeture de session forcée des utilisateurs pour AutoScale. Une nouvelle option, **Ne pas notifier ni forcer fermeture de la session utilisateur**, est désormais disponible sur la page **Gérer Autoscale > Notifications de déconnexion utilisateur**. Si cette option est sélectionnée, Autoscale ne force pas les utilisateurs à se déconnecter des machines en état de drainage et ne les invite pas non plus à se déconnecter et se connecter à une autre machine. Pour plus d'informations, consultez la section Notifications de fermeture de session utilisateur.

Possibilité de redémarrer les PC Windows 365 Cloud. Vous pouvez désormais utiliser Citrix DaaS pour redémarrer les PC Windows 365 Cloud.

Détails supplémentaires sur la session. Lorsque vous affichez une session dans **Configuration complète > Recherche > Sessions**, l'affichage de la session (dans le volet inférieur) inclut désormais des détails supplémentaires sur la session pour vous aider à résoudre et à identifier les problèmes du client :

- **Heure de reconnexion.** Heure à laquelle une session s'est reconnectée après avoir été déconnectée.
- **Plate-forme du client.** Plate-forme utilisée pour lancer la session.
- **Version du client.** Version de la plate-forme cliente utilisée pour lancer la session.
- **IP de l'hôte distant.** Adresse IP de l'hôte distant sur lequel Citrix Workspace est hébergé.

Prise en charge du changement de nom des groupes de sécurité Azure AD pour les machines virtuelles. Pour les machines virtuelles ajoutées à un groupe de sécurité Azure AD via Citrix DaaS, vous pouvez désormais renommer le groupe de sécurité en utilisant **Configuration complète > Modifier le catalogue de machines**. Le changement de nom se produit une fois que vous avez enregistré la modification.

Sélection du domaine par défaut pour les comptes de machines. Lorsque vous créez un catalogue, le domaine dans lequel réside la ressource (connexion) est sélectionné par défaut pour les comptes de machines.

Possibilité d'afficher les groupes de sécurité attribués à Azure AD auxquels les machines virtuelles peuvent se joindre. Dans Configuration complète, lorsque vous créez des machines virtuelles jointes à Azure Active Directory, une option, **Rejoindre un groupe de sécurité attribué en tant que membre**, est désormais disponible. Elle vous permet d'ajouter le groupe de sécurité Azure AD dans lequel résident les machines virtuelles à un groupe de sécurité attribué. Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager.

Prise en charge du changement de réseau pour les connexions. Dans Configuration complète, vous pouvez désormais modifier les réseaux pour une connexion. Vous ne pouvez pas dissocier les réseaux d'une connexion s'ils sont utilisés. Pour plus d'informations, voir Modifier le réseau.

Possibilité de supprimer les balises dans les environnements Azure. Auparavant, les commandes PowerShell `Remove-ProvVM` et `Remove-ProvScheme` avec le paramètre `ForgetVM` supprimaient les machines virtuelles et les catalogues de machines de la base de données Citrix. Toutefois, les commandes ne supprimaient pas les balises des ressources. Vous deviez gérer individuellement les machines virtuelles et les catalogues de machines qui n'étaient pas complètement supprimés de toutes les ressources. Grâce à cette fonctionnalité, vous pouvez utiliser :

- `Remove-ProvVM` avec le paramètre `ForgetVM` pour supprimer les machines virtuelles et les balises créées sur les ressources d'une seule machine virtuelle ou d'une liste de machines virtuelles d'un catalogue de machines virtuelles.
- `Remove-ProvScheme` avec le paramètre `ForgetVM` pour supprimer un catalogue de machines de la base de données Citrix et les balises créées sur les ressources d'un catalogue de machines complet.

Cette implémentation permet d'identifier les ressources orphelines créées par MCS mais qui ne sont plus utilisées par MCS.

Cette fonctionnalité s'applique uniquement aux machines virtuelles persistantes. Pour plus d'informations, veuillez consulter la section Supprimer les balises.

Alerte Machines défectueuses. La fonctionnalité d'alertes et de notifications proactives de Director a été améliorée pour inclure une nouvelle alerte, Machines défectueuses (en %), basée sur le pourcentage de machines défectueuses dans un groupe de mise à disposition. La nouvelle 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. Pour plus d'informations, consultez la section Machines défectueuses de l'article Alertes.

Avril 2023

Fonctionnalités nouvelles et améliorées

Publication sur des plates-formes cloud spécifiques à l'aide de Citrix Provisioning dans le service de portabilité des images. Des workflow spécifiques permettant d'utiliser le service de portabilité des images pour publier dans AWS, Azure et Google Cloud sont désormais disponibles. En outre, les autorisations requises pour Azure et la mise en réseau ont été mises à jour. Consultez Migrer des charges de travail vers un cloud public pour plus de détails.

Possibilité d'identifier les raisons pour lesquelles une machine est en mode de maintenance. Auparavant, PowerShell était votre seul choix pour identifier les raisons pour lesquelles une machine était en mode de maintenance. Vous pouvez désormais le faire dans Configuration complète :

1. Utilisez la fonctionnalité Recherche pour localiser la machine.
2. Vérifiez la **raison de la maintenance** dans l'onglet **Détails** du volet inférieur. Vous pouvez également placer le pointeur de la souris sur la colonne **Mode de maintenance**. Les informations suivantes peuvent apparaître :

- Par administrateur : placé en mode de maintenance par l'administrateur
- Nombre maximal d'échecs d'enregistrements : placé en mode de maintenance car la machine a dépassé le nombre maximal de tentatives d'enregistrement autorisées.

De plus, un filtre, **Raison de la maintenance**, est désormais disponible. Vous pouvez l'utiliser pour identifier les machines cibles.

Cette fonctionnalité peut aider les administrateurs à résoudre les problèmes liés aux machines en mode maintenance.

Utilisation de variables pour informer les utilisateurs du temps restant avant qu'ils ne soient déconnectés. Lorsque vous forcez la fermeture de session d'un utilisateur, vous pouvez désormais utiliser `%s%` ou `%m%` en tant que variables pour indiquer le délai spécifié dans le message de notification. Pour exprimer le délai en secondes, utilisez `%s%`. Pour exprimer le délai en minutes, utilisez `%m%`. Pour plus d'informations, consultez la section Notifications de fermeture de session utilisateur.

Personnalisation du 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. Auparavant, dans ces scénarios, la machine virtuelle restait éteinte et un message d'échec vous était envoyé. Grâce à cette fonctionnalité, vous pouvez 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. Pour plus d'informations, voir Personnaliser le comportement de mise sous tension en cas d'échec du changement de type de stockage.

Activation de MAK. Vous pouvez désormais provisionner des catalogues de machines persistants et non persistants avec des machines virtuelles activées via la clé d'activation multiple (MAK). Grâce à cette fonctionnalité, MCS peut désormais également communiquer avec les machines virtuelles provisionnées. Cette implémentation permet d'activer le système Windows sans perdre d'activations. Pour plus d'informations, consultez la section Activation des licences en volume.

Chiffrement de disque Azure sur l'hôte. Grâce à cette fonctionnalité, vous pouvez désormais créer un catalogue de machines MCS avec fonction de chiffrement 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. Pour plus d'informations, consultez Chiffrement de disque Azure sur l'hôte.

Dans ce type de chiffrement, 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, consultez Chiffrement à l'hôte : chiffrement de bout en bout pour vos données de machine virtuelle.

Modèle d'instance GCP comme entrée pour le profil de la machine. Grâce à cette fonctionnalité, vous pouvez désormais 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. Pour procéder, utilisez les commandes PowerShell. Pour plus d'informations sur l'utilisation des commandes PowerShell afin de créer et mettre à jour des catalogues de machines en sélectionnant un modèle d'instance GCP, voir Créer un catalogue de machines avec un profil de machine en tant que modèle d'instance.

Modification du nom du groupe de sécurité dynamique Azure AD. Vous pouvez modifier ou supprimer le nom d'un groupe de sécurité dynamique Azure AD depuis le portail Azure. Suite à cette action, le nom du groupe de sécurité dynamique Azure AD peut être désynchronisé avec le groupe de sécurité dynamique associé à un catalogue de machines. Grâce à cette fonctionnalité, vous pouvez désormais modifier le nom du groupe de sécurité dynamique Azure AD associé à un catalogue de machines.

Cette modification vous permet de vous assurer que les informations du groupe de sécurité dynamique Azure AD stockées dans l'objet du pool d'identités Azure AD correspondent aux informations stockées dans le portail Azure. Pour plus d'informations, consultez la section Modifier le nom du groupe de sécurité dynamique Azure AD.

Autorisations supplémentaires requises dans GCP. Les autorisations requises pour effectuer les opérations suivantes sont désormais ajoutées :

- Créer une connexion hôte
- Gérer l'alimentation des machines virtuelles
- Provisionner des catalogues

Pour plus d'informations, consultez À propos des autorisations GCP.

Gestion des informations d'identification. Pour une sécurité renforcée, par défaut, les informations d'identification ne sont pas transférées vers le cloud pour les utilisateurs qui ne sont pas dans le même domaine que leurs VDA. Les tentatives de connexion échouent lorsque toutes les conditions suivantes sont remplies :

- L'utilisateur se trouve dans un domaine différent du VDA
- Il n'existe aucune confiance entre les domaines
- StoreFront est installé dans le même domaine que le VDA

Auparavant, dans ces conditions, l'utilisateur ne pouvait pas être authentifié auprès de StoreFront. Le Cloud Connector transmettait donc les informations d'identification de l'utilisateur au cloud pour acheminer la demande d'authentification vers la destination appropriée pour cet utilisateur. Ce comportement peut toujours être configuré si nécessaire. Pour plus d'informations, consultez le paramètre `CredentialForwardingToCloudAllowed` de Set-Brokersite dans le DaaS PowerShell SDK.

Mars 2023

Fonctionnalités nouvelles et améliorées

Configuration du rôle et de l'étendue des administrateurs. Citrix Cloud offre désormais un plus haut degré de flexibilité et de personnalisation lors de la configuration de l'accès pour un administrateur. Auparavant, vous ne pouviez sélectionner que des paires prédéfinies de rôles et d'étendues. Grâce à cette amélioration, vous pouvez sélectionner un rôle, puis l'associer à l'étendue de votre choix.

Pour plus d'informations, consultez Configurer un accès personnalisé pour un administrateur.

Possibilité de créer un groupe de sécurité dynamique dans un groupe de sécurité attribué existant. Auparavant, vous pouviez créer des groupes de sécurité dynamiques Azure AD pour un catalogue de machines. Grâce à cette fonctionnalité, vous pouvez également ajouter un groupe de sécurité dynamique Azure AD sous un groupe de sécurité attribué à Azure AD existant. Vous pouvez effectuer les opérations suivantes :

- Obtenir des informations sur les groupes de sécurité.

- Obtenir tous les groupes de sécurité attribués à Azure AD qui sont synchronisés à partir du serveur AD local ou aux groupes de sécurité attribués auxquels des rôles Azure AD peuvent être attribués.
- Obtenir tous les groupes de sécurité dynamiques Azure AD.
- Ajouter un groupe de sécurité dynamique Azure AD en tant que membre de groupe attribué à Azure AD.
- Supprimer l'appartenance entre le groupe de sécurité dynamique Azure AD et le groupe de sécurité attribué à Azure AD lorsque le groupe de sécurité dynamique Azure AD est supprimé en même temps que le catalogue de machines.

Pour plus d'informations, voir Créer un groupe de sécurité dynamique Azure AD sous un groupe de sécurité attribué à Azure AD existant.

Prise en charge du groupe de sécurité dynamique Azure AD pour les machines virtuelles jointes à Azure AD. Citrix prend désormais en charge les groupes de sécurité dynamiques pour un catalogue lors de la création d'un catalogue de machines MCS. Les règles de groupe de sécurité dynamique placent les machines virtuelles du catalogue dans un groupe de sécurité dynamique en fonction du schéma de dénomination du catalogue de machines. Cette fonctionnalité est utile lorsque vous souhaitez gérer les machines virtuelles avec Azure Active Directory (Azure AD). Elle est également utile lorsque vous souhaitez appliquer des stratégies d'accès conditionnel ou distribuer des applications depuis Intune en filtrant les machines virtuelles avec le groupe de sécurité dynamique Azure AD. Lorsque vous supprimez un catalogue, le groupe de sécurité dynamique est également supprimé. Pour plus d'informations, consultez la section Groupe de sécurité dynamique Azure Active Directory.

Pour plus d'informations sur les exigences de licence pour l'utilisation de groupes de sécurité dynamiques, consultez le document Microsoft Créer ou mettre à jour un groupe dynamique dans Azure Active Directory.

Ajout de machines virtuelles aux groupes de sécurité Azure AD via Configuration complète. Une nouvelle option, **Groupe de sécurité Azure AD**, est désormais disponible lorsque vous créez des machines virtuelles jointes à Azure AD. Cette option vous permet d'ajouter les machines virtuelles à un groupe de sécurité Azure AD en fonction de leur schéma de dénomination. Pour plus d'informations, voir Créer un catalogue Microsoft Azure.

Possibilité de modifier le type de stockage des machines virtuelles existantes vers un niveau inférieur lors de l'arrêt dans les environnements Azure. Dans les environnements Azure, vous pouvez désormais 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 plus d'informations, voir Définir le type de stockage des machines virtuelles existantes sur un niveau inférieur lors de l'arrêt.

Identifiants de sécurité autorisés lors de la création de machines virtuelles. Auparavant, lors

de la création de nouvelles machines virtuelles avec la configuration spécifiée par un schéma de provisioning, vous ne pouviez pas ajouter d'identifiant de sécurité (`ADAccountSid`) à la commande `NewProvVM`. Grâce à cette fonctionnalité, vous pouvez désormais ajouter le paramètre `ADAccountSid` pour identifier de manière unique les machines lors de la création de nouvelles machines virtuelles. Pour plus d'informations, consultez la section Ajouter des SID lors de la création de machines virtuelles.

Possibilité d'obtenir des avertissements associés aux catalogues MCS. Auparavant, vous ne receviez aucune information indiquant des problèmes avec votre catalogue de machines. Grâce à cette fonctionnalité, vous pouvez désormais obtenir les avertissements pour comprendre les problèmes liés à vos catalogues MCS et les résoudre.

Les avertissements, contrairement aux erreurs, n'entraînent pas l'échec d'une tâche de provisioning lancée.

Pour obtenir des avertissements, utilisez les commandes PowerShell. Pour plus d'informations, voir Récupérer les avertissements associés à un catalogue.

Locataires partagés pour les connexions. Vous pouvez désormais 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. Pour plus d'informations, consultez la section Modifier les paramètres de connexion.

Suppression de la prise en charge de la modification du type de système d'exploitation pour les catalogues Azure. Lorsque vous modifiez les images du catalogue, seules les images ayant le même type de système d'exploitation que l'image utilisée sont affichées. Grâce à cette amélioration, Citrix DaaS ne prend plus en charge la modification du type de système d'exploitation pour les catalogues Azure après la création du catalogue, par exemple le passage du système d'exploitation Windows à Linux et vice versa.

Février 2023

Fonctionnalités nouvelles et améliorées

Prise en charge du partage d'images entre différents locataires Azure. Auparavant, dans les environnements Azure, vous pouviez partager des images uniquement avec des abonnements partagés à l'aide d'Azure Compute Gallery. Grâce à cette fonctionnalité, vous pouvez désormais sélectionner une image dans la galerie Azure Compute qui appartient à un autre abonnement partagé auprès d'un client différent afin de créer et de mettre à jour un catalogue MCS. Pour plus d'informations, voir Partage d'images entre locataires Azure.

Modélisation de stratégie. La fonctionnalité de modélisation de stratégie est désormais disponible.

Vous pouvez simuler des stratégies à des fins de planification et de test. Pour plus d'informations, consultez la section Utiliser l'assistant de modélisation de stratégie.

Possibilité d'activer ou de désactiver les fonctionnalités préliminaires. Dans Configuration complète > Accueil, en tant qu'administrateur Citrix Cloud disposant d'un accès complet, vous pouvez désormais activer ou désactiver les fonctionnalités en version préliminaire sans contacter Citrix. Pour plus d'informations, consultez la section Page d'accueil de l'interface Configuration complète.

Rechercher des diagnostics de session à l'aide du nom d'utilisateur. Cette fonctionnalité permet d'utiliser les diagnostics de lancement de session en commençant par le nom d'utilisateur si vous ne possédez pas l'identifiant de transaction. Cette fonctionnalité est particulièrement utile aux administrateurs du service d'assistance pour trier les échecs de session si l'utilisateur final n'a pas saisi l'identifiant de transaction.
Vous pouvez rechercher un nom d'utilisateur et sélectionner une session à trier dans la liste des sessions avec échec que l'utilisateur a tenté de lancer au cours des dernières 48 heures. La page Diagnostics de lancements de session affiche les détails de la session ayant échoué. Elle répertorie le composant exact et le stade où la panne s'est produite. Pour plus d'informations, consultez Diagnostics de lancements de session.

Déployer des applications Web et SaaS sécurisées avec Secure Private Access. Dans l'onglet **Configuration complète > Applications > Applications**, une nouvelle option, **Ajouter des applications Web/SaaS**, est désormais disponible dans la barre d'actions. Cette option vous permet de déployer des applications Web et SaaS sécurisées avec Secure Private Access. Citrix Secure Private Access offre aux utilisateurs distants un moyen simple et flexible d'accéder à des applications Web, SaaS et client-serveur en utilisant une approche zéro confiance. Il permet l'authentification unique aux applications Web et SaaS, ainsi que des contrôles de sécurité précis tels que le filigrane et les contrôles de copier/coller, entre autres fonctionnalités de sécurité. Avec Citrix Secure Private Access, vous pouvez regrouper toutes vos applications virtualisées et non virtualisées en un seul endroit et améliorer l'expérience de vos utilisateurs. Voir Citrix Secure Private Access.

Filtrer le contenu du journal pour une durée spécifique. Une nouvelle option, **Personnalisé**, est désormais disponible dans la liste des durées dans **Configuration complète > Journalisation > Événements**. Utilisez-la pour spécifier la période des événements pour lesquels vous souhaitez filtrer votre recherche. Pour plus d'informations, consultez la section Journalisation de la configuration.

Mises à jour de la fonctionnalité Autoscale. Nous avons mis à jour l'option **Contrôlez le moment où Autoscale démarre les machines balisées** afin qu'elle soit plus facile à comprendre. L'option contrôle le moment où Autoscale commence à démarrer les machines balisées en fonction du pourcentage de la capacité restante des machines non 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. Pour plus d'informations, consultez la section Autoscaling des machines balisées (cloud bursting).

Stratégies de protection des applications. Vous pouvez désormais activer la protection des appli-

cations lors de la création ou de la modification d'un groupe de mise à disposition. Cette fonction fournit des fonctionnalités de protection contre les programmes d'enregistrement de frappe et de capture d'écran pour les sessions client. Pour plus d'informations, consultez Créer des groupes de mise à disposition et Gérer des groupes de mise à disposition.

Utilisation du GPU en temps réel disponible pour les GPU AMD. Vous pouvez désormais consulter l'utilisation des GPU AMD Radeon Instinct MI25 et des processeurs AMD EPYC 7V12 (Rome) sur Surveillance. Surveillance prend déjà en charge les GPU NVIDIA Tesla M60. L'utilisation du GPU affiche le pourcentage d'utilisation en temps réel 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. Les graphiques d'utilisation du GPU AMD ne sont disponibles que pour les VDA exécutant Windows 64 bits et Citrix Virtual Apps and Desktops 7 2212 ou version ultérieure. Pour plus d'informations, consultez la section Utilisation du GPU.

Prise en charge de la planification des mises à jour de la configuration dans Azure. Dans les environnements Azure, vous pouvez désormais planifier un créneau horaire pour les mises à jour de configuration des machines provisionnées par MCS à l'aide de la commande PowerShell `Schedule-ProvVMUpdate`. Toute mise sous tension ou redémarrage pendant le créneau horaire prévu applique une mise à jour planifiée du schéma de provisioning à une machine. Vous pouvez également annuler la mise à jour de la configuration avant le créneau prévu en utilisant `Cancel-ProvVMUpdate` .

Vous pouvez planifier et annuler la mise à jour de la configuration de :

- Une ou plusieurs machines virtuelles
- Un catalogue complet

Pour plus d'informations, voir Planifier les mises à jour de la configuration.

Prise en charge de l'utilisation d'images Citrix directement depuis Google Cloud Marketplace. Vous pouvez désormais parcourir et sélectionner les images proposées par Citrix sur Google Cloud Marketplace pour créer des catalogues MCS. Actuellement, MCS prend uniquement en charge le workflow de profil de machine pour cette fonctionnalité. Pour plus d'informations, consultez Google Cloud Marketplace.

Limiter la portée des groupes d'hôtes dans la connexion hôte à SCVMM. Auparavant, la connexion hôte à SCVMM exigeait que l'administrateur ait configuré un seul groupe d'hôtes de niveau supérieur. L'administrateur devait avoir pour cela une visibilité sur tous les groupes d'hôtes, clusters ou hôtes situés sous le seul groupe d'hôtes de niveau supérieur. Grâce à cette fonctionnalité, dans les déploiements de grande envergure où un seul SCVMM gère plusieurs clusters dans différents centres de données, vous pouvez désormais limiter la portée des groupes d'hôtes par les administrateurs. Pour ce faire, vous pouvez utiliser le rôle d'administrateur délégué dans la console Microsoft System Center Virtual Machine Manager (VMM) pour sélectionner les groupes d'hôtes auxquels un administrateur doit avoir accès. Pour plus d'informations, voir Installer et configurer un hyperviseur.

Prise en charge du stockage redondant interzone dans Azure. Auparavant, MCS ne proposait qu'un stockage localement redondant. Grâce à cette fonctionnalité, le stockage redondant interzone est désormais une option dans Azure, ce qui vous permet de sélectionner un type de stockage en fonction du type de redondance que vous souhaitez utiliser. Le stockage redondant interzone 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. Pour plus d'informations, voir Activer le stockage redondant interzone.

Janvier 2023

Fonctionnalités nouvelles et améliorées

Possibilité de mettre à niveau le disque de stockage vers une version antérieure, vers un disque dur standard, lorsque les machines virtuelles s'arrêtent. Une nouvelle option, **Activer la réduction des coûts de stockage**, est désormais disponible sur la page **Paramètres du disque** lorsque vous créez ou mettez à jour des catalogues Azure. Cette option permet de réduire les coûts de stockage en rétrogradant le disque de stockage et le disque de cache à écriture différée vers le disque dur standard lorsque la machine virtuelle s'arrête. La machine virtuelle revient à ses paramètres d'origine au redémarrage. Pour plus d'informations, voir Créer un catalogue Microsoft Azure.

Possibilité de configurer l'itinérance des sessions dans Configuration complète. Auparavant, PowerShell était votre seul choix pour configurer l'itinérance de session pour les applications et les bureaux. Vous pouvez désormais le faire dans **Configuration complète**. Pour de plus amples informations, consultez la section Gérer les groupes de mise à disposition.

Certaines actions ont été renommées pour mieux correspondre à leur signification réelle. Nous avons renommé les actions suivantes dans **Configuration complète > Catalogues de machines** et **Configuration complète > Groupes de mise à disposition**. Les workflow pour effectuer ces actions restent inchangés.

- **Mettre à jour les machines** est maintenant **Modifier image principale**
- **Restaurer la mise à jour de la machine** est maintenant **Restaurer image principale**
- **Mettre à niveau le catalogue** est maintenant **Modifier le niveau fonctionnel**
- **Mettre à niveau le groupe de mise à disposition** est maintenant **Modifier le niveau fonctionnel**
- **Annuler la mise à niveau du catalogue** est maintenant **Annuler modification du niveau fonctionnel**
- **Annuler la mise à niveau du groupe de mise à disposition** est maintenant **Annuler modification du niveau fonctionnel**

Prise en charge de l'organisation de groupes d'applications sous forme de dossiers Vous pouvez désormais créer des dossiers imbriqués pour organiser les groupes d'applications afin d'en faciliter l'

accès. Pour plus d'informations, voir Organiser les groupes d'applications sous forme de dossiers.

Améliorations des restrictions pour les groupes de mise à disposition. Auparavant, lorsque vous limitiez l'utilisation d'applications ou de bureaux pour un groupe de mise à disposition, vous pouviez spécifier uniquement les utilisateurs et les groupes d'utilisateurs autorisés à les utiliser dans un groupe de mise à disposition. Vous pouvez désormais également ajouter des utilisateurs et des groupes d'utilisateurs que vous souhaitez bloquer. Cette amélioration est utile lorsque vous ajoutez un groupe d'utilisateurs à une liste verte mais souhaitez bloquer un sous-ensemble d'utilisateurs de la liste verte. Pour plus d'informations, consultez la section Créer des groupes de mise à disposition.

Accès à Citrix Analytics for Performance - Détails de la session depuis Monitor. La page Détails de la session de Citrix Analytics for Performance est désormais intégrée à Moniteur. Cliquez sur **Afficher chronologie de la session** dans la page Sessions de Moniteur pour ouvrir la page Détails de la session de Citrix Analytics for Performance dans Moniteur. Cela nécessite que vous disposiez d'un droit Citrix Analytics for Performance valide. Les détails des sessions sont disponibles pour les sessions classées dans la catégorie Excellente, Acceptable ou Médiocre de Citrix Analytics for Performance.

Vous pouvez voir une tendance pour l'expérience de la session au cours des trois derniers jours, ainsi que les facteurs qui ont contribué à l'expérience. Ces informations complètent les données en temps réel disponibles dans Moniteur, utilisées par l'administrateur du service d'assistance lors de la résolution des problèmes liés à l'expérience de session.

Pour plus d'informations, consultez l'article Analyse de site.

Les machines virtuelles non persistantes sont supprimées des hyperviseurs ou des services cloud lorsque vous les supprimez ou supprimez leurs catalogues de machines dans Configuration complète. L'option permettant de conserver des machines virtuelles dans des hyperviseurs ou des services cloud n'est désormais disponible que pour les machines virtuelles persistantes. Pour de plus amples informations, consultez l'article Gérer des catalogues de machines.

Décembre 2022

Fonctionnalités nouvelles et améliorées

Prise en charge de la création de catalogues joints à Azure AD, joints à Azure AD Hybride et compatibles avec Microsoft Intune avec des VM principales jointes à Azure AD. Vous pouvez désormais créer des catalogues joints à Azure AD, joints à Azure AD Hybride et compatibles avec Microsoft Intune avec des VM principales jointes à Azure AD, à Azure AD Hybride et non jointes à un domaine. Si vous souhaitez gérer une VM principale à l'aide de Microsoft Intune, utilisez la version 2212 ou ultérieure du VDA et n'ignorez pas la préparation des images lors de la création ou de la mise à jour de catalogues de machines.

Pour plus d'informations sur les identités des machines, consultez Joint à Azure Active Directory, Microsoft Intune et Joint à Azure Active Directory Hybride.

Prise en charge dans MCS de la suppression des objets de machine virtuelle sans accéder à l'hyperviseur. Vous pouvez désormais supprimer des objets de machine virtuelle dans MCS sans avoir accès à l'hyperviseur. Lors de la suppression d'une machine virtuelle ou d'un schéma de provisioning, MCS doit supprimer les balises afin que les ressources ne soient plus suivies ou identifiées. Auparavant, si l'hyperviseur n'était pas accessible, les échecs de suppression des balises étaient ignorés. Avec cette fonctionnalité, si l'hyperviseur n'est pas accessible lors de l'utilisation de la commande `Remove-ProvVM`, la suppression de la balise échouera, mais en utilisant l'option `PurgeDBOnly`, vous pouvez toujours supprimer l'objet de ressource de la VM de la base de données. Pour plus d'informations, voir Supprimer des machines sans accès à l'hyperviseur.

Novembre 2022

Fonctionnalités nouvelles et améliorées

Prise en charge de la mise à disposition d'applications MSIX et d'applications packagées via l'attachement d'application MSIX Dans **Configuration complète > Packages d'applications**, vous pouvez désormais charger des applications MSIX et des applications packagées via l'attachement d'application MSIX vers Citrix Cloud et les mettre à disposition auprès de vos utilisateurs. Pour plus d'informations, consultez la section Packages d'applications.

Invite concernant les versions de VDA et niveaux fonctionnels non compatibles. L'interface Configuration complète vous alerte désormais en cas de versions et de niveaux fonctionnels de VDA non compatibles. Pour éviter les problèmes potentiels :

- Si une machine exécute une version de VDA non compatible, vous êtes invité à effectuer une mise à niveau vers une version compatible.
- Si le niveau fonctionnel d'un catalogue ou d'un groupe de mise à disposition n'est pas compatible, vous êtes invité à le définir à un niveau supérieur.

> **Conseil :**
>
> Les VDA sont couverts par les cycles de vie CR et LTSR de Citrix Virtual Apps and Desktops.

Possibilité d'annoter les images principales étendue à la création de catalogue. Lorsque vous créez un catalogue MCS dans **Configuration complète**, vous pouvez désormais annoter son image principale. Pour plus d'informations, veuillez consulter la section Image principale.

Prise en charge de l'exportation des données d'attribution de bureau via Configuration complète. Lorsque vous consultez les attributions de bureau pour un groupe de mise à disposition d'OS mono-session, vous pouvez désormais exporter les données d'attribution dans un fichier CSV à des

fins d'audit. Pour ce faire, sélectionnez ce groupe de mise à disposition dans **Configuration complète > Groupes de mise à disposition**, accédez à l'onglet **Bureaux**, puis cliquez sur **Exporter** dans le coin supérieur gauche de l'onglet.

Tous les onglets Applications et Dossiers d'applications sont regroupés en un seul. Dans **Configuration complète > Applications**, les onglets **Toutes les applications** et **Dossiers d'applications** ont été regroupés en un seul onglet, **Applications**. Cette modification unifie l'expérience utilisateur en matière de gestion des vues de dossiers sur les nœuds Configuration complète.

Prise en charge du changement de type de stockage vers un niveau inférieur lorsqu'une machine virtuelle est arrêtée dans des environnements Azure. Dans les environnements Azure, vous pouvez désormais 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 `WBCDiskStorageType`). Pour plus d'informations, consultez Changer le type de stockage vers un niveau inférieur lorsqu'une machine virtuelle est arrêtée.

Mises à jour dans la vue Filtres. La page Filtres de Moniteur est mise à jour pour inclure des listes distinctes de filtres enregistrés et de filtres par défaut afin d'améliorer la visualisation et l'accessibilité des filtres. Vous pouvez sélectionner une vue parmi les machines, les sessions, les connexions ou les instances d'application. Vous pouvez ensuite sélectionner un filtre dans la liste des filtres enregistrés ou des filtres par défaut pour afficher la liste des données filtrées. Vous pouvez utiliser les listes déroulantes pour affiner les critères de filtre ou modifier les critères existants. Vous pouvez enregistrer votre filtre dans la liste des filtres enregistrés. Pour plus d'informations, veuillez consulter l'article Filtres.

Possibilité de réinitialiser le disque d'OS d'une VM persistante dans un catalogue de machines créé par MCS. Dans les environnements de virtualisation VMware, vous pouvez désormais utiliser la commande PowerShell `Reset-ProvVMDisk` pour réinitialiser le disque d'OS d'une VM persistante dans un catalogue de machines créé par MCS. La fonctionnalité automatise le processus de réinitialisation du disque d'OS. Par exemple, elle permet de réinitialiser la machine virtuelle à son état initial dans un catalogue de bureau de développement persistant créé à l'aide de MCS.

Pour plus d'informations sur l'utilisation de la commande PowerShell pour réinitialiser le disque d'OS, voir Réinitialiser le disque d'OS.

Prise en charge de la mise à jour du profil de machine et des propriétés personnalisées supplémentaires des machines provisionnées par MCS dans les environnements Azure. Auparavant, dans les environnements Azure, vous pouviez utiliser `Request-ProvVMUpdate` pour mettre à jour la propriété `ServiceOffering` personnalisée d'une machine provisionnée par MCS. Désormais,

vous pouvez également mettre à jour le profil de la machine et les propriétés personnalisées suivantes :

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

Pour plus d'informations, consultez Mettre à jour les machines provisionnées vers l'état du schéma de provisioning actuel.

Prise en charge du profil de machine dans GCP. Lorsque vous créez un catalogue pour provisionner des machines à l'aide de Machine Creation Services (MCS) dans des environnements Google Cloud Platform (GCP), 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.

Les profils de machines fonctionnent avec les systèmes d'exploitation Linux et Windows.

Pour plus d'informations sur la création d'un catalogue de machines avec un profil de machine, voir Créer un catalogue de machines à l'aide d'un profil de machine.

Prise en charge de la mise à jour des machines provisionnées avec MCS dans les environnements GCP. Dans les environnements GCP, `Set-ProvScheme` modifie le modèle (schéma de provisioning) et n'affecte pas les machines existantes. À l'aide de la commande Powershell `Request-ProvVMUpdate`, vous pouvez désormais appliquer le schéma de provisioning actuel à une machine existante (ou à un ensemble de machines). Actuellement, dans GCP, la mise à jour des propriétés prise en charge par cette fonctionnalité est le profil de machine. Pour plus d'informations, voir Mettre à jour les machines provisionnées à l'aide de PowerShell.

Octobre 2022

Fonctionnalités nouvelles et améliorées

Prise en charge de l'utilisation simultanée de profils de machines et de groupes d'hôtes. Lorsque vous créez un catalogue à l'aide d'une image principale d'Azure Resource Manager, vous pouvez désormais utiliser simultanément un profil de machine et un groupe d'hôtes. Cela est utile dans les

scénarios où vous souhaitez utiliser le lancement fiable pour améliorer la sécurité et exécuter les machines sur des hôtes dédiés. Pour de plus amples informations, consultez Environnements de virtualisation Microsoft Azure Resource Manager.

Prise en charge de l'organisation de groupes de mise à disposition sous forme de dossiers Vous pouvez désormais créer une arborescence de dossiers pour organiser les groupes de mise à disposition afin d'en faciliter l'accès. Pour plus d'informations, voir Organiser les groupes de mise à disposition sous forme de dossiers.

Prise en charge de la planification d'un redémarrage unique pour les machines via la configuration complète. Une nouvelle option, **Une fois**, est désormais disponible lorsque vous créez des calendriers de redémarrage pour les groupes de mise à disposition. Avec cette option, vous pouvez programmer les machines d'un groupe de mise à disposition pour qu'elles redémarrent une seule fois, à une date et une heure spécifiées. Pour plus d'informations, consultez la rubrique Créer un programme de redémarrage.

Planification avancée des analyses. La planification améliorée des analyses d'application et de bureau peut désormais être effectuée à partir de l'onglet Surveiller. À l'aide de cette fonctionnalité, Citrix Probe Agent peut être configuré pour exécuter les tâches d'analyse certains jours de la semaine et les répéter à des intervalles spécifiés au cours de la journée. Cela vous permet de planifier une seule tâche d'analyse à répéter à des moments spécifiques de la journée et de la semaine. Vous pouvez désormais vérifier de manière proactive l'état de santé de votre site grâce à des analyses configurées pour s'exécuter régulièrement à des moments appropriés. Cette fonctionnalité simplifie la configuration et la gestion des analyses dans l'onglet Surveiller. Pour plus d'informations, consultez Analyse d'applications et de bureaux.

Septembre 2022

Fonctionnalités nouvelles et améliorées

Les anciennes versions du SDK Remote PowerShell sont désormais obsolètes. Si vous utilisez une version obsolète, le SDK cesse de fonctionner et un message d'erreur vous invite à télécharger la version actuelle. Dans ce cas, téléchargez la dernière version du SDK Remote PowerShell depuis le site Web de Citrix.

Catalogues de machines avec lancement fiable dans Azure. Dans les environnements Azure, vous pouvez créer des catalogues de machines compatibles avec le lancement fiable et utiliser la propriété `SupportsTrustedLaunch` de l'inventaire des machines virtuelles pour déterminer la taille des machines virtuelles qui prennent en charge le lancement fiable.

Le lancement fiable est un moyen transparent d'améliorer la sécurité des machines virtuelles de deuxième génération. Un lancement fiable protège contre les techniques d'attaque avancées et persistantes. Pour plus d'informations, voir Catalogues de machines avec lancement fiable.

Prise en charge de l'identification de ressources Microsoft System Center Virtual Machine Manager créées par MCS. Vous pouvez désormais identifier les ressources Microsoft System Center Virtual Machine Manager (SCVMM) créées par MCS à l'aide de balises. Pour plus d'informations sur les balises que MCS ajoute aux ressources, consultez Identifier les ressources créées par MCS.

Prise en charge de l'identification des ressources VMware créées par MCS. Vous pouvez désormais identifier les ressources VMware créées par MCS à l'aide de balises. Pour plus d'informations sur les balises que MCS ajoute aux ressources, consultez Identifier les ressources créées par MCS.

Prise en charge de l'optimisation de la limitation d'AWS Workspace. Vous pouvez désormais allumer et éteindre un grand nombre de machines dans AWS Workspace sans rencontrer de problèmes de limitation. Des problèmes de limitation se produisent lorsque le nombre de demandes envoyées à AWS Workspace dépasse le nombre de demandes que le serveur peut gérer. Par conséquent, Citrix regroupe désormais plusieurs demandes en une seule demande avant de l'envoyer au SDK AWS Workspace.

Possibilité de vérifier les détails de la machine lors de la visualisation du nombre de machines sur la page d'accueil. Lorsque vous consultez le nombre de machines par état de disponibilité dans **Accueil**, vous pouvez désormais cliquer sur un état pour afficher les détails des machines dans cet état. Pour plus d'informations, consultez la section Page d'accueil de l'interface Configuration complète.

Prise en charge de la création de catalogues de machines à l'aide d'une image provenant d'un abonnement différent dans le même locataire Azure. Auparavant, dans les environnements Azure, vous pouviez uniquement sélectionner une image dans votre abonnement pour créer un catalogue de machines. Grâce à cette fonctionnalité, vous pouvez désormais sélectionner une image dans Azure Compute Gallery (anciennement Shared Imaged Gallery) qui appartient à un autre abonnement partagé pour créer et mettre à jour des catalogues MCS.

Pour plus d'informations sur la création d'un catalogue, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager.

Pour plus d'informations sur le partage d'images avec un autre principal de service chez le même locataire, consultez la section Partage d'images avec un autre principal de service chez le même locataire.

Pour plus d'informations sur les commandes PowerShell permettant de sélectionner une image provenant d'un autre abonnement, consultez la section Utilisation de PowerShell pour sélectionner une image provenant d'un autre abonnement.

Pour plus d'informations sur Azure Compute Gallery, consultez Azure Shared Image Gallery.

Août 2022

Fonctionnalités nouvelles et améliorées

Prise en charge de l'identification des ressources Citrix Hypervisor créées par MCS. Vous pouvez désormais identifier les ressources Citrix Hypervisor créées par MCS à l'aide de balises. Pour plus d'informations sur les balises que MCS ajoute aux ressources, consultez Identifier les ressources créées par MCS.

Prise en charge de l'utilisation simultanée de groupes d'hôtes et de zones de disponibilité Azure. Dans les environnements Azure, il existe désormais une vérification préliminaire permettant de déterminer si la création d'un catalogue de machines sera réussie en fonction de la zone de disponibilité Azure spécifiée dans la propriété personnalisée et de la zone du groupe d'hôtes. La création du catalogue échoue si la propriété personnalisée de la zone de disponibilité ne correspond pas à la zone du groupe d'hôtes.

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. Les zones de disponibilité Azure sont des emplacements physiquement distincts au sein de chaque région Azure qui sont tolérantes aux défaillances locales.

Pour plus d'informations sur les différentes combinaisons de zone de disponibilité et de zone de groupe d'hôtes qui entraînent la réussite ou l'échec de la création du catalogue de machines, consultez la section Utilisation simultanée de groupes d'hôtes et de zones de disponibilité Azure.

Prise en charge de la mise à jour de l'ID de dossier d'un catalogue de machines dans VMware. Dans les environnements de virtualisation VMware, vous pouvez désormais mettre à jour l'ID de dossier d'un catalogue de machines MCS à l'aide de la propriété personnalisée `FolderID` dans `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. Pour plus d'informations sur la mise à jour de l'ID de dossier, consultez Mettre à jour l'ID de dossier d'un catalogue de machines.

Configuration du fuseau horaire. Vous pouvez désormais configurer le format de date et d'heure de l'interface en fonction de vos préférences à l'aide du paramètre **Date et heure**. Pour plus d'informations, consultez la section Configuration du fuseau horaire.

Le service de portabilité des images (IPS) prend désormais en charge Amazon Web Services (AWS). Si les autorisations et les composants requis pour AWS sont configurés, les workflow IPS peuvent être utilisés avec un compte AWS. Consultez Migrer des charges de travail vers un cloud public pour plus de détails.

Configuration du fichier d'échange lors de la préparation de l'image dans les environnements Azure. Dans les environnements Azure, vous pouvez désormais éviter toute confusion potentielle

avec l'emplacement du fichier d'échange. À cette fin, MCS détermine désormais l'emplacement du fichier d'échange lorsque vous créez le schéma de provisioning lors de la préparation de l'image. Ce calcul est basé sur certaines règles. Les fonctionnalités telles que le disque d'OS éphémère (EOS) et E/S de MCS disposent de leur propre emplacement de fichier d'échange attendu et s'excluent mutuellement. De plus, si vous déconnectez la préparation de l'image de la création du schéma de provisioning, MCS détermine correctement l'emplacement du fichier d'échange. Pour plus d'informations sur l'emplacement du fichier d'échange, voir Emplacement du fichier d'échange.

Prise en charge de la mise à jour des paramètres du fichier d'échange dans les environnements Azure. Lors de la création d'un catalogue dans un environnement Azure, vous pouvez désormais spécifier le paramètre du fichier d'échange, y compris son emplacement et sa taille, à l'aide des commandes PowerShell. Cela remplace le paramètre du fichier d'échange déterminé par MCS. Pour ce faire, exécutez la commande `New-ProvScheme` avec 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

Pour plus d'informations sur la mise à jour du paramètre du fichier d'échange, consultez la section Mettre à jour le paramètre.

Mises à jour de la page d'accueil. Le widget Démarrer a maintenant une nouvelle apparence. Les autres mises à jour de la page d'accueil incluent :

- Les nouvelles icônes d'actualisation et d'aide dans le coin supérieur droit.
- Les nombres de ressources cliquables, ce qui permet d'accéder rapidement aux pages de ressources pertinentes.
- Amélioration de l'icône Je n'aime pas. Si vous n'aimez pas une recommandation, celle-ci disparaît. Si vous n'aimez pas le widget de recommandation, celui-ci disparaît.

Pour plus d'informations, consultez la page d'accueil.

Prise en charge de l'activation des extensions de machines virtuelles Azure. Lorsque vous utilisez une spécification de modèle ARM comme profil de machine pour créer un catalogue de machines, vous pouvez désormais ajouter des extensions Azure VM aux machines virtuelles du catalogue, afficher la liste des extensions prises en charge et supprimer les extensions que vous avez ajoutées. Les extensions Azure VM sont de petites applications qui fournissent des tâches de configuration et d'automatisation post-déploiement sur les machines virtuelles Azure. Par exemple, si une machine virtuelle nécessite l'installation d'un logiciel, une protection antivirus ou la possibilité d'exécuter un script à l'intérieur de celle-ci, vous pouvez utiliser une extension VM. Pour plus d'informations sur la façon d'activer les extensions Azure VM, consultez Utiliser PowerShell pour activer les extensions Azure VM.

Prise en charge du lancement fiable pour les disques d'OS éphémères. Vous pouvez désormais créer des schémas de provisioning à l'aide du disque d'OS éphémère sous Windows avec lancement fiable. Le lancement fiable est un moyen transparent d'améliorer la sécurité des machines virtuelles de deuxième génération. Il protège contre les techniques d'attaque avancées et persistantes en combinant des technologies qui peuvent être activées indépendamment, comme le démarrage sécurisé et la version virtualisée du module de plate-forme sécurisée (vTPM). Pour plus d'informations sur la création d'un catalogue de machines, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager.

Juillet 2022

Fonctionnalités nouvelles et améliorées

Délais d'expiration de session dynamique pour les machines avec OS mono-session. Les délais d'expiration de session dynamique prennent désormais en charge les machines avec OS mono-session Un groupe de mise à disposition avec au moins un VDA version 2206 ou ultérieure est requis. Assurez-vous que ces VDA se sont enregistrés auprès de Citrix Cloud au moins une fois. Pour plus d'informations, consultez la section Délai d'expiration de session dynamique.

Envoyer des rappels de fermeture de session sans forcer l'utilisateur à se déconnecter. Une nouvelle fonctionnalité est désormais disponible dans **Notifications de fermeture de session utilisateur** (anciennement **Forcer fermeture de la session utilisateur**) dans Autoscale. Cette fonctionnalité vous permet d'envoyer des rappels de fermeture de session aux utilisateurs sans les forcer à se déconnecter. Cela permet d'éviter les pertes de données potentielles causées par la fermeture forcée des sessions utilisateur. Pour plus de détails, consultez la section Notifications de fermeture de session utilisateur.

Possibilité de définir le type de licence du système d'exploitation Linux lors de la création de catalogues de machines virtuelles Linux dans Azure. À l'aide de l'interface Configuration complète, vous pouvez désormais choisir le type de licence du système d'exploitation Linux lors de la création de catalogues de machines virtuelles Linux dans Azure. Vous avez le choix entre deux licences Linux : Red Hat Enterprise Linux et SUSE Linux Enterprise Server. Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager.

Expérience de recherche améliorée dans Configuration complète. Le nœud Rechercher fournit les nouvelles fonctionnalités et améliorations suivantes :

- **Possibilité d'exporter les résultats de recherche**. Vous pouvez désormais exporter les résultats de recherche. Pour ce faire, cliquez sur l'icône d'exportation dans le coin supérieur droit.
- **Nouveau filtre disponible**. Un filtre, Action d'alimentation en attente, est désormais disponible. Utilisez ce filtre pour affiner votre recherche.

- **Prise en charge de la recherche « Ne contient pas » pour certains éléments.** Des éléments tels que les noms de machines et les balises prennent désormais en charge les critères de recherche « Ne contient pas ».
- **Prise en charge de la recherche d'objets lors de l'ajout de filtres.** Lorsque vous ajoutez des filtres aux objets suivants, vous pouvez désormais les rechercher : connexions, catalogues de machines, groupes de mise à disposition, groupes d'applications et balises.

Pour plus d'informations, voir Utiliser la recherche dans l'interface de gestion Configuration complète.

Prise en charge des profils de stockage VMware. Lorsque vous créez un catalogue de machines à l'aide d'une image principale sur un datastore vSAN, vous pouvez désormais copier la stratégie de stockage telle que les informations RAID-1 ou RAID-5 de l'image principale sur les machines cibles créées. Pour les catalogues existants, la stratégie de stockage reste inchangée même si vous mettez à jour le catalogue.

Enregistrement SPN RestrictedKrbHost. Tous les comptes d'ordinateurs créés par Citrix MCS sont désormais enregistrés avec Service Principal Names (SPN) `RestrictedKrbHost`. Cela évite d'avoir à exécuter la commande `setspn` pour enregistrer le SPN pour les comptes d'ordinateurs une fois que MCS les a créés.

Packages d'applications dans Configuration complète pour fournir des applications Microsoft sous forme de packages. Le nœud App-V est désormais nommé Packages d'applications et a été remanié pour gérer davantage de types d'applications Microsoft packagées. Auparavant, vous deviez utiliser le module de détection pour ajouter des applications packagées App-V à votre environnement en vue de leur mise à disposition. Vous pouvez désormais ajouter et mettre à disposition les applications en un seul endroit à l'aide du nœud Packages d'applications. Pour plus d'informations, consultez la section Packages d'applications.

Prise en charge de l'utilisation de spécifications de modèles ARM en tant que profils de machines. Auparavant, vous pouviez uniquement utiliser des machines virtuelles comme profils de machine. Vous pouvez désormais utiliser les spécifications des modèles ARM comme profils de machine lors de la création de catalogues de machines Azure. Cette fonctionnalité vous permet de tirer parti des fonctionnalités du modèle Azure ARM telles que la gestion des versions. Pour nous assurer que la spécification sélectionnée est correctement configurée et contient les configurations requises, nous procédons à sa validation. Si la validation échoue, vous êtes invité à sélectionner un autre profil de machine. Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager.

Prise en charge de la validation des spécifications du modèle ARM. Vous pouvez désormais valider 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 :

- À l'aide de l'interface de gestion Configuration complète
- À l'aide de la commande PowerShell

Pour plus d'informations sur la validation de la spécification du modèle ARM, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager.

Juin 2022

Fonctionnalités nouvelles et améliorées

Prise en charge du programme de redémarrage pour les machines avec OS mono-session. Auparavant, la fonction de programme de redémarrage n'était disponible que pour les machines avec OS multi-session. Il est désormais également disponible pour les machines avec OS mono-session. Vous pouvez désormais créer des programmes de redémarrage pour les groupes de mise à disposition contenant des machines avec OS mono-session. Pour plus d'informations, voir Créer et gérer des programmes de redémarrage pour les machines d'un groupe de mise à disposition.

Possibilité d'effectuer des pré-vérifications du nom d'utilisateur. Une option, **Vérifier le nom**, est désormais disponible lorsque vous entrez les informations d'identification du domaine. Cette option vous permet de 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.

Pour plus d'informations, voir Informations d'identification du domaine.

Possibilité de modifier le paramètre réseau pour un schéma de provisioning existant. Vous pouvez désormais 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. Seules les machines virtuelles nouvellement provisionnées à partir du schéma auront les nouveaux paramètres de sous-réseau. Vous devez également vous assurer que les sous-réseaux se trouvent sous la même unité d'hébergement. Pour plus d'informations, consultez la section Modifier le paramètre réseau pour un schéma de provisioning existant.

Récupération des informations de nom de région pour les machines virtuelles Azure, les disques gérés, les instantanés, le disque dur virtuel Azure et le modèle ARM. Vous pouvez désormais afficher les informations de nom de région pour une machine virtuelle Azure, des disques gérés, des instantanés, un disque dur virtuel Azure et un modèle ARM. Ces informations sont affichées pour les

ressources de l'image principale lorsqu'un catalogue de machines est affecté. Pour plus d'informations, consultez la section Récupérer les informations de nom de région pour les machines virtuelles Azure, les disques gérés, les instantanés, le disque dur virtuel Azure et le modèle ARM.

Possibilité d'utiliser les valeurs des propriétés de profil de machine dans l'environnement Azure. Lorsque vous créez un catalogue Azure avec un profil de machine, vous pouvez désormais définir les valeurs des propriétés à partir de la spécification du modèle ARM ou de la machine virtuelle, selon ce qui est utilisé comme profil de machine, si les valeurs ne sont pas explicitement définies dans les propriétés personnalisées. Les propriétés concernées par cette fonctionnalité sont les suivantes :

- Zone de disponibilité
- ID de groupe d'hôtes dédié
- ID de jeu de chiffrement de disque
- Type d'OS
- Type de licence
- Offre de services
- Type de stockage

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. Pour plus d'informations, voir Utiliser les valeurs des propriétés du profil machine.

Prise en charge étendue de la mise à niveau de VDA. À l'aide de l'interface Configuration complète, vous pouvez désormais mettre à niveau des machines persistantes provisionnées par MCS. Vous pouvez les mettre à niveau par catalogue ou par machine. Pour plus d'informations, consultez Mettre à niveau les VDA à l'aide de l'interface Configuration complète.

Citrix Probe Agent dans les plans de contrôle Citrix Cloud Japan et Citrix Cloud Government. Citrix Probe Agent prend désormais en charge les sites hébergés sur Citrix Cloud Japan et Citrix Cloud Government Planes. Pour utiliser l'agent dans ces plans, définissez la valeur de registre du chemin "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region"sur 2 pour Japan et sur 3 pour Government. Citrix Probe Agent automatise le processus de vérification de l'intégrité des applications et des bureaux virtuels publiés sur un site. Pour plus d'informations, consultez Analyse d'applications et de bureaux.

Personnaliser le port utilisé pour la communication entre les VDA et les Cloud Connector. Vous pouvez désormais personnaliser le port que le VDA utilise pour communiquer avec les Cloud Connector en fonction de vos exigences de sécurité spécifiques. Cette fonctionnalité est utile si votre équipe chargée de la sécurité n'autorise pas l'ouverture du port par défaut (port 80) ou si le port par défaut est déjà utilisé. Pour plus d'informations, consultez Personnaliser le port pour communiquer avec les Cloud Connector.

Organisation des catalogues de machines sous forme de dossiers. Vous pouvez désormais créer

des dossiers imbriqués pour organiser les catalogues de machines afin d'en faciliter l'accès. Pour plus d'informations, voir Organiser les catalogues sous forme de dossiers.

Prise en charge de SCVMM 2022. Citrix DaaS prend désormais en charge Microsoft System Center Virtual Machine Manager (SCVMM) 2022. SCVMM fournit une gamme de services qui incluent la maintenance des ressources dont vous avez besoin pour déployer des machines virtuelles. Pour plus d'informations sur les nouvelles fonctionnalités prises en charge dans SCVMM 2022, consultez Nouveautés de System Center Virtual Machine Manager.

Prise en charge de la configuration du paramètre d'opérations de provisioning simultanées maximum sur AWS. Citrix DaaS prend désormais en charge `MaximumConcurrentProvisioningOperation` en tant que propriété personnalisée configurable pour MCS sur AWS. `MaximumConcurrentProvisioningOp` est la propriété qui détermine le nombre de machines virtuelles que vous pouvez créer ou supprimer simultanément. Bien que MCS prenne en charge un maximum de 100 opérations de provisioning simultanées par défaut, vous pouvez désormais saisir des commandes PowerShell pour personnaliser cette valeur. Vous pouvez saisir une plage comprise entre 1 et 1 000. La définition de cette propriété sur la valeur de votre choix vous permet de contrôler le nombre de tâches parallèles que vous pouvez effectuer lors de la création ou de la suppression de machines virtuelles. Pour plus de détails sur la configuration des opérations de provisioning simultanées maximales, voir Valeurs par défaut des connexions hôtes.

Mai 2022

Fonctionnalités nouvelles et améliorées

Diagnostic de lancement de session amélioré. Citrix DaaS prend désormais en charge un diagnostic d'échec de lancement de session détaillé. Vous pouvez désormais afficher les composants impliqués dans la séquence de lancement de session. Les composants qui ont échoué, ainsi que les derniers codes d'erreur générés sont mis en surbrillance. Cela permet d'identifier la raison exacte d'un échec de lancement de session et de prendre les mesures recommandées.

La page Transaction est complétée par le panneau Détails de la transaction qui contient une liste de composants indiquant l'occurrence de l'erreur. Cliquez sur le nom du composant pour afficher les champs Détails du composant et Détails de la dernière défaillance connue. Les champs Raison de l'échec et Code d'erreur s'affichent. Cliquez sur le lien En savoir plus sur l'erreur pour afficher le code d'erreur spécifique dans la section Codes d'erreur qui contient la description détaillée et l'action recommandée. Pour plus d'informations, consultez Diagnostic de lancement de session.

Prise en charge de l'utilisation de Set-ProvServiceConfigurationData dans le SDK Remote PowerShell. Vous pouvez désormais exécuter `Set-ProvServiceConfigurationData` à l'aide du SDK Remote PowerShell pour configurer tous les paramètres applicables. Vous pouvez également ignorer l'activation de DHCP pendant la préparation de l'image à l'aide de cette commande. Voici la

liste des paramètres pris en charge par `Set-ProvServiceConfigurationData` :

- Modifier le délai de préparation de l'image : `Set-ProvServiceConfigurationData -Name "ImageManagementPrep_PreparationTimeout"-value 60`
- Ignorer Activer DHCP : `Set-ProvServiceConfigurationData -Name ImageManagementPrep_ -Value EnableDHCP`
- Ignorer Réarmer Microsoft Windows KMS : `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OsRearm`
- Ignorer Réarmer Microsoft Office KMS : `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OfficeRearm`
- Désactiver l'arrêt automatique de la VM de préparation : `Set-ProvServiceConfigurationData –Name ImageManagementPrep_NoAutoShutdown –Value true`
- Désactiver l'injection de domaine : `Set-ProvServiceConfigurationData –Name DisableDomainInjection –Value true`

Possibilité de définir le type de licence Linux lors de la création de catalogues de machines Linux à l'aide des commandes PowerShell. À l'aide des commandes PowerShell, vous pouvez définir le type de licence Linux lors de la création de catalogues de machines Linux. Vous avez le choix entre deux licences Linux : RHEL_BYOS et SLES_BYOS. Le paramètre par défaut est la licence Azure Linux. Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager.

Prise en charge de l'identification de toutes les ressources Azure créées par MCS. Vous pouvez désormais identifier toutes les ressources Azure créées par MCS, telles que l'image, le disque ID, le disque du système d'exploitation, la carte réseau, la machine virtuelle, etc. qui sont associées à un paramètre ProvScheme à l'aide d'une balise appelée `provschemeID`. Pour plus d'informations sur les balises que MCS ajoute aux ressources, consultez Identifier les ressources créées par MCS.

Prise en charge du provisioning Azure Stack HCI via SCVMM. MCS prend désormais en charge le provisioning Azure Stack HCI via Microsoft System Center Virtual Machine Manager (SCVMM). Vous pouvez gérer le cluster Azure Stack HCI avec vos outils existants, y compris SCVMM. Pour de plus amples informations, consultez Environnements de virtualisation Microsoft System Center Virtual Machine Manager.

Prise en charge de l'ajout manuel d'utilisateurs non Active Directory. À l'aide de l'interface de gestion Configuration complète, vous pouvez désormais entrer une liste de noms d'utilisateur séparés par des points-virgules lorsque vous ajoutez des utilisateurs non Active Directory à un catalogue. Tenez compte du format lors de l'ajout d'utilisateurs résidant dans des répertoires différents. Par exemple, si les utilisateurs se trouvent dans Active Directory, entrez directement les noms. Si ce n'est pas le cas, entrez les noms au format suivant : `<identity provider>:<user name>`. Exemple :

`AzureAD:username`. Pour de plus amples informations, consultez l'article Créer un catalogue de machines.

Avril 2022

Fonctionnalités nouvelles et améliorées

Page d'accueil de l'interface Configuration complète. L'interface Configuration complète dispose désormais d'une page d'accueil, qui fournit une vue d'ensemble de votre déploiement et de vos charges de travail Citrix DaaS, ainsi que des informations qui vous aident à tirer le meilleur parti de votre abonnement. La page comprend les parties suivantes :

- **Aperçu du service**. Fournit une vue d'ensemble de votre déploiement et de vos charges de travail Citrix DaaS.
- **Recommandations**. Recommande les fonctionnalités disponibles avec votre abonnement et recueille vos commentaires.
- **Nouveautés**. Affiche les dernières fonctionnalités.
- **Fonctionnalités préliminaires**. Affiche les fonctionnalités actuellement en version préliminaire.
- **Mise en route**. Affiche les étapes qui vous guideront tout au long de la configuration initiale.

Pour plus d'informations, consultez la page d'accueil.

Afficher la progression de la création et des mises à jour de catalogue. L'interface Configuration complète vous permet désormais de rester informé de la création et des mises à jour du catalogue. Vous pouvez obtenir une vue d'ensemble du processus de création et de mise à jour, consulter l'historique des étapes effectuées et suivre la progression et la durée d'exécution de l'étape en cours. Pour plus d'informations, voir Commencer à créer le catalogue.

Afficher les hyperviseurs et les services cloud disponibles en fonction de la zone sélectionnée. Dans Configuration complète, lorsque vous créez des connexions d'hébergement, vous devez sélectionner une zone avant de sélectionner un type de connexion. La liste déroulante Type de connexion affiche les hyperviseurs et les services cloud disponibles avec la zone. Auparavant, pour vous assurer que la liste Type de connexion indiquait un hyperviseur ou un service cloud requis, vous deviez installer son plug-in dans chaque zone. Avec cette nouvelle séquence de configuration, vous pouvez désormais installer le plug-in uniquement dans la zone requise.

Vous pouvez également utiliser la commande PowerShell pour obtenir la liste des plug-ins d'hyperviseur disponibles avec la zone sélectionnée. Pour de plus amples informations, consultez Créer une connexion et des ressources.

Prise en charge des utilisateurs non joints à une instance AD locale dans Configuration complète. Un nouveau champ, **Sélectionner le type d'identité**, est disponible dans les interfaces dans

lesquelles vous attribuez des utilisateurs à des bureaux ou applications provisionnés, à des groupes de mise à disposition ou à des groupes d'applications. Avec ce champ, vous pouvez désormais sélectionner des comptes utilisateur parmi l'un des fournisseurs d'identité suivants auxquels votre Citrix Cloud est connecté :

- Active Directory
- Azure Active Directory
- Okta

Possibilité de rejeter des propriétés personnalisées non valides dans des environnements Google Cloud Platform (GCP) et Azure. Vous pouvez désormais éviter toute confusion potentielle si les propriétés personnalisées définies sur `New-ProvScheme` et `Set-ProvScheme` ne prennent pas effet. Si vous spécifiez une ou plusieurs propriétés personnalisées inexistantes, un message d'erreur s'affiche. Pour plus d'informations, voir Considérations importantes concernant la définition de propriétés personnalisées.

Prise en charge de la création de machines jointes à Azure Active Directory. Dans **Configuration complète**, lorsque vous créez un catalogue, un type d'identité **Joint à Azure Active Directory** est désormais disponible dans **Identités des machines**. Avec ce type d'identité, vous pouvez utiliser MCS pour créer des machines qui sont jointes à Azure Active Directory. Vous avez également une option supplémentaire, **Inscrire les machines dans Microsoft Intune**, pour inscrire les machines dans Microsoft Intune à des fins de gestion.

Pour plus d'informations sur la création de catalogues joints à Azure Active Directory, voir Créer des catalogues de machines. Pour plus d'informations sur les exigences et les considérations relatives à la jonction à Azure Active Directory, voir Joint à Azure Active Directory.

Prise en charge de la création de machines jointes à Azure Active Directory hybride. Dans **Configuration complète**, lorsque vous créez un catalogue, un type d'identité **Joint à Azure Active Directory hybride** est désormais disponible dans **Identités des machines**. Avec ce type d'identité, vous pouvez utiliser MCS pour créer des machines jointes à Azure Active Directory Hybride. Ces machines appartiennent à une organisation et sont connectées avec un compte des services de domaine Active Directory appartenant à cette organisation.

Pour plus d'informations sur la création de catalogues joints à Azure Active Directory hybride, voir Créer des catalogues de machines. Pour plus d'informations sur les exigences et les considérations relatives à la jonction à Azure Active Directory Hybride, voir Joint à Azure Active Directory Hybride.

Prise en charge du lancement fiable Azure pour les instantanés. Outre les images, le lancement fiable Azure est désormais également disponible pour les instantanés. Si vous sélectionnez un instantané pour lequel le lancement fiable est activé, l'utilisation d'un profil de machine est obligatoire. Vous devez également sélectionner un profil de machine pour lequel le lancement fiable est activé. Pour de plus amples informations, consultez Environnements de cloud Microsoft Azure Resource Manager.

Exporter des machines. Vous pouvez désormais exporter les machines répertoriées sur la page **Machines** de l'assistant **Configuration du catalogue de machines** vers un fichier CSV, à utiliser comme modèle lors de l'ajout de machines à un catalogue en bloc. Pour plus d'informations, voir Exporter des machines à partir d'un catalogue.

Option permettant d'accéder à la console Web Workspace Environment Management. Une option, Gestion de l'environnement (Web), est désormais disponible dans le menu de l'onglet **Gérer**. Cette option vous permet d'accéder à la nouvelle console web, Workspace Environment Management. Pour accéder à l'ancienne console, utilisez **Gestion de l'environnement**. Nous sommes en train de migrer l'ensemble complet des fonctionnalités de l'ancienne console vers la console Web. La console Web répond généralement plus rapidement que l'ancienne console. Pour plus d'informations, consultez Service Workspace Environment Management.

Possibilité de gérer les paramètres ProvScheme. Lorsque vous utilisez MCS pour créer un catalogue, vous obtenez désormais une erreur si vous définissez les paramètres `New-ProvScheme` dans des hyperviseurs non pris en charge lors de la création du catalogue de machines ou si vous mettez à jour les paramètres `Set-ProvScheme` après la création du catalogue de machines. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.

Augmentation des limites d'emplacement des ressources. Les limites d'emplacement des ressources pour les VDA mono-session et les VDA multi-session ont augmenté à 10 000 et 1 000 respectivement. Pour plus d'informations, consultez la section Limites.

Prise en charge du redémarrage des machines dont l'alimentation n'est pas gérée lorsque toutes les sessions ont été épuisées. Citrix DaaS vous permet désormais de créer des programmes de redémarrage pour les machines dont l'alimentation n'est pas gérée après que toutes les sessions ont été vidées des machines. Dans l'interface Configuration complète, sélectionnez **Redémarrer toutes les machines après le vidage des sessions** comme **Durée du redémarrage**. Pour plus d'informations, consultez la rubrique Créer un programme de redémarrage.

Prise en charge de la mise à niveau des machines VDA (version préliminaire) À l'aide de l'interface Configuration complète, vous pouvez désormais mettre à niveau des machines VDA pour votre déploiement Citrix DaaS. Vous pouvez les mettre à niveau par catalogue ou par machine. La fonctionnalité s'applique aux machines qui ne sont pas créées à l'aide de MCS (par exemple, les machines physiques). Pour plus d'informations, consultez Mettre à niveau les VDA à l'aide de l'interface Configuration complète.

Les machines ne sont pas arrêtées en cas de panne. Citrix DaaS empêche désormais les machines virtuelles d'être arrêtées par le broker lorsque la zone dans laquelle se trouvent les machines subit une panne. Les machines deviennent automatiquement disponibles pour les connexions à la fin de la panne. Vous n'avez aucune mesure à prendre pour rendre les machines disponibles après la panne.

Diagnostics de lancement de session. Citrix DaaS prend désormais en charge un diagnostic d'échec de lancement de session amélioré. Utilisez l'ID de transaction à 32 chiffres (8-4-4-4-12) généré par l'ap-

plication Citrix Workspace à partir de Citrix Monitor (c'est-à-dire le service Citrix Director) pour cibler le composant et l'étape exacts où le problème s'est produit et appliquez les actions recommandées pour résoudre le problème. Pour plus d'informations, consultez Diagnostics de lancement de session.

Possibilité d'accéder au service d'enregistrement de session. Une option, Enregistrement de session, est désormais disponible dans le menu de l'onglet **Gérer**. Le service d'enregistrement de session fournit une gestion centralisée des stratégies, de la lecture et des configurations de serveur. Il permet d'alléger la charge des administrateurs informatiques en fournissant un point d'entrée unifié pour gérer et observer les objets distribués dans l'ensemble de votre organisation. Pour plus d'informations, consultez Service d'enregistrement de session (version Technical Preview).

Rebranding de Citrix Virtual Apps and Desktops Service Citrix Virtual Apps and Desktops Service a été renommé **Citrix DaaS**. Pour en savoir plus sur le changement de nom, consultez l'annonce sur notre blog.

Les offres suivantes de Citrix Virtual Apps and Desktops Service ont été renommées.

- **Citrix Virtual Apps service Advanced** a été renommé **Citrix DaaS Advanced**.
- **Citrix Virtual Apps Service Premium** a été renommé **Citrix DaaS Premium**.
- **Citrix Virtual Desktops Service Premium** a été renommé **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops Service Advanced** a été renommé **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops Service Premium** est désormais disponible en tant que **Citrix DaaS Premium et Citrix DaaS Premium Plus**.
- **Citrix Virtual Apps and Desktops Standard pour Azure** a été renommé **Citrix DaaS Standard pour Azure**.
- **Citrix Virtual Apps and Desktops Standard pour Google Cloud** a été renommé **Citrix DaaS Standard pour Google Cloud**.
- **Citrix Virtual Apps and Desktops Premium pour Google Cloud** a été renommé **Citrix DaaS Premium pour Google Cloud**.

L'implémentation de cette transition dans nos produits et leur documentation est en cours. Nous vous remercions de votre patience pendant cette transition.

- L'interface utilisateur du produit, le contenu intégré au produit, ainsi que les images et les instructions de la documentation produit seront mis à jour au cours des prochaines semaines.
- Il est possible que certains éléments (tels que les commandes et les MSI) continuent à conserver leurs anciens noms pour éviter de casser les scripts clients existants.
- La documentation produit associée et les autres ressources (telles que les vidéos et les billets de blog) auxquelles la documentation de ce produit renvoie peuvent toujours contenir des noms anciens.

> **Remarque :**
>
> Le nom du produit **Citrix Virtual Apps and Desktops** local reste le même.

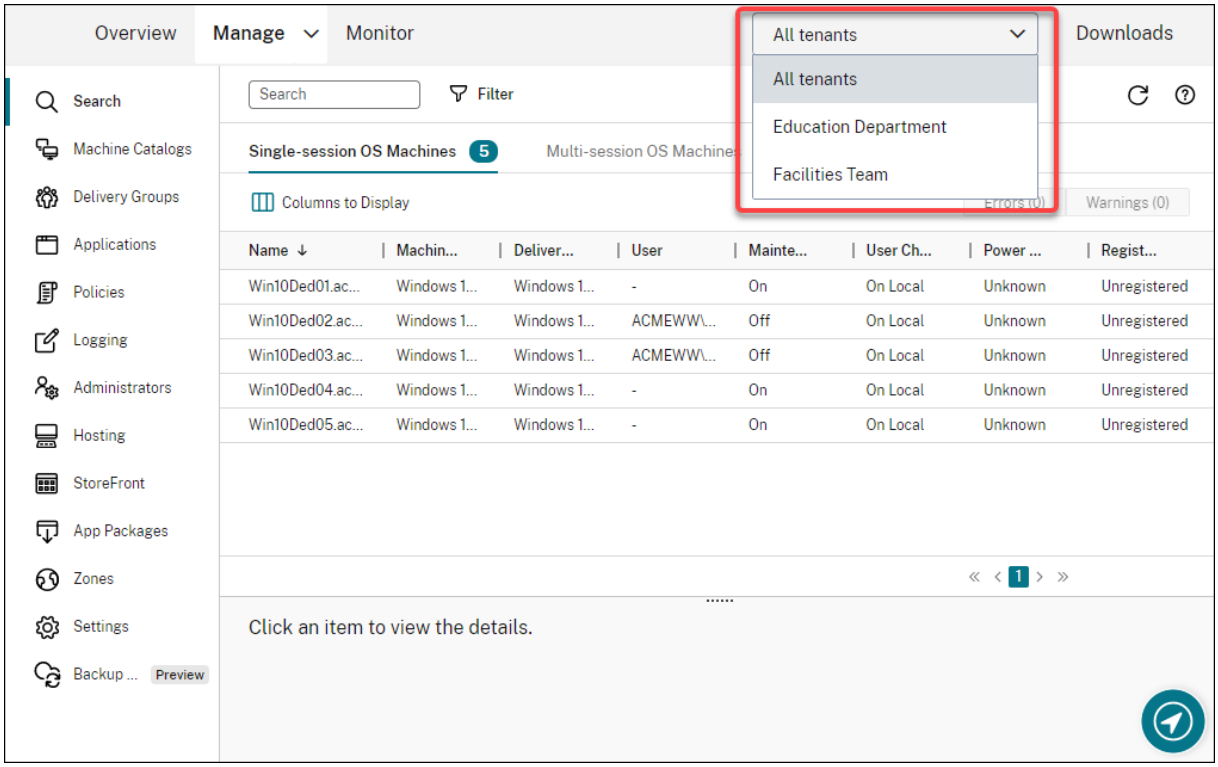
Prise en charge des locataires dans Configuration complète. Vous pouvez désormais créer des partitions de configuration au sein d'une seule instance DaaS Citrix. Pour ce faire, créez des étendues de locataire dans **Administrateurs > Étendues** et associez des objets de configuration associés, tels que des catalogues de machines et des groupes de mise à disposition, à ces locataires. Par conséquent, les administrateurs ayant accès à un client peuvent gérer uniquement les objets associés au locataire. Cette fonctionnalité est utile, par exemple, si votre organisation :

- dispose de différents silos métier (divisions indépendantes ou équipes de gestion informatique distinctes) ou
- possède plusieurs sites et souhaite conserver la même configuration dans une seule instance Citrix DaaS.

En outre, l'interface Configuration complète vous permet de filtrer les clients locataires par nom. Par défaut, l'interface affiche des informations sur tous les locataires.

La fonctionnalité est disponible pour les fournisseurs de services Citrix (CSP) et les fournisseurs non-CSP. L'interface dans un environnement CSP est essentiellement la même que celle d'un environnement non-CSP, à l'exception de la méthode utilisée pour créer des locataires.

- Les CSP intègrent les clients locataires à Citrix DaaS, puis configurent l'accès administrateur à Citrix DaaS. Pour plus d'informations, consultez Citrix DaaS pour les fournisseurs de services Citrix.
- Les fournisseurs non-CSP créent des clients locataires en créant d'abord des étendues, puis en configurant un accès personnalisé pour les administrateurs respectifs. Pour plus d'informations, consultez Créer et gérer des étendues.



Mises à jour de la fonctionnalité Autoscale. La fonctionnalité Autoscale a été mis à jour avec un style de panneau pour vous offrir une meilleure expérience utilisateur. Les workflows pour configurer vos paramètres restent les mêmes. Les autres mises à jour apportées à Autoscale incluent :

- L'option **Limiter Autoscale** a été renommée **Autoscaling des machines balisées** pour faciliter la compréhension.
- L'option **Contrôler le moment où Autoscale démarre la mise sous tension des machines balisées** a été ajoutée. L'option vous permet de contrôler le moment où Autoscale démarre la mise sous tension des machines balisées en fonction de l'utilisation de machines non balisées.

Pour plus d'informations sur l'autoscaling des machines balisées, consultez Autoscaling des machines balisées

Contrôle de validité des licences. L'interface Configuration complète vérifie désormais automatiquement la validité des licences utilisées par les connexions hôtes. Une connexion hôte est placée en mode de maintenance si sa licence n'est pas valide. Par conséquent, vous ne pouvez pas effectuer certaines opérations, telles que la modification de la connexion et la désactivation du mode de maintenance. Une licence devient caduque, par exemple lorsque :

- La licence a expiré. Dans ce cas, contactez votre représentant commercial Citrix pour la renouveler ou pour acheter de nouvelles licences.
- La licence a été supprimée du serveur de licences.

Style de panneau appliqué aux nœuds Catalogues de machines et Stratégies. Les styles de pan-

neau sont désormais appliqués à tous les nœuds dans Configuration complète

Prise en charge de la mise à jour des machines provisionnées avec MCS dans les environnements Azure. `Set-ProvScheme` modifie le modèle (schéma de provisioning) et n'affecte pas les machines existantes. À l'aide de la commande Request-ProvVMUpdate, vous pouvez désormais appliquer le schéma de provisioning actuel à une machine existante (ou à un ensemble de machines). Actuellement, la mise à jour des propriétés prise en charge par cette fonctionnalité est `ServiceOffering`. Pour plus d'informations, consultez Mettre à jour les machines provisionnées vers l'état du schéma de provisioning actuel.

Mars 2022

Fonctionnalités nouvelles et améliorées

Citrix Virtual Apps and Desktops pour Google Cloud est disponible sur Google Cloud Marketplace. Citrix Virtual Apps and Desktops Premium pour Google Cloud est désormais disponible à l'achat sur Google Cloud Marketplace. Citrix Virtual Apps and Desktops Premium pour Google Cloud exécute le plan de contrôle de Citrix Virtual Apps and Desktops Service sur Google Cloud.

Prise en charge du lancement fiable Azure. Le lancement fiable Azure est désormais disponible pour l'interface de gestion Configuration complète. Si vous choisissez de sélectionner une image pour laquelle le lancement fiable est activé, l'utilisation d'un profil de machine est obligatoire. Vous devez également sélectionner un profil de machine pour lequel le lancement fiable est activé. Pour de plus amples informations, consultez Environnements de cloud Microsoft Azure Resource Manager.

Style de panneau appliqué aux assistants dans trois nœuds supplémentaires dans Configuration complète. Les nœuds sont **Recherche**, **Groupes de mise à disposition** et **Applications**.

Le service de portabilité des images (IPS) est désormais disponible pour tous. L'IPS simplifie la gestion des images sur toutes les plates-formes. Cette fonctionnalité est utile pour gérer les images entre un emplacement de ressources sur site et le cloud public. Les API REST Citrix Virtual Apps and Desktops peuvent être utilisées pour automatiser l'administration des ressources au sein d'un site Citrix Virtual Apps and Desktops. Pour plus d'informations, consultez Migrer des charges de travail vers un cloud public.

Février 2022

Fonctionnalités nouvelles et améliorées

Autorisations Azure. Deux ensembles d'autorisations sont nécessaires pour répondre aux exigences de sécurité et pour minimiser les risques.

- Autorisations minimales : cet ensemble d'autorisations offre un meilleur contrôle de la sécurité. Toutefois, les nouvelles fonctionnalités qui nécessitent des autorisations supplémentaires échoueront si des autorisations minimales sont utilisées.
- Autorisations générales : cet ensemble d'autorisations ne vous empêche pas de profiter des nouvelles améliorations.

Pour plus d'informations, consultez À propos des autorisations Azure.

Prise en charge de l'utilisation du disque temporaire de la machine virtuelle pour héberger le disque de cache en écriture différée dans les environnements Azure. Nous avons ajouté une option, **Utiliser un disque de cache en écriture différée non persistant**, à la page **Configuration du catalogue de machines > Paramètres du disque** de l'interface **Gérer > Configuration complète**. Sélectionnez cette option si vous ne souhaitez pas que le disque de cache en écriture différée persiste pour les machines virtuelles provisionnées. Lorsque cette option est sélectionnée, nous utilisons le disque temporaire de la machine virtuelle pour héberger le disque de cache en écriture différée si le disque temporaire dispose de suffisamment d'espace. Cela réduit vos coûts. Pour de plus amples informations, consultez Environnements de cloud Microsoft Azure Resource Manager.

Mises à jour des paramètres par défaut de connexion d'hôte AWS. Les valeurs des paramètres par défaut de la connexion hôte AWS sont mises à jour vers des valeurs plus élevées et très probablement les mêmes pour toutes les configurations de plate-forme cloud AWS. Cela permet de créer des connexions hôtes dans les environnements cloud AWS, sans évaluer ni configurer les valeurs des paramètres par défaut en fonction de la configuration individuelle. Pour plus d'informations, consultez Valeurs par défaut des connexions hôtes.

Ajout de la prise en charge de différents niveaux de stockage dans les environnements GCP. Vous pouvez désormais fournir les propriétés personnalisées suivantes dans les environnements GCP pour définir le type de stockage des disques attachés à la machine virtuelle nouvellement créée :

- StorageType
- IdentityDiskStorageType
- WBCDiskStorageType

Pour plus d'informations, voir Citrix Virtual Apps and Desktops Service.

Modification de certains paramètres de machine virtuelle après la création de catalogues de machines virtuelles Azure. À l'aide de l'interface de gestion Configuration complète, vous pouvez désormais modifier les paramètres suivants après avoir créé un catalogue :

- Taille de la machine
- Zones de disponibilité
- Le profil de la machine
- Licences Windows

Pour ce faire, sur le nœud **Catalogues de machines**, sélectionnez le catalogue, puis **Modifier le catalogue de machines** dans la barre d'actions. Pour plus d'informations, consultez la section Modifier un catalogue.

Prise en charge du stockage du disque d'OS éphémère Azure sur le disque cache ou le disque temporaire. Citrix Virtual Apps and Desktops Service vous permet désormais de stocker le disque d'OS éphémère Azure sur un disque cache ou un disque temporaire pour 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 de plus amples informations, consultez Environnements de cloud Microsoft Azure Resource Manager.

Prise en charge des clusters Nutanix sur AWS. Citrix Virtual Apps and Desktops Service prend en charge les clusters Nutanix 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, consultez Clusters Nutanix sur AWS.

Prise en charge de VMware Cloud sur Amazon Web Services (AWS). VMware Cloud on Amazon Web Services (AWS) vous permet de migrer des charges de travail Citrix sur site basées sur VMware vers AWS Cloud et votre environnement principal Citrix Virtual Apps and Desktops vers Citrix Virtual Apps and Desktops Service. Pour plus d'informations, consultez Cloud VMware sur Amazon Web Services (AWS).

Prise en charge de la configuration du disque de cache en écriture différée pour les machines fonctionnant sur Google Cloud Platform (GCP). Dans l'interface de gestion Configuration complète, lorsque vous provisionnez des machines sur GCP, vous pouvez désormais configurer les paramètres de disque de cache en écriture différée suivants :

- Taille du disque
- Mémoire allouée au cache
- Type de stockage sur disque
- Persistance du disque

Pour plus d'informations, consultez Créer un catalogue de machines dans l'article Environnements de virtualisation Google Cloud Platform.

Janvier 2022

Fonctionnalités nouvelles et améliorées

Prise en charge des clusters Nutanix sur AWS. Citrix Virtual Apps and Desktops Service prend désormais en charge les clusters Nutanix sur AWS. 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 Environnements de virtualisation Nutanix.

Nouvelles fonctionnalités disponibles dans Vérification de l'état du cloud. L'outil Vérification de l'état du cloud a été mis à jour vers une nouvelle version avec des fonctionnalités telles que :

- **Correction automatique.** L'outil Vérification de l'état du cloud prend désormais en charge la détection et la résolution automatiques de certains problèmes identifiés sur les machines sur lesquelles il est en cours d'exécution. Il existe désormais un rapport de résultats pour vous montrer quelles mesures spécifiques ont été prises. Pour plus d'informations, consultez la section Correction automatique.
- **Utilisation de la ligne de commande.** La vérification de l'état du cloud peut désormais être exécutée à partir de la ligne de commande. Pour plus d'informations, consultez la section Exécution de Vérification de l'état du cloud sur la ligne de commande.
- **État du pilote CTXUVI.** La vérification de l'état du cloud affiche désormais l'état du pilote Citrix UVI et propose une vérification du journal des événements associée aux pilotes Citrix UVI.
- **Vérification du registre de lancement de session.** La vérification de l'état du cloud vérifie désormais les paramètres du registre de lancement de session.
- **Mises à jour du rapport de vérification.** Pour les éléments vérifiés qui ont plusieurs points de contrôle, le rapport de vérification final répertorie désormais toutes les vérifications qui ont été effectuées pour indiquer les actions exécutées pendant le processus.

Pour plus d'informations, consultez la section Vérification de l'état du cloud.

Dépanner les problèmes d'enregistrement et de lancement de session VDA à l'aide de l'interface Configuration complète. À l'aide de l'interface de gestion Configuration complète, vous pouvez désormais exécuter des vérifications qui évaluent l'état des VDA. Les vérifications de l'état du VDA identifient les causes possibles des problèmes courants d'enregistrement de VDA et de lancement de session. Vous pouvez effectuer des vérifications individuellement et par lots. Pour plus d'informations, consultez la section Vérifications de l'état de VDA.

Possibilité de spécifier la date d'expiration du secret Azure pour les connexions existantes. À l'aide de l'interface de gestion Configuration complète, vous pouvez désormais spécifier la date après laquelle le secret d'application expire. Pour savoir comment afficher la date d'expiration du secret, consultez Environnements de cloud Microsoft Azure Resource Manager. Lorsque vous utilisez cette fonctionnalité, tenez compte des différences suivantes :

- Pour les principaux de service créés manuellement dans Azure, vous pouvez directement modifier la date d'expiration sur la page **Modifier la connexion > Propriétés de la connexion**.
- Lorsque vous modifiez pour la première fois la date d'expiration des principaux de service créés par le biais de Configuration complète en votre nom, accédez à **Modifier la connexion > Modifier les paramètres > Utiliser existant**. Vous pouvez apporter des modifications ultérieures sur la page **Modifier la connexion > Propriétés de la connexion**.

Un bouton pour ajouter des administrateurs. Nous avons ajouté un bouton, **Ajouter un administrateur**, à l'onglet **Configuration complète > Administrateurs > Administrateurs**. Ce bouton permet d'accéder rapidement à **Gestion des identités et des accès > Administrateurs**, où vous pouvez ajouter (inviter) des administrateurs. Pour plus d'informations, consultez la section Ajouter un administrateur.

Nouvelle apparence des assistants dans Configuration complète. Nous avons modifié le style des assistants des nœuds suivants, y compris les couleurs, les polices et d'autres modifications de mise en forme, afin de vous offrir une meilleure expérience utilisateur : **Administrateurs**, **Hébergement**, **StoreFront**, **Packages d'applications**, **Zones** et **Paramètres**. Les nouveaux assistants apparaissent sous forme de panneaux avec des fenêtres d'affichage plus larges, ce qui permet d'afficher davantage de contenu. Les workflows pour configurer vos paramètres restent les mêmes.

Prise en charge de la conservation du disque système lorsque les E/S MCS sont activées pour les machines fonctionnant sur Google Cloud Platform (GCP). Dans l'interface de gestion Configuration complète, lorsque vous provisionnez des machines sur GCP, vous pouvez désormais conserver le disque système pendant les cycles d'alimentation lorsque l'optimisation du stockage MCS (E/S MCS) est activée. Pour plus d'informations, consultez Activation des mises à jour de l'optimisation du stockage MCS.

Prise en charge du chargement ou du téléchargement direct depuis EBS sur Amazon Web Services (AWS). AWS fournit désormais une API pour permettre la création directe d'un volume EBS avec le contenu souhaité. Vous pouvez désormais utiliser l'API pour ne pas avoir besoin de travailleur de volume pour la création de catalogue et l'ajout de machines virtuelles. Pour plus d'informations sur les autorisations AWS requises pour cette fonctionnalité, consultez Environnements de cloud Amazon Web Services.

Capacité à identifier les ressources Amazon Web Services (AWS) créées par MCS. Nous avons ajouté une nouvelle balise nommée `CitrixProvisioningSchemeID` pour identifier les ressources AWS créées par MCS. Pour plus d'informations, voir Identifier les ressources créées par MCS.

Possibilité de configurer l'accès à la gestion et à la surveillance. L'interface de gestion Configuration complète vous fournit désormais des options supplémentaires pour contrôler si vous souhaitez accorder aux rôles personnalisés l'accès à **Gérer** et **Surveiller**. Pour plus d'informations, consultez Créer et gérer des rôles.

Décembre 2021

Fonctionnalités nouvelles et améliorées

Prise en charge de Google Cloud VMware Engine. La plate-forme vous permet désormais de migrer les charges de travail Citrix locales basées sur VMware vers Google Cloud et votre environnement

principal Citrix Virtual Apps and Desktops vers Citrix Virtual Apps and Desktops Service. Pour plus d'informations, consultez la section Prise en charge de Google Cloud Platform (GCP) VMware Engine.

Possibilité de spécifier par quoi les noms de compte commencent lors de la spécification d'un schéma de dénomination. Cette version introduit une option sur la page **Création d'un catalogue de machines > Identités des machines** de l'interface de gestion Configuration complète. L'option vous permet de spécifier des chiffres ou des lettres par lesquels les noms de comptes commencent, ce qui vous permet de mieux contrôler la façon dont les comptes de machines sont nommés lors de la création du catalogue. Pour plus d'informations, consultez la section Identités des machines.

Prise en charge de la création de connexions Nutanix AHV XI et Nutanix AHV Prism Central (PC). Dans l'interface de gestion Configuration complète, vous pouvez désormais créer des connexions Nutanix AHV XI et Nutanix AHV PC. Pour plus d'informations, veuillez consulter Environnements de virtualisation Nutanix.

Prise en charge de la sélection du type de stockage pour les disques d'OS lors du provisioning de machines virtuelles sur GCP. Dans l'interface de gestion Configuration complète, lorsque vous provisionnez des machines virtuelles sur GCP, vous pouvez désormais sélectionner le type de stockage pour le disque d'OS. Les options de stockage disponibles sur la page **Création d'un catalogue de machines > Stockage** incluent **Disque persistant standard**, **Disque persistant équilibré** et **Disque persistant SSD**. Pour de plus amples informations, consultez l'article Créer un catalogue de machines.

L'interface de gestion Configuration complète prend désormais en charge le disque éphémère Azure. Auparavant, PowerShell était votre seul choix pour créer des machines utilisant des disques d'OS éphémères. Nous ajoutons maintenant une option, **Disque d'OS éphémère Azure**, à la page **Création d'un catalogue de machines > Types de stockage et de licence**. Sélectionnez cette option si vous souhaitez utiliser le disque local de la machine virtuelle pour héberger le disque du système d'exploitation. Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager.

Protéger les ressources gérées par Machine Creation Services (MCS) contre toute suppression accidentelle. Vous pouvez désormais protéger les ressources gérées par MCS sur Google Cloud Platform (GCP) en appliquant l'indicateur `deletionProtection` de GCP activé pour les machines virtuelles. L'autorisation `compute.instances.setDeletionProtection` ou le rôle IAM Administrateur de Compute vous permet de réinitialiser l'indicateur pour autoriser la suppression de la ressource. Cette fonctionnalité s'applique aux catalogues persistants et non persistants. Pour plus d'informations, consultez Protection contre la suppression accidentelle de machine.

Novembre 2021

Fonctionnalités nouvelles et améliorées

Annotation d'une image lors de la mise à jour des machines. Dans l'interface de gestion Configuration complète, vous pouvez désormais annoter une image en y ajoutant une note lors de la mise à jour d'un catalogue créé par MCS. Chaque fois que vous mettez à jour le catalogue, une entrée liée à la note est créée, que vous ajoutiez ou non une note. Si vous mettez à jour le 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**. Pour plus d'informations, consultez la rubrique Mettre un catalogue à jour.

Prise en charge des licences multitypes. L'interface de gestion Configuration complète prend désormais en charge les licences multitypes, vous permettant de spécifier le droit de licence que vous souhaitez que votre site (votre déploiement d'un produit de Citrix Virtual Apps and Desktops Service) ou un groupe de mise à disposition utilise.

- Au niveau du site, vous déterminez quelle licence utiliser à l'échelle du site lorsque les utilisateurs lancent une application ou un bureau sur leurs appareils. La licence sélectionnée s'applique à tous les groupes de mise à disposition, à l'exception de ceux configurés avec une licence différente.
- Au niveau du groupe de mise à disposition, vous déterminez la licence que vous souhaitez que le groupe de mise à disposition utilise, en profitant de la flexibilité et des avantages des licences multitypes.

Pour plus d'informations, consultez la section Licences multitypes.

Affichage des informations sur le plan d'achat Azure Marketplace. Dans l'interface de gestion Configuration complète, lors de la création d'un catalogue de machines, vous pouvez désormais afficher les informations de plan d'achat pour les images principales provenant d'images Azure Marketplace.

Octobre 2021

Fonctionnalités nouvelles et améliorées

Possibilité de mettre à jour les catalogues MCS persistants. Nous avons introduit l'option **Mettre à jour les machines** pour les catalogues MCS persistants dans l'interface de gestion Configuration complète. Cette option vous permet de gérer l'image ou le modèle utilisé par le catalogue. Lorsque vous mettez à jour un catalogue persistant, tenez compte des points suivants : Seules les machines que vous ajoutez au catalogue ultérieurement sont créées à l'aide de la nouvelle image ou du niveau

modèle. Nous ne déployons pas la mise à jour sur les machines existantes du catalogue. Pour plus d'informations, consultez la rubrique Mettre un catalogue à jour.

Possibilité de provisionner des machines virtuelles sur un hôte dédié Azure. Nous avons ajouté une option, **Utiliser un groupe d'hôtes**, à la page **Création d'un catalogue de machines > Image principale** de l'interface de gestion Configuration complète. Cette option vous permet de spécifier le groupe d'hôtes que vous souhaitez utiliser lors du provisioning de machines virtuelles dans des environnements Azure. Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager.

Améliorer les performances en préservant une machine virtuelle provisionnée lors d'un cycle d'alimentation. Nous avons ajouté un paramètre, **Conserver les VM durant les cycles d'alimentation**, à la page **Création d'un catalogue de machines > Paramètres de disque** de l'interface de gestion Configuration complète. Ce paramètre vous permet de conserver une machine virtuelle provisionnée lors d'un cycle d'alimentation dans des environnements Azure. Pour plus d'informations, consultez la section Optimisation du stockage MCS. Vous pouvez également configurer la fonctionnalité à l'aide de PowerShell. Pour plus d'informations, consultez la section Conservation d'une machine virtuelle provisionnée lors des cycles d'alimentation.

Lier un catalogue de machines à un jeu de configuration Workspace Environment Management. Lorsque vous créez un catalogue de machines, vous pouvez désormais le lier à un jeu de configuration Workspace Environment Management. Cela vous permet d'utiliser Workspace Environment Management Service pour offrir la meilleure expérience d'espace de travail possible à vos utilisateurs. Vous pouvez également choisir de lier le catalogue après avoir créé le catalogue. Pour plus d'informations, consultez les sections Créer des catalogues de machines et Gérer les catalogues de machines.

Septembre 2021

Fonctionnalités nouvelles et améliorées

Ajout de description informative pour les mises à jour d'images. Vous pouvez désormais ajouter des descriptions informatives sur les modifications liées aux mises à jour des images pour les catalogues de machines. Cette fonctionnalité est utile pour les administrateurs qui souhaitent ajouter des étiquettes descriptives lors de la mise à jour d'une image utilisée par un catalogue, par exemple, *Office 365 installé*. À l'aide des commandes PowerShell, vous pouvez créer et afficher ces messages. Pour plus d'informations, consultez la section Ajout de descriptions à une image.

Intégration de la solution Azure VMware (AVS). Citrix Virtual Apps and Desktops Service prend en charge AVS, la solution Azure VMware. AVS fournit une infrastructure cloud contenant des clusters vSphere créés par Azure. Tirez parti de Citrix Virtual Apps and Desktops Service pour utiliser AVS pour provisionner votre charge de travail VDA de la même manière que vous utiliseriez vSphere dans des environnements locaux. Pour plus d'informations, consultez Intégration de la solution Azure VMware.

Même groupe de ressources pour plusieurs catalogues. Vous pouvez désormais utiliser le même groupe de ressources pour mettre à jour et créer des catalogues dans Citrix Virtual Apps and Desktops Service. Ce processus :

- s'applique à tout groupe de ressources contenant un ou plusieurs catalogues de machines ;
- prend en charge les groupes de ressources qui ne sont pas créés par Machine Creation Services ;
- crée la machine virtuelle et les ressources associées ;
- supprime les ressources du groupe de ressources lorsque la machine virtuelle ou le catalogue est supprimé.

Pour plus d'informations, consultez la rubrique Groupes de ressources Azure.

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, un disque de système d'exploitation, un instantané et une définition d'image de 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. Pour plus d'informations, consultez Récupérer des informations sur les machines virtuelles Azure, les instantanés, le disque du système d'exploitation et la définition d'image de la galerie.

Nouvelle mise à jour pour la configuration automatisée. La configuration automatisée a été mise à jour vers une nouvelle version avec des fonctionnalités telles que :

- Prise en charge de Machines Creation Services (MCS) - La configuration automatisée prend désormais en charge les catalogues MCS. Pour plus d'informations, consultez la rubrique Présentation de la migration des catalogues provisionnés Machine Creation Services.

Autres mises à jour de la configuration automatisée :

- Prise en charge améliorée des zones en préremplissant le fichier ZoneMapping.yml avec les noms des zones locales pendant l'exportation et les emplacements de ressources cloud lors de la sauvegarde.
- StoreFront est devenu un composant gérable au niveau supérieur. Avant cela, StoreFront était géré dans le cadre de groupes de mise à disposition. Cette séparation facilite la fusion des sites.
- `AddMachinesOnly` est devenu `MergeMachines` pour correspondre au modèle des options de fusion actuelles et nouvelles.
- Ajout de l'utilisation du fichier SecurityClient.csv pour importer l'ID client et le secret lors de la création et de la mise à jour du fichier CustomerInfo.yml lors de l'utilisation des applets de commande de support.
- Ajout de la migration des préférences de zone utilisateur.
- Correction de la prise en charge du plan de contrôle japonais.
- Autres correctifs et améliorations.

Téléchargez l'outil de configuration automatisée sur Téléchargements Citrix. Pour plus d'informations sur la configuration automatisée, consultez la section Migrer une configuration vers Citrix Cloud.

Plus d'options de planification sont disponibles avec les programmes de redémarrage. L'interface de gestion Configuration complète vous offre désormais des options supplémentaires pour contrôler le moment où les redémarrages planifiés se produisent. En plus des programmes de redémarrage récurrents quotidiens, vous pouvez désormais définir des modèles de récurrence hebdomadaires et mensuels. Pour plus d'informations, consultez la rubrique Créer un programme de redémarrage.

Préservez les colonnes personnalisées qui dégradent les performances. Auparavant, dans le nœud **Recherche** de l'interface de gestion Configuration complète, les colonnes personnalisées qui dégradaient les performances disparaissaient après actualisation de la fenêtre du navigateur ou déconnexion/reconnexion à la console. Vous pouvez désormais définir si ces colonnes personnalisées doivent être conservées. Pour plus d'informations, voir Utiliser la recherche dans l'interface de gestion Configuration complète.

Utilisez l'outil de configuration automatisée pour effectuer une sauvegarde et une restauration. Nous avons ajouté un nœud, **Sauvegarde et restauration**, à l'interface de gestion Configuration complète. Ce nœud regroupe toutes les ressources liées à l'outil de configuration automatisée, y compris les informations sur :

- Planification des sauvegardes automatisées de votre configuration Citrix Virtual Apps and Desktops à l'aide d'une seule commande
- Restauration à partir d'une sauvegarde précédente si nécessaire
- Sauvegardes et restaurations granulaires
- Autres cas d'utilisation pris en charge

Pour plus d'informations, consultez la documentation relative à la configuration automatisée .

Prise en charge des catalogues non joints à un domaine. Nous avons ajouté un type d'identité, **Non joint au domaine**, à la page **Création d'un catalogue de machines > Identités des machines** de l'interface de gestion Configuration complète. Avec ce type d'identité, vous pouvez utiliser MCS pour créer des machines qui ne sont associées à aucun domaine. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.

Prise en charge de l'utilisation d'un profil de machine. Nous avons ajouté une option, **Utiliser un profil de machine**, à la page **Création d'un catalogue de machines > Image principale** de l'interface de gestion Configuration complète. L'option vous permet de spécifier le profil de machine dont vous souhaitez que les machines virtuelles héritent des configurations lors de la création de machines virtuelles dans des environnements Azure. Les machines virtuelles du catalogue peuvent alors hériter des configurations du profil de machine sélectionné. Voici des exemples de configurations :

- 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

Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager.

Prise en charge de Windows Server 2022. Nécessite un VDA 2106 au minimum.

Août 2021

Fonctionnalités nouvelles et améliorées

Étendre le nombre d'éléments triables de 500 à 5 000. Sur le nœud **Recherche** de l'interface de gestion Configuration complète, vous pouvez désormais trier jusqu'à 5 000 éléments selon n'importe quel en-tête de colonne. Lorsque le nombre d'éléments dépasse 5 000, utilisez des filtres pour réduire le nombre d'éléments à 5 000 ou moins afin de faciliter le tri. Pour plus d'informations, voir Utiliser la recherche dans l'interface de gestion Configuration complète.

Prise en charge de types de stockage Azure supplémentaires. Vous pouvez désormais sélectionner différents types de stockage pour les machines virtuelles dans des environnements Azure utilisant MCS. Pour plus d'informations, consultez la section Types de stockage.

Prise en charge de la sélection du type de stockage pour les disques de cache en écriture différée. Dans l'interface de gestion Configuration complète, lorsque vous créez un catalogue MCS, vous pouvez désormais sélectionner le type de stockage pour le disque de cache en écriture différée. Les types de stockage disponibles incluent : SSD Premium, SSD standard et HDD standard. Pour de plus amples informations, consultez l'article Créer des catalogues de machines.

Arrêter les machines suspendues. Dans l'interface **Gérer > Configuration complète**, nous avons ajouté une option, **Quand aucune reconnexion après (minutes)**, à la page **Paramètres basés sur la charge** de l'interface utilisateur Gérer Autoscale pour les groupes de mise à disposition OS mono-session. L'option devient disponible lorsque vous avez sélectionné **Suspendre**, ce qui vous permet de spécifier quand arrêter les machines suspendues. Les machines suspendues restent disponibles pour les utilisateurs déconnectés lorsqu'ils se reconnectent, mais ne sont pas disponibles pour les nouveaux utilisateurs. Lorsqu'elles sont arrêtées, les machines deviennent à nouveau disponibles pour gérer toutes les charges de travail. Pour plus d'informations, consultez la section Autoscale.

Prise en charge étendue de l'utilisation de fichiers CSV pour ajouter en vrac des machines à un catalogue. Dans l'interface **Gérer > Configuration complète**, vous pouvez désormais utiliser un fichier CSV pour ajouter en vrac des machines déjà présentes dans votre centre de données à un catalogue où l'alimentation de ces machines est gérée. Pour plus d'informations, consultez les sections Créer des catalogues de machines et Gérer les catalogues de machines.

Juillet 2021

Fonctionnalités nouvelles et améliorées

Journalisation de la configuration. L'interface utilisateur **Journalisation** a été modifiée dans **Gérer > Configuration complète**. Les trois onglets suivants constituent l'interface :

- **Événements** (anciennement journalisation de la configuration). Cet onglet vous permet de suivre les modifications de configuration et les activités administratives.
- **Tâches**. Cet onglet vous permet d'afficher les tâches liées aux opérations de catalogue de machines.
- **API**. Cet onglet vous permet d'afficher les demandes d'API REST effectuées pendant une certaine période.

Pour plus d'informations, consultez la section Journalisation de la configuration.

Autoscale vous offre désormais des options de délai d'expiration de session dynamique. Vous pouvez 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. Pour plus d'informations, consultez la section Délai d'expiration de session dynamique.

Prise en charge des clés de chiffrement gérées par le client (CMEK) Google Cloud Platform (GCP). Vous pouvez désormais utiliser les CMEK de Google avec les catalogues MCS. Les clés CMEK offrent un meilleur contrôle sur les clés utilisées pour chiffrer les données d'un projet Google Cloud. Pour plus d'informations, consultez la section Clés de chiffrement gérées par le client (CMEK). Pour configurer cette fonctionnalité, consultez Utilisation de clés de chiffrement gérées par le client (CMEK). Cette fonctionnalité est disponible sur la page **Création d'un catalogue de machines > Paramètres du disque** de l'interface **Gérer > Configuration complète**.

> **Remarque :**
>
> Cette fonctionnalité est disponible en tant que version préliminaire.

Mises à jour de l'onglet Gérer. Nous avons mis à jour les options dans le menu de l'onglet **Gérer** :

- **Configuration complète** : auparavant, cette option vous dirigeait vers l'ancienne console. Elle vous amène maintenant à la nouvelle console Web (Web Studio). La console Web présente une parfaite parité avec l'ancienne console et comprend plusieurs améliorations. Nous vous recommandons de commencer à l'utiliser maintenant.
- **Ancienne configuration** : Cette option vous amène à l'ancienne console, dont la suppression est prévue en septembre 2021. Après cela, **Configuration complète** sera la seule interface qui offre un accès à toute la gamme d'actions de configuration et de gestion.

Web Studio vous permet désormais de choisir une connexion de gestion de l'alimentation pour un catalogue Remote PC Access. Auparavant, vous pouviez utiliser Studio pour créer une connexion

hôte Wake on LAN à votre emplacement de ressources (en sélectionnant **Remote PC Wake on LAN** comme type de connexion). Cependant, PowerShell était votre seul choix pour associer cette connexion à un catalogue Remote PC Access. Vous pouvez désormais utiliser Studio pour le faire. Pour plus d'informations, consultez Configurer Wake on LAN dans l'interface Configuration complète.

Juin 2021

Fonctionnalités nouvelles et améliorées

Accédez aux images d'Azure Shared Image Gallery. Lorsque vous créez un catalogue de machines, vous pouvez désormais accéder aux images d'Azure Shared Image Gallery sur l'écran Image principale. Pour plus d'informations, consultez Accéder aux images d'Azure Shared Image Gallery.

Prise en charge des machines virtuelles protégées sur Google Cloud Platform (GCP). 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, consultez VM protégées.

Appliquer HTTPS ou HTTP. Utilisez les paramètres du Registre pour forcer le trafic HTTPS ou HTTP via le service XML.

Utilisez toujours un SSD standard pour un disque d'identité afin de réduire les coûts dans les environnements Azure. Les catalogues de machines utilisent le type de stockage SSD standard pour les disques d'identité. Les disques SSD standard Azure sont une option de stockage économique optimisée pour les charges de travail nécessitant des performances constantes à des niveaux d'E/S par seconde inférieurs. Pour plus d'informations sur les types de stockage, consultez Image principale Azure Resource Manager.

> **Remarque :**
>
> Pour plus d'informations sur la tarification des disques gérés Azure, consultez Tarification Disques managés.

Nouvelle fonctionnalité disponible dans Web Studio. Les fonctionnalités suivantes sont désormais disponibles dans la console Web :

- **Studio prend désormais en charge l'authentification auprès d'Azure pour créer un principal de service**. Vous pouvez désormais établir une connexion hôte à Azure en vous authentifiant auprès d'Azure pour créer un principal de service. Cette prise en charge élimine la nécessité de créer manuellement un principal de service dans votre abonnement Azure avant de créer une connexion dans Studio. Pour de plus amples informations, consultez Environnements de virtualisation Microsoft Azure Resource Manager.

- **Studio prend désormais en charge le clonage de catalogues de machines existants**. Cette fonctionnalité vous permet de cloner un catalogue de machines existant pour l'utiliser comme modèle pour un nouveau catalogue, éliminant ainsi la nécessité de créer un catalogue similaire à partir de zéro. Lorsque vous clonez un catalogue, 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. Pour plus d'informations, consultez la rubrique Cloner un catalogue.
- **Un nouveau nœud appelé Paramètres est désormais disponible dans le volet de navigation Studio**. Le nœud **Paramètres** vous permet de configurer les paramètres qui s'appliquent à l'ensemble du site (votre déploiement d'un produit Citrix Virtual Apps and Desktops Service). Les paramètres suivants sont disponibles :
  - **Catalogues multi-sessions d'équilibrage de charge**. Sélectionnez l'option d'équilibrage de charge qui répond à vos besoins. Ce paramètre s'applique à tous vos catalogues. Auparavant, vous accédiez à cette fonctionnalité en cliquant sur l'icône en forme d'engrenage dans le coin supérieur droit de la console. Pour plus d'informations, consultez la section Équilibrer la charge des machines.
- **Expérience de recherche améliorée dans Studio**. Cette version améliore votre expérience de recherche Studio. Lorsque vous utilisez des filtres pour effectuer une recherche avancée, la fenêtre Ajouter des filtres apparaît au premier plan, laissant la vue d'arrière-plan inchangée. Pour plus d'informations, voir Utiliser la recherche dans l'interface de gestion Configuration complète.
- **Possibilité de suspendre et de réactiver les VM Google Cloud dans MCS**. Vous pouvez désormais suspendre et réactiver les VM Google Cloud dans MCS comme n'importe quelle machine virtuelle. Pour de plus amples informations, consultez la section Gérer des groupes d'applications. Pour activer cette fonctionnalité, définissez les autorisations `compute.instances.suspend` et `compute.instances.resume` dans le compte de service Google Cloud. Le rôle Compute Admin est fourni avec ces autorisations.

  Dans Citrix Virtual Apps and Desktops, vous pouvez également utiliser la commande PowerShell `New-BrokerHostingPowerAction` pour suspendre et réactiver les VM. Pour plus de détails, voir New-Brokerhostingpoweraction.

  Google Cloud impose certaines limitations quant au type et à la configuration des instances pouvant être suspendues. Pour plus d'informations, reportez-vous à la Suspendre et réactiver une instance sur le site Google Cloud.

May 2021

Fonctionnalités nouvelles et améliorées

Reconnexion de session après déconnexion d'une machine en mode de maintenance. Auparavant, lorsque des utilisateurs de bureaux monosession (VDI) regroupés (aléatoires) étaient déconnectés d'une machine en mode de maintenance, la reconnexion de session n'était autorisée à aucune machine du groupe. Les machines multisession et monosession statiques autorisaient toujours la reconnexion à la session dans ce cas de figure.

Désormais, à l'aide de PowerShell, vous pouvez contrôler au niveau du groupe de mise à disposition si la reconnexion de session est autorisée après une déconnexion sur une machine en mode de maintenance. Cela s'applique à tous les VDA du groupe (monosession et multisession).

Pour plus d'informations consultez Contrôler la reconnexion de session en cas de déconnexion d'une machine en mode de maintenance.

Prise en charge de la recherche d'applications et de bureaux dans toutes les éditions de Citrix Virtual Apps and Desktops Service. En plus de la prise en charge existante de l'édition **Premium**, la recherche d'applications et de bureaux est désormais disponible dans les éditions **Citrix Virtual Apps Advanced Service** et **Citrix Virtual Apps and Desktops Advanced Service**.

Nouvelle fonctionnalité disponible dans Web Studio. La fonctionnalité suivante est désormais disponible dans la console Web :

- **Studio prend désormais en charge la sélection des zones de disponibilité Azure**. Auparavant, PowerShell était votre seule option pour provisionner des machines dans une zone de disponibilité spécifique dans des environnements Azure. Lorsque vous utilisez Studio pour créer un catalogue de machines, vous pouvez désormais sélectionner une ou plusieurs zones de disponibilité dans lesquelles vous souhaitez provisionner des machines. Si aucune zone n'est spécifiée, Machine Creation Services (MCS) laisse Azure de placer les machines dans la région. Si plusieurs zones sont spécifiées, MCS distribue les machines de manière aléatoire dans ces zones. Pour plus d'informations, consultez Provisionner des machines dans des zones de disponibilité spécifiées.

Disque éphémère Azure. Citrix Virtual Apps and Desktops Service prend en charge le disque éphémère Azure. Un disque éphémère vous permet de réutiliser le disque cache 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.

> **Remarque :**
>
> Les catalogues persistants ne prennent pas en charge les disques d'OS éphémères. En outre, lorsque vous utilisez cette fonctionnalité, tenez compte du fait que le disque extra performant

> entraîne un coût supplémentaire. Il est avantageux de réutiliser le disque cache pour stocker le disque d'OS au lieu de payer pour un disque géré supplémentaire.

Les disques d'OS éphémères nécessitent que votre schéma de provisioning utilise des disques gérés et une galerie d'images partagées. Pour plus d'informations, consultez Disques éphémères Azure.

Amélioration des performances pour les VDA gérés par MCS sur Azure. Citrix Virtual Apps and Desktops Service améliore les performances des VDA gérés avec Machine Creation Services (MCS) sur Azure. Cette amélioration modifie les valeurs par défaut pour *Actions simultanées absolues* pour la connexion d'hébergement à 500 et *Nouvelles actions maximales par minute* pour la connexion d'hébergement à 2 000. Aucune tâche de configuration manuelle n'est requise pour profiter de cette amélioration. Pour plus d'informations, consultez la section Limitation des demandes Azure.

Nouvelles fonctionnalités disponibles dans Vérification de l'état du cloud. L'outil Vérification de l'état du cloud a été mis à jour vers une nouvelle version avec des fonctionnalités telles que :

- **Découverte automatique des machines VDA**. L'outil Vérification de l'état du cloud peut désormais détecter et récupérer automatiquement des VDA à partir de vos déploiements de Citrix Virtual Apps and Desktops Service. Pour plus d'informations, consultez la section Récupérer des machines VDA.
- **Planification des vérifications de l'état**. L'outil Vérification de l'état du cloud vous permet désormais de configurer des planifications pour effectuer des vérifications périodiques de l'état. Pour plus d'informations, consultez la section Planificateur Vérification de l'état du cloud.
- **Informations de version de la vérification de l'état du cloud.** Vous pouvez maintenant vérifier quelle version de Vérification de l'état du cloud vous utilisez. Pour afficher les informations de version, cliquez sur l'icône en forme d'engrenage dans le coin supérieur droit de la fenêtre principale Vérification de l'état du cloud.
- **Correction automatique**. L'outil Vérification de l'état du cloud prend désormais en charge la détection et la résolution automatiques de certains problèmes identifiés sur les machines sur lesquelles il est en cours d'exécution. Pour plus d'informations, consultez la section Correction automatique.

  > **Remarque :**
  >
  > La correction automatique est disponible sous forme d'aperçu.

Avril 2021

Fonctionnalités nouvelles et améliorées

Récupérer les instances dynamiques à l'aide de l'API AWS. Le service Citrix Virtual Apps and Desktops interroge désormais AWS pour récupérer les types d'instance dynamiquement. Cette

fonctionnalité élimine le besoin de créer un fichier `InstanceTypes.xml` personnalisé pour les clients souhaitant utiliser des tailles de machine au-delà de celles définies dans le service Citrix Virtual Apps and Desktops. Cette information a déjà été fournie par le fichier `InstanceTypes.xml`. Pour faciliter cet accès dynamique aux types d'instance AWS disponibles, les utilisateurs doivent mettre à jour les autorisations sur leurs entités de service pour inclure les autorisations `ec2:DescribeInstanceTypes`. Pour prendre en charge la rétrocompatibilité pour les clients qui choisissent de ne pas mettre à jour leurs autorisations d'entités de service, les types d'instance AWS répertoriés dans `InstanceTypes.xml` sont utilisés. Ce processus génère un message d'avertissement dans le journal CDF MCS.

> **Remarque :**
>
> Citrix Studio n'affiche pas le message d'avertissement contenu dans le journal CDF.

Pour plus d'informations sur les autorisations, consultez Définition des autorisations IAM et À propos des autorisations AWS.

Nouvelle fonctionnalité disponible dans Web Studio. La fonctionnalité suivante est désormais disponible dans la console Web :

- **Studio affiche désormais la date et l'heure de votre fuseau horaire**. Auparavant, Studio affichait uniquement la date et l'heure en fonction de l'horloge système et du fuseau horaire. Studio prend désormais en charge l'affichage de la date et de l'heure locale dans votre fuseau horaire lorsque vous placez le pointeur de la souris sur un événement. L'heure est exprimée en UTC.

Prise en charge des E/S MCS pour les machines virtuelles Azure sans stockage temporaire. Les E/S MCS prennent désormais en charge la création de catalogue de machines pour les machines virtuelles qui ne disposent pas de disques temporaires ou de stockage connecté. Avec cette prise en charge :

- L'instantané (disque géré) est récupéré depuis la machine virtuelle source *sans* stockage temporaire. Les machines virtuelles du catalogue de machines ne disposent pas de stockage temporaire.
- L'instantané (disque géré) est récupéré depuis la machine virtuelle source *avec* stockage temporaire. Les machines virtuelles du catalogue de machines disposent d'un stockage temporaire.

Pour plus d'informations, voir Optimisation du stockage MCS (Machine Creation Services).

Nouvelle fonctionnalité disponible dans Web Studio. La fonctionnalité suivante est désormais disponible dans la console Web :

- **Forcer la déconnexion**. Autoscale vous permet désormais de fermer de force la session existante sur les machines lorsque la période de grâce établie expire, ce qui rend la machine éligible à l'arrêt. Cela permet à Autoscale d'éteindre les machines beaucoup plus rapidement,

réduisant ainsi les coûts. Vous pouvez envoyer des notifications aux utilisateurs avant qu'ils ne soient déconnectés. Pour plus d'informations, consultez la section Autoscale.

Nouvelle mise à jour pour la configuration automatisée. La configuration automatisée a été mise à jour vers une nouvelle version avec des fonctionnalités telles que :

- **Fusion de plusieurs sites** : vous pouvez fusionner plusieurs sites en un seul site tout en évitant les collisions de noms à l'aide de préfixes et de suffixes. Pour plus d'informations, reportez-vous à la rubrique Fusion de plusieurs sites en un seul site.
- **Activation du site** : vous pouvez choisir si votre déploiement local ou cloud contrôle les ressources telles que les planifications de redémarrage et les schémas d'alimentation. Pour plus d'informations, consultez Activation de sites.

Autres mises à jour de la configuration automatisée :

- Possibilité de migrer les rôles et les étendues administrateur.
- Paramètre `Quiet` pour sélectionner les applets de commande permettant de supprimer la journalisation de la console.
- Paramètre `SecurityFileFolder` permettant de placer le fichier CvadAcSecurity.yml dans un partage de fichiers réseau sécurisé qui nécessite une authentification.
- Possibilité de filtrer par nom de machine dans les catalogues de machines et les groupes de mise à disposition.
- Améliorations des paramètres de sélection des composants pour utiliser la méthode de paramètre commutateur, éliminant ainsi la nécessité d'ajouter `$true` après le nom du composant.
- Nouvelle applet de commande (`New-CvadAcZipInfoForSupport`) permettant de compresser tous vos fichiers journaux à envoyer à Citrix pour obtenir une assistance.

Téléchargez l'outil de configuration automatisée sur Téléchargements Citrix. Pour plus d'informations sur la configuration automatisée, consultez la section Migration vers le cloud.

Préserver les instances GCP sur l'ensemble des cycles d'alimentation. Les instances Google Cloud Platform (GCP) non persistantes ne sont plus supprimées lors de la mise hors tension. Au lieu de cela, les instances sont préservées sur l'ensemble des cycles d'alimentation. Lorsqu'une instance non persistante est mise hors tension, le disque du système d'exploitation est détaché et supprimé. Lorsque l'instance est sous tension, le disque du système d'exploitation est recréé à partir du disque de base et attaché à l'instance existante.

Prise en charge des images Azure Gen2. Vous pouvez désormais provisionner un catalogue de machines virtuelles Gen2 à l'aide d'un instantané Gen2 ou d'un disque géré Gen2 pour améliorer les

performances de démarrage. Pour de plus amples informations, consultez l'article Créer des catalogues de machines. Les systèmes d'exploitation suivants sont pris en charge pour les images Azure Gen2 :

- Windows Server 2019, 2016, 2012 et 2012 R2
- Windows 10

> **Remarque :**
>
> La création d'un catalogue de machines Gen2 à l'aide d'un instantané Gen1, ou d'un disque géré, n'est pas prise en charge. De même, la création d'un catalogue de machines Gen1 à l'aide d'un instantané Gen2, ou d'un disque géré, n'est pas non plus prise en charge. Pour plus d'informations, consultez la section Prise en charge des machines virtuelles Gen2 sur Azure.

Désactivation des comptes de stockage de table. Machine Creation Services (MCS) ne crée plus de comptes de stockage de table pour les catalogues qui utilisent des disques gérés lors du provisioning des VDA sur Azure. Pour plus d'informations, consultez la section Stockage de table Azure.

Élimination des verrous des comptes de stockage. Lors de la création d'un catalogue dans Azure à l'aide d'un disque géré, un compte de stockage n'est plus créé. Les comptes de stockage créés pour les catalogues existants restent inchangés. Cette modification s'applique uniquement aux disques gérés. Pour les disques non gérés, le comportement existant ne change pas. Machine Creation Services (MCS) continue de créer des comptes de stockage et des verrous.

Nouvelles fonctionnalités disponibles dans Web Studio. Les fonctionnalités suivantes sont désormais disponibles dans la console Web :

- **Utiliser une clé de chiffrement gérée par le client pour chiffrer les données sur les machines**. Studio ajoute désormais un paramètre appelé **Clé de chiffrement gérée par le client** à la page **Création d'un catalogue de machines > Paramètres du disque**. Ce paramètre vous permet de choisir de chiffrer les données sur les machines à provisionner dans le catalogue. Pour plus d'informations, consultez la section Clés de chiffrement gérées par le client.
- **Studio prend désormais en charge la restriction d'Autoscale aux machines balisées**. Auparavant, vous deviez utiliser PowerShell pour restreindre Autoscale à certaines machines d'un groupe de mise à disposition. Vous pouvez maintenant également utiliser Studio. Pour plus d'informations, consultez Restreindre Autoscale à certaines machines dans un groupe de mise à disposition.

March 2021

Fonctionnalités nouvelles et améliorées

Hôtes dédiés Azure. Les hôtes dédiés Azure vous permettent de provisionner des machines virtuelles sur du matériel dédié à un seul client. Lors de l'utilisation d'un hôte dédié, Azure garantit que vos machines virtuelles sont les seules machines exécutées sur cet hôte. Cela donne plus de contrôle et de visibilité aux clients et leur garantit qu'elles respectent leurs exigences réglementaires ou internes en matière de sécurité. Un groupe d'hôtes Azure préconfiguré, dans la région de l'unité d'hébergement, est requis lors de l'utilisation du paramètre `HostGroupId`. En outre, le placement automatique Azure est requis. Pour plus d'informations, consultez la section Hôtes dédiés Azure.

> **Conseil :**
>
> Lorsque vous utilisez des hôtes dédiés Azure, la sélection de la **zone de disponibilité Azure** n'a aucun effet. La machine virtuelle est placée par le processus de placement automatique Azure.

Prise en charge du chiffrement Azure côté serveur. Citrix Virtual Apps and Desktops Service prend en charge les clés de chiffrement gérées par le client pour les disques gérés Azure. 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 Azure côté serveur.

Provisionnez des machines dans des zones de disponibilité spécifiées sur Azure. Vous pouvez désormais provisionner des machines dans une zone de disponibilité spécifique dans les environnements Azure. Avec cette fonctionnalité :

- Vous pouvez spécifier une ou plusieurs zones de disponibilité sur Azure. Les machines sont nominalement réparties de manière égale dans toutes les zones fournies si plus d'une zone est fournie.
- La machine virtuelle et le disque correspondant sont placés dans la (ou les zones) spécifiées.
- Vous pouvez parcourir les zones de disponibilité pour une offre de service ou une région donnée. Les zones de disponibilité valides sont affichées à l'aide des commandes PowerShell. Affichez les éléments d'inventaire de l'offre de service à l'aide de `Get-Item`.

Pour plus d'informations, consultez Provisionner des machines dans des zones de disponibilité spécifiées sur Azure.

Nouvelles fonctionnalités disponibles dans Web Studio. Les fonctionnalités suivantes sont désormais disponibles dans la console Web :

- **Studio prend désormais en charge l'association d'applications avec des icônes personnalisées**. Auparavant, vous deviez utiliser PowerShell pour ajouter des icônes personnalisées à

utiliser avec des applications publiées. Vous pouvez maintenant utiliser Studio pour cela. Pour de plus amples informations, consultez l'article Gérer des groupes d'applications.

- **Studio prend désormais en charge l'application de balises aux catalogues de machines**. Auparavant, vous pouviez utiliser Studio pour créer ou supprimer des balises à utiliser avec un catalogue. Toutefois, vous deviez utiliser PowerShell pour appliquer les balises au catalogue. Vous pouvez désormais utiliser Studio pour appliquer ou supprimer une balise à un catalogue ou à partir d'un catalogue, comme vous le faites avec les groupes de mise à disposition. Pour plus d'informations, consultez la rubrique Appliquer des balises aux catalogues de machines.
- **Studio prend désormais en charge le basculement entre les modes « équilibrage de charge horizontal » et « équilibrage de charge vertical »**. Auparavant, PowerShell était votre seul choix pour basculer entre les modes d'équilibrage de charge horizontal et vertical. Studio vous offre désormais plus de flexibilité pour équilibrer la charge des machines avec OS multi-session. Pour plus d'informations, consultez la section Équilibrer la charge des machines.
- **Studio prend désormais en charge l'inclusion des machines en mode maintenance dans les programmes de redémarrage**. Auparavant, PowerShell était votre seul choix pour configurer les redémarrages programmés pour les machines en mode maintenance. Vous pouvez désormais utiliser Studio pour contrôler si ces machines doivent être inclues dans un programme de redémarrage. Pour plus d'informations, consultez la rubrique Créer un programme de redémarrage.
- **Studio prend désormais en charge la configuration de Wake on LAN pour Remote PC Access**. Auparavant, vous deviez utiliser PowerShell pour configurer Wake on LAN pour Remote PC Access. Vous pouvez désormais utiliser Studio pour configurer cette fonctionnalité. Pour plus d'informations, consultez la section Configurer Wake on LAN.
- **Studio prend désormais en charge l'application des propriétés d'instance AWS et le balisage des ressources opérationnelles**. Lorsque vous créez un catalogue pour provisionner des machines dans AWS à l'aide de MCS, vous pouvez indiquer si le rôle IAM et les propriétés de balise doivent être appliqués à ces machines. Vous pouvez également indiquer si vous souhaitez appliquer des balises de machine aux ressources opérationnelles. Vous disposez des deux options suivantes :

  - **Appliquer les propriétés du modèle de machine aux machines virtuelles**
  - **Appliquer balises de machine aux ressources opérationnelles**

  Pour plus d'informations, consultez Application des propriétés d'instance AWS et balisage des ressources opérationnelles.

Azure Shared Image Gallery. Citrix Virtual Apps and Desktops Service prend en charge Azure Shared Image Gallery en tant que référentiel d'images publiées pour les machines provisionnées avec MCS dans Azure. Les administrateurs ont la possibilité de stocker une image dans la galerie pour accélérer

la création et l'hydratation des disques du système d'exploitation. Ce processus améliore les temps de démarrage et de lancement des applications pour les machines virtuelles non persistantes. Pour plus d'informations sur cette fonctionnalité, consultez la rubrique Azure Shared Image Gallery.

> **Remarque :**
>
> La fonctionnalité Shared Image Gallery est compatible avec les disques gérés. Elle n'est pas disponible pour les anciens catalogues de machines.

Compartiments de stockage créés dans la même région Google Cloud Platform que le catalogue de machines. Dans les versions précédentes, MCS créait des compartiments de stockage temporaires pendant le provisioning dans le cadre du processus de chargement sur disque. Ces compartiments couvrent plusieurs régions, que Google définit comme une grande zone géographique contenant deux emplacements géographiques ou plus. Ces compartiments temporaires résidaient dans l'emplacement géographique États-Unis, indépendamment de l'endroit où le catalogue était provisionné. MCS crée désormais des compartiments de stockage dans la région où vous provisionnez vos catalogues. Les compartiments de stockage ne sont plus temporaires ; ils restent dans votre projet Google Cloud Platform une fois que vous avez terminé le processus de provisioning. Les futures opérations de provisioning utiliseront le compartiment de stockage existant, s'il en existe un dans cette région. Un nouveau compartiment de stockage est créé s'il n'en existe pas dans la région spécifiée.

Février 2021

Fonctionnalités nouvelles et améliorées

Prise en charge des images Azure Gen2. Vous pouvez désormais provisionner des disques gérés à l'aide des machines virtuelles Gen2 dans des environnements Azure pour améliorer les performances de démarrage. Les systèmes d'exploitation suivants sont pris en charge :

- Windows Server 2019, 2016, 2012 et 2012 R2
- Windows 10

> **Remarque :**
>
> Seul un sous-ensemble de machines virtuelles est pris en charge. Par exemple, certaines machines virtuelles peuvent être des types Gen1 et Gen2, tandis que d'autres machines virtuelles ne peuvent être que Gen1. Pour plus d'informations, consultez la section Prise en charge des machines virtuelles Gen2 sur Azure.

Programmes de redémarrage de la machine. Citrix Studio ajoute désormais une option appelée **Redémarrer toutes les machines après le vidage des sessions** dans le menu **Durée du redémarrage**. Cette option vous permet de choisir de redémarrer toutes les machines 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. Pour plus d'informations, consultez la rubrique Créer un programme de redémarrage.

Nouvelles fonctionnalités disponibles dans Web Studio. Les fonctionnalités suivantes sont désormais disponibles dans la console Web :

- **Studio prend désormais en charge l'utilisation de fichiers CSV pour ajouter en vrac des machines à un catalogue**. Cette fonctionnalité vous permet d'utiliser un fichier CSV pour :
  - Ajouter en vrac des machines à un catalogue de systèmes d'exploitation multi-session ou mono-session où les machines ne sont pas gérées via Studio.
  - Ajouter en vrac des machines à un catalogue Remote PC Access. Auparavant, vous deviez choisir des unités d'organisation pour ajouter en vrac des machines à un catalogue Remote PC Access. Toutefois, cette solution n'est pas facile dans les scénarios avec des restrictions de structure d'unité d'organisation. Cette fonctionnalité vous donne plus de flexibilité pour ajouter des machines en vrac. Vous pouvez ajouter uniquement des machines (à utiliser avec des attributions utilisateur automatiques) ou ajouter des machines avec attributions utilisateur.

  Pour plus d'informations, consultez les sections Créer des catalogues de machines et Gérer les catalogues de machines.
- **Prise en charge étendue de Azure géré par Citrix.** Azure géré par Citrix est désormais disponible dans les éditions de service Citrix Virtual Apps and Desktops suivantes : Standard pour Azure, Advanced, Premium et Workspace Premium Plus.
- **Prise en charge du placement d'images principales dans Shared Image Gallery d'Azure**. Studio vous offre désormais la possibilité de placer des images principales dans Shared Image Gallery d'Azure (SIG). SIG est un référentiel pour la gestion et le partage d'images. Il vous permet de mettre vos images à disposition de l'ensemble de votre organisation. Nous vous recommandons de stocker une image principale 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. Pour de plus amples informations, consultez Environnements de virtualisation Microsoft Azure Resource Manager.
- **Conserver le disque système pour les catalogues de machines MCS dans Azure**. Studio vous permet désormais d'indiquer si vous souhaitez conserver les disques système pour les VDA pendant les cycles d'alimentation. Normalement, le disque système est supprimé à l'arrêt et recréé au démarrage. Cela garantit que le disque est toujours dans un état propre, mais entraîne des temps de redémarrage de la machine virtuelle plus longs. Si les écritures système sont redirigées vers le cache et réécrites sur le disque cache, le disque système reste inchangé. Pour éviter la recréation inutile du disque, utilisez l'option **Conserver le disque système pendant les cycles d'alimentation**, disponible sur la page **Création d'un catalogue de machines**

> Paramètres du disque. L'activation de cette option réduit les temps de redémarrage des machines virtuelles mais augmente vos coûts de stockage. Cette option peut être utile dans les scénarios où un environnement contient des charges de travail avec des temps de redémarrage sensibles. Pour plus d'informations, consultez la section Optimisation du stockage MCS.

- **Studio prend désormais en charge la création de catalogues de machines MCS avec disque de cache en écriture différée persistant**. Auparavant, PowerShell était votre seul choix pour créer un catalogue avec disque de cache en écriture différée persistant. Vous pouvez désormais utiliser Studio pour indiquer si le disque de cache en écriture persiste pour les machines virtuelles provisionnées dans Azure lorsque vous créez un catalogue. Si cette option est désactivée, le disque de cache en écriture est supprimé au cours de chaque cycle d'alimentation afin de réduire les coûts de stockage, ce qui entraîne la perte de toutes les données redirigées vers le disque. Pour conserver les données, activez l'option **Utiliser disque de cache en écriture différée persistant**, disponible sur la page **Création d'un catalogue de machines > Paramètres du disque**. Pour plus d'informations, consultez la section Optimisation du stockage MCS.

Prise en charge de la protection des applications pour Citrix Virtual Apps and Desktops Service avec StoreFront. Pour plus d'informations, consultez la section Protection des applications.

Janvier 2021

Nouvelles fonctionnalités disponibles dans Web Studio. Les fonctionnalités suivantes sont désormais disponibles dans la console Web :

- **Studio prend désormais en charge l'association d'applications avec des icônes personnalisées**. Auparavant, vous deviez utiliser PowerShell pour ajouter des icônes personnalisées à utiliser avec des applications publiées. Vous pouvez maintenant utiliser Studio pour cela. Pour de plus amples informations, consultez l'article Gérer des groupes d'applications.
- **Studio prend désormais en charge l'application de balises aux catalogues de machines**. Auparavant, vous pouviez utiliser Studio pour créer ou supprimer des balises à utiliser avec un catalogue. Toutefois, vous deviez utiliser PowerShell pour appliquer les balises au catalogue. Vous pouvez désormais utiliser Studio pour appliquer ou supprimer une balise à un catalogue ou à partir d'un catalogue, comme vous le faites avec les groupes de mise à disposition. Pour plus d'informations, consultez la rubrique Appliquer des balises aux catalogues de machines.
- **Studio prend désormais en charge le basculement entre les modes « équilibrage de charge horizontal » et « équilibrage de charge vertical »**. Auparavant, PowerShell était votre seul choix pour basculer entre les modes d'équilibrage de charge horizontal et vertical. Studio vous offre désormais plus de flexibilité pour équilibrer la charge des machines avec OS multi-session. Pour plus d'informations, consultez la section Équilibrer la charge des machines.

- **Studio prend désormais en charge l'inclusion des machines en mode maintenance dans les programmes de redémarrage**. Auparavant, PowerShell était votre seul choix pour configurer les redémarrages programmés pour les machines en mode maintenance. Vous pouvez désormais utiliser Studio pour contrôler si ces machines doivent être inclues dans un programme de redémarrage. Pour plus d'informations, consultez la rubrique Créer un programme de redémarrage.
- **Studio prend désormais en charge la configuration de Wake on LAN pour Remote PC Access**. Auparavant, vous deviez utiliser PowerShell pour configurer Wake on LAN pour Remote PC Access. Vous pouvez désormais utiliser Studio pour configurer cette fonctionnalité. Pour plus d'informations, consultez la section Configurer Wake on LAN.
- **Studio prend désormais en charge l'application des propriétés d'instance AWS et le balisage des ressources opérationnelles**. Lorsque vous créez un catalogue pour provisionner des machines dans AWS à l'aide de MCS, vous pouvez indiquer si le rôle IAM et les propriétés de balise doivent être appliqués à ces machines. Vous pouvez également indiquer si vous souhaitez appliquer des balises de machine aux ressources opérationnelles. Vous disposez des deux options suivantes :

  - **Appliquer les propriétés du modèle de machine aux machines virtuelles**
  - **Appliquer balises de machine aux ressources opérationnelles**

  Pour plus d'informations, consultez Application des propriétés d'instance AWS et balisage des ressources opérationnelles.
- **Hôte dédié AWS**. Citrix Studio propose désormais une option appelée **Utiliser un hôte dédié** sur la page **Création d'un catalogue de machines > Sécurité**. Ce paramètre convient aux déploiements avec des restrictions de licence ou exigences de sécurité qui nécessitent d'utiliser un hôte dédié. Avec un hôte dédié, vous possédez la totalité d'un hôte physique et vous êtes facturé sur une base horaire. Posséder cet hôte vous permet de faire tourner autant d'instances EC2 que cet hôte le permet, sans frais supplémentaires. Pour plus d'informations, consultez la section Location AWS.
- **Studio prend désormais en charge l'exécution immédiate d'un programme de redémarrage**. Studio vous permet désormais d'exécuter immédiatement un programme de redémarrage pour redémarrer toutes les machines applicables de ce programme. Pour plus d'informations, consultez Exécuter immédiatement un programme de redémarrage.
- **Autoscale.** Autoscale fournit les nouvelles fonctionnalités et améliorations suivantes :

  - **Studio prend désormais en charge l'affichage des machines à l'état de drainage**. Auparavant, PowerShell était votre seul choix pour identifier les machines en état de drainage. Vous pouvez désormais utiliser Studio pour identifier les machines qui sont en état de drainage. Pour plus d'informations, voir Afficher les machines en état de drainage.

- **Studio prend désormais en charge la définition d'heures de pointe à un niveau granulaire de 30 minutes pour les groupes de mise à disposition VDI**. Auparavant, vous deviez utiliser PowerShell pour 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 VDI. Vous pouvez maintenant utiliser Studio pour cela. Vous pouvez définir le nombre minimum de machines exécutées dans un groupe de mise à disposition VDI séparément pour chaque demi-heure de la journée.

Azure Shared Image Gallery. Citrix Virtual Apps and Desktops Service prend en charge Azure Shared Image Gallery en tant que référentiel d'images publiées pour les machines provisionnées avec MCS dans Azure. Les administrateurs ont la possibilité de stocker une image dans la galerie pour accélérer la création et l'hydratation des disques du système d'exploitation à partir de l'image principale. Ce processus améliore les temps de démarrage et de lancement des applications pour les machines virtuelles non persistantes.

La galerie 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 principale. MCS crée une définition d'image pour chaque image principale 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 principale. Le service Citrix Virtual Apps and Desktops crée toujours une version d'image Standard_LRS (version 1.0.0) pour chaque image avec le nombre approprié de réplicas dans la région du catalogue. Cette configuration est basée sur le nombre de machines dans le catalogue, le ratio de réplica configuré et le nombre maximal de réplicas configuré.

> **Remarque :**
>
> La fonctionnalité Shared Image Gallery ne fonctionne qu'avec les disques gérés. Elle n'est pas disponible pour les anciens catalogues de machines.

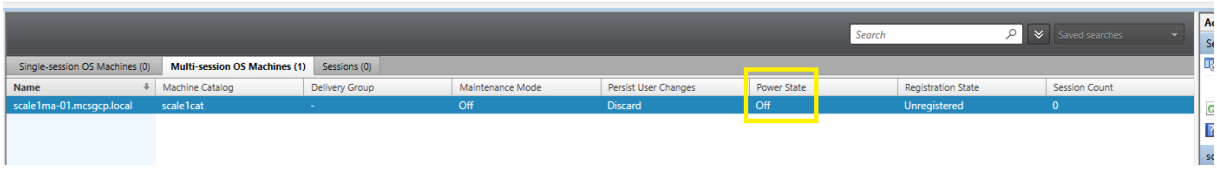
Pour plus d'informations sur cette fonctionnalité, consultez Configurer Azure Shared Image Gallery.

Compartiments de stockage créés dans la même région Google Cloud Platform que le catalogue de machines. Dans les versions précédentes, MCS créait des compartiments de stockage temporaires pendant le provisioning dans le cadre du processus de chargement sur disque. Ces compartiments couvrent plusieurs régions, que Google définit comme une grande zone géographique contenant deux emplacements géographiques ou plus. Ces compartiments temporaires résidaient dans l'emplacement géographique États-Unis, indépendamment de l'endroit où le catalogue était provisionné. MCS crée désormais des compartiments de stockage dans la région où vous provisionnez vos catalogues.

Les compartiments de stockage ne sont plus temporaires ; ils restent dans votre projet Google Cloud Platform une fois que vous avez terminé le processus de provisioning. Les futures opérations de provisioning utiliseront le compartiment de stockage existant. S'il en existe un dans cette région ou un nouveau compartiment de stockage est créé s'il n'en existe pas dans la région spécifiée.

Option PowerShell qui définit par défaut la réutilisation des VDA regroupés pendant une panne. Une nouvelle option de commande PowerShell (`-DefaultReuseMachinesWithoutShutdownInOutage`) étend la possibilité de réutiliser les VDA de bureau regroupés qui n'ont pas été arrêtés pendant une panne, par défaut. Voir Prise en charge des applications et des bureaux.

Provisioning à la demande Google Cloud Platform. Le service Citrix Virtual Apps and Desktops met à jour la façon dont Google Cloud Platform (GCP) fournit des catalogues de machines. Lors de la création d'un catalogue de machines, l'instance de machine correspondante n'est pas créée dans GCP et l'état d'alimentation est défini sur **Désactivé**. Les machines ne sont pas provisionnées au moment de la création du catalogue, mais plutôt lors de la première mise sous tension des machines. Par exemple, après la création d'un catalogue, l'état d'alimentation de la machine virtuelle est défini sur **Désactivé** :

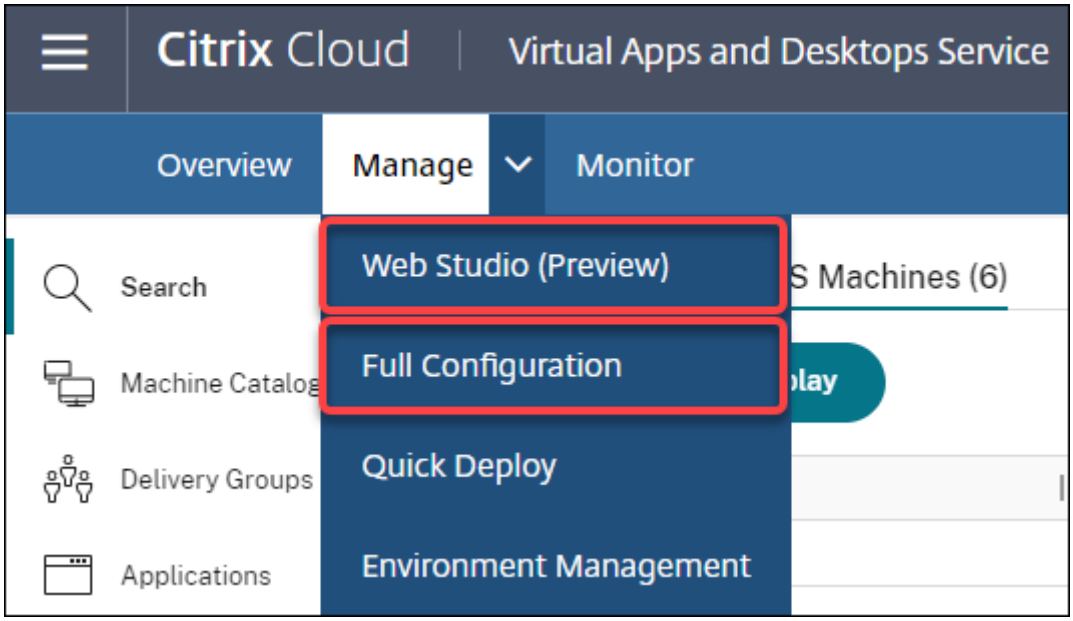


Décembre 2020

Fonctionnalités nouvelles et améliorées

Web Studio est disponible en version préliminaire. Une nouvelle console Web est maintenant disponible. Nous sommes en train de migrer l'ensemble complet des fonctionnalités Studio de l'ancienne console vers la nouvelle console Web. La console Web répond généralement plus rapidement que l'ancienne console. Par défaut, vous vous connectez automatiquement à la console Web. Vous pouvez facilement basculer entre la console Web et l'ancienne console depuis l'onglet **Gérer** pour effectuer vos tâches de configuration ou de gestion du site. Cliquez sur la flèche vers le bas en regard de **Gérer** et sélectionnez une option :

- **Web Studio (Aperçu)**. Vous dirige vers la nouvelle console Web.
- **Configuration complète**. Vous dirige vers l'ancienne console.



Les fonctionnalités suivantes sont disponibles uniquement dans la console Web :

- **Prise en charge du type de disque SSD standard pour Azure**. Studio prend désormais en charge le type de disque SSD standard. Les disques SSD standard Azure sont une option de stockage économique optimisée pour les charges de travail nécessitant des performances constantes à des niveaux d'E/S par seconde inférieurs. Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'une image principale Azure Resource Manager.
- **Studio prend désormais en charge la configuration du délai de mise hors tension pour les groupes de mise à disposition VDI statiques**. Auparavant, vous pouviez configurer le délai de mise hors tension pour les groupes de mise à disposition VDI statiques uniquement via le SDK PowerShell. Studio vous permet désormais de configurer le délai de mise hors tension dans l'interface utilisateur Autoscale pour les groupes de mise à disposition VDI statiques. Pour plus d'informations, consultez la section Autoscale.

Octobre 2020

Fonctionnalités nouvelles et améliorées

Rejeter plusieurs alertes d'hyperviseur. Citrix Monitor prend désormais en charge le rejet automatique des alertes d'hyperviseur de plus d'un jour. Pour plus d'informations, consultez la section Surveillance des alertes d'hyperviseur.

Supprimer l'adresse IP externe. Une adresse IP externe sur une machine virtuelle temporaire utilisée pour préparer une image provisionnée dans Google Cloud Platform (GCP) n'est plus requise. Cette adresse IP externe permet à la machine virtuelle temporaire d'accéder à l'API publique Google pour terminer le processus de provisioning.

Activez l'accès privé à Google pour permettre à la machine virtuelle d'accéder à l'API publique Google directement à partir du sous-réseau. Pour plus d'informations, consultez la rubrique Activer l'accès privé à Google.

Le nouveau modèle traite de la façon dont les identités de machine sont gérées. Les identités de machine utilisées dans les catalogues de machines ont été gérées à l'aide d'Active Directory. Toutes les machines créées par MCS rejoindront désormais Active Directory. Le nouveau modèle de service Citrix Virtual Apps and Desktops gère la façon dont les identités de machine sont gérées. Ce modèle permet la création de catalogues de machines à l'aide de *groupes de travail* ou de machines n'appartenant pas au domaine.

> **Conseil :**
>
> Cette fonctionnalité prend en charge un nouveau service d'identité, l'*approbation FMA*, ajouté à Citrix Cloud pour les machines n'appartenant pas au domaine.

MCS communique avec le nouveau service d'approbation FMA pour la gestion des identités. Les informations d'identité sont stockées dans le disque d'identité sous la forme de paire de GUID et de paires de clés privées, au lieu du paradigme de mot de passe de domaine SID et de compte d'ordinateur utilisé par Active Directory. Les VDA utilisant des machines n'appartenant pas au domaine utilisent cette combinaison GUID et clé privée pour l'enregistrement de broker. Pour plus d'informations, consultez la rubrique Configurer la prise en charge des catalogues n'appartenant pas au domaine.

Utilisez le téléchargement direct pour les disques gérés Azure. Cette version vous permet d'utiliser le téléchargement direct lors de la création de disques gérés dans un environnement Azure. Cette fonctionnalité réduit les coûts associés aux comptes de stockage supplémentaires. Vous n'avez plus besoin de transformer le disque dur virtuel en compte de stockage avant de le convertir en disque géré. En outre, le téléchargement direct élimine la nécessité d'attacher un disque géré vide à une machine virtuelle. Le téléchargement direct sur un disque géré Azure simplifie le workflow en vous permettant de copier directement un disque dur virtuel local pour l'utiliser en tant que disque géré. Les disques gérés pris en charge comprennent le disque dur standard, le disque SSD standard et le disque SSD Premium.

Pour plus d'informations sur cette fonctionnalité, consultez le blog Microsoft Azure.

Pour plus d'informations sur les disques gérés Azure, consultez la page de documentation.

Groupe de ressources unique dans Azure. Vous pouvez désormais créer et utiliser un seul groupe de ressources Azure pour mettre à jour et créer des catalogues dans Citrix Virtual Apps and Desktops. Cette amélioration s'applique à la fois aux principaux de services à étendue complète et à étendue limitée.
La limite précédente de 240 machines virtuelles/800 disques gérés par groupe de ressources Azure a été supprimée. Le nombre de machines virtuelles, de disques gérés, d'instantanés et d'images par groupe de ressources Azure n'est plus limité.

Pour de plus amples informations, consultez Environnements de virtualisation Microsoft Azure Resource Manager.

Septembre 2020

Fonctionnalités nouvelles et améliorées

Déploiement rapide. La nouvelle fonctionnalité Déploiement rapide remplace l'ancienne fonctionnalité Déploiement rapide d'Azure. La nouvelle fonctionnalité offre un moyen rapide de commencer à utiliser le service Citrix Virtual Apps and Desktops à l'aide de Microsoft Azure. Vous pouvez utiliser Déploiement rapide pour fournir des bureaux et des applications et configurer Remote PC Access.

Session Administrator (rôle intégré). Citrix Studio ajoute désormais un nouveau rôle intégré appelé **Session Administrator**. Ce rôle permet à un administrateur d'afficher les groupes de mise à disposition et de gérer leurs sessions et machines associées sur la page **Filtres** de l'onglet **Surveiller**. Avec cette fonctionnalité, vous pouvez configurer les autorisations d'accès des administrateurs existants ou des administrateurs que vous invitez en fonction de leur rôle dans votre organisation. Pour plus d'informations sur le rôle intégré, consultez la section Étendues et rôles intégrés. Pour plus d'informations sur l'attribution du rôle intégré à un administrateur, reportez-vous à la section Administration déléguée et surveillance.

Pour un niveau de contrôle plus précis sur l'accès à la page **Filtres** liée aux sessions et aux machines, créez un rôle personnalisé et sélectionnez l'une des options suivantes pour l'objet Director : **page Afficher les filtres - Machines uniquement**, **page Afficher les filtres - Sessions uniquement**. Pour plus d'informations sur la création d'un rôle personnalisé, reportez-vous à la section Créer et gérer les rôles.

Prise en charge d'un nouveau type de machine. Cette version ajoute la prise en charge de la série NV v4 et DA v4 de machines AMD, lors de la configuration des disques Premium pour un catalogue de machines. Pour plus d'informations, consultez la section Créer des groupes de mise à disposition.

Août 2020

Fonctionnalités nouvelles et améliorées

Accès limité au SDK Remote PowerShell en cas de panne. Auparavant, vous ne pouviez pas utiliser les commandes PowerShell lors d'une panne. Désormais, le cache d'hôte local permet un accès limité au SDK Remote PowerShell lors d'une panne. Voir Fonctionnalités indisponibles durant une panne.

Prise en charge de deux nouvelles éditions de service Citrix Virtual Apps and Desktops. Citrix Monitor prend désormais en charge deux nouvelles éditions de service Citrix Virtual Apps and Desktops, à savoir **Citrix Virtual Apps Advanced Service** et **Citrix Virtual Apps and Desktops Advanced**

Service. Pour de plus amples informations, consultez le Tableau de compatibilité des fonctionnalités de Citrix Monitor.

Prise en charge des VPC partagés dans Google Cloud Platform. Le service Citrix Virtual Apps and Desktops prend en charge les VPC partagés sur Google Cloud Platform en tant que ressource hôte. Vous pouvez utiliser Machine Creation Services (MCS) pour provisionner des machines dans un VPC partagé et les gérer à l'aide de Citrix Studio. Pour plus d'informations sur Shared VPC, consultez Cloud privé virtuel partagé.

Prise en charge de la sélection de zones pour Google Cloud Platform. Le service Citrix Virtual Apps and Desktops prend en charge la sélection de zones sur Google Cloud Platform. Cette fonctionnalité permet aux administrateurs de spécifier une ou plusieurs zones au sein d'une région pour créer un catalogue.

Pour les machines virtuelles de type locataire unique, la sélection de zone permet aux administrateurs de placer des nœuds locataires uniques sur les zones de leur choix. Pour les machines virtuelles qui ne sont pas de type locataire unique, la sélection de zone leur permet de placer des machines virtuelles de manière déterministe dans les zones de leur choix, offrant ainsi une flexibilité dans la conception du déploiement. Pour plus d'informations sur la configuration, voir Activer la sélection de zone.

Considérez également les points suivants :

- La location unique offre un accès exclusif à un nœud locataire unique, qui est un serveur Compute Engine physique dédié à l'hébergement exclusif des machines virtuelles de votre projet. Ces nœuds vous permettent de regrouper vos machines virtuelles sur le même matériel ou de les séparer des machines virtuelles d'autres projets.
- Les nœuds à locataire unique peuvent vous aider à répondre aux exigences de matériel dédié pour les scénarios Bring Your Own License (BYOL). Ils vous permettent également de respecter la stratégie de contrôle d'accès réseau, les exigences de sécurité et de confidentialité telles que HIPAA.

> **Remarque :**
>
> La location unique est le seul moyen d'utiliser les déploiements VDI de Windows 10 sur Google Cloud. Server VDI prend également en charge cette méthode. Vous trouverez une description détaillée de la location unique sur le site de documentation Google.

Amélioration des performances de démarrage pour les disques système Azure. Cette version prend en charge l'amélioration des performances de démarrage pour les implémentations Citrix Cloud à l'aide d'Azure lorsque MCSIO est activé. Avec cette prise en charge, vous pouvez conserver le disque système. Cela offre les avantages suivants :

- Les machines virtuelles et les applications démarrent maintenant avec des performances similaires à l'image principale.

- Réduction de la consommation de quotas d'API, des suppressions/créations du disque système, et du délai de transition d'état causé lors de la suppression d'une machine virtuelle.

Par exemple, utilisez la propriété personnalisée `PersistOSDisk` PowerShell dans la commande `New-ProvScheme` pour configurer cette fonctionnalité.

```
-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>'
<!--NeedCopy-->
```

Pour plus d'informations sur la configuration, consultez la section Améliorer les performances de démarrage.

Juillet 2020

Fonctionnalités nouvelles et améliorées

Prise en charge de l'accès granulaire basé sur les rôles à la page Filtres. Citrix Studio offre désormais un contrôle plus précis sur l'accès à la page **Surveiller > Filtres** lorsque vous créez un rôle personnalisé. En particulier, vous pouvez affecter des autorisations pour afficher n'importe quelle combinaison de **machines**, de **sessions**, de **connexions** et **d'instances d'application** à un rôle personnalisé. Nous avons ajouté quatre options pour l'objet **Director** dans la fenêtre **Créer un rôle** :

- Page Afficher les filtres - Instances d'application uniquement
- Page Afficher les filtres - Connexions uniquement
- Page Afficher les filtres - Machines uniquement
- Page Afficher les filtres - Sessions uniquement

Pour plus d'informations sur la création de rôles, consultez la section Créer et gérer des rôles.

Prise en charge du délai de mise hors tension pour les machines VDI attribuées (PowerShell uniquement). Dans les versions antérieures, le délai de mise hors tension s'appliquait uniquement aux machines non attribuées. À partir de cette version, le délai de mise hors tension s'applique aux machines attribuées et non attribuées. Pour plus d'informations, consultez la section Comment Autoscale gère les machines.

Prise en charge des licences Windows Client. Le service Citrix Virtual Apps and Desktops prend désormais en charge l'utilisation de licences Client Windows pour provisionner des machines virtuelles dans Azure. Pour exécuter les machines virtuelles Windows 10 dans Azure, vérifiez que votre contrat de licence en volume avec Microsoft est admissible à cette utilisation. Pour plus d'informations, consultez Créer un catalogue de machines à l'aide d'une image principale Azure Resource Manager.

Mai 2020

Fonctionnalités nouvelles et améliorées

Planifications du redémarrage de la machine. Vous pouvez maintenant indiquer si une planification de redémarrage affecte les machines en mode de maintenance. Cette fonctionnalité est disponible uniquement dans PowerShell. Pour plus d'informations, consultez la section Redémarrages planifiés des machines en mode de maintenance.

Disponibilité des ressources. Vous pouvez désormais garantir la disponibilité des ressources pendant une panne sans avoir à publier des ressources dans chaque zone (emplacement des ressources). Pour plus d'informations, consultez la section Disponibilité des ressources.

Avril 2020

Fonctionnalités nouvelles et améliorées

Granularité de la planification améliorée pour les groupes de mise à disposition VDI (PowerShell uniquement). Autoscale prend désormais en charge la définition des heures de pointe pour les jours inclus dans un calendrier à un niveau granulaire de 30 minutes. Vous pouvez définir le nombre minimum de machines exécutées dans un groupe de mise à disposition VDI séparément pour chaque demi-heure de la journée. De plus, Autoscale peut désormais augmenter ou réduire le nombre de machines sous tension dans les groupes de mise à disposition VDI sur une base demi-heure plutôt que sur une base horaire. Pour plus d'informations, consultez la section Commandes SDK PowerShell de Broker.

Découverte MTU. Le protocole Citrix Enlightened Data Transport (EDT) dispose désormais de fonctionnalités de découverte MTU. La découverte MTU permet à EDT de déterminer et de définir automatiquement la taille de la charge utile pour la session. Cette fonctionnalité permet à la session ICA de s'adapter aux réseaux ayant des besoins non standard en unité de transmission maximale (MTU) ou en taille maximale de segment (MSS). La possibilité d'ajustement évite la fragmentation des paquets qui pourrait entraîner une dégradation des performances ou l'échec de l'établissement d'une session ICA. Cette mise à jour nécessite au minimum l'application Citrix Workspace 1911 pour Windows. Si vous utilisez Citrix Gateway, la version minimale du firmware Citrix ADC requise est 13.0.52.24 ou 12.1.56.22. Pour plus d'informations, consultez la section Découverte MTU EDT.

Mars 2020

Fonctionnalités nouvelles et améliorées

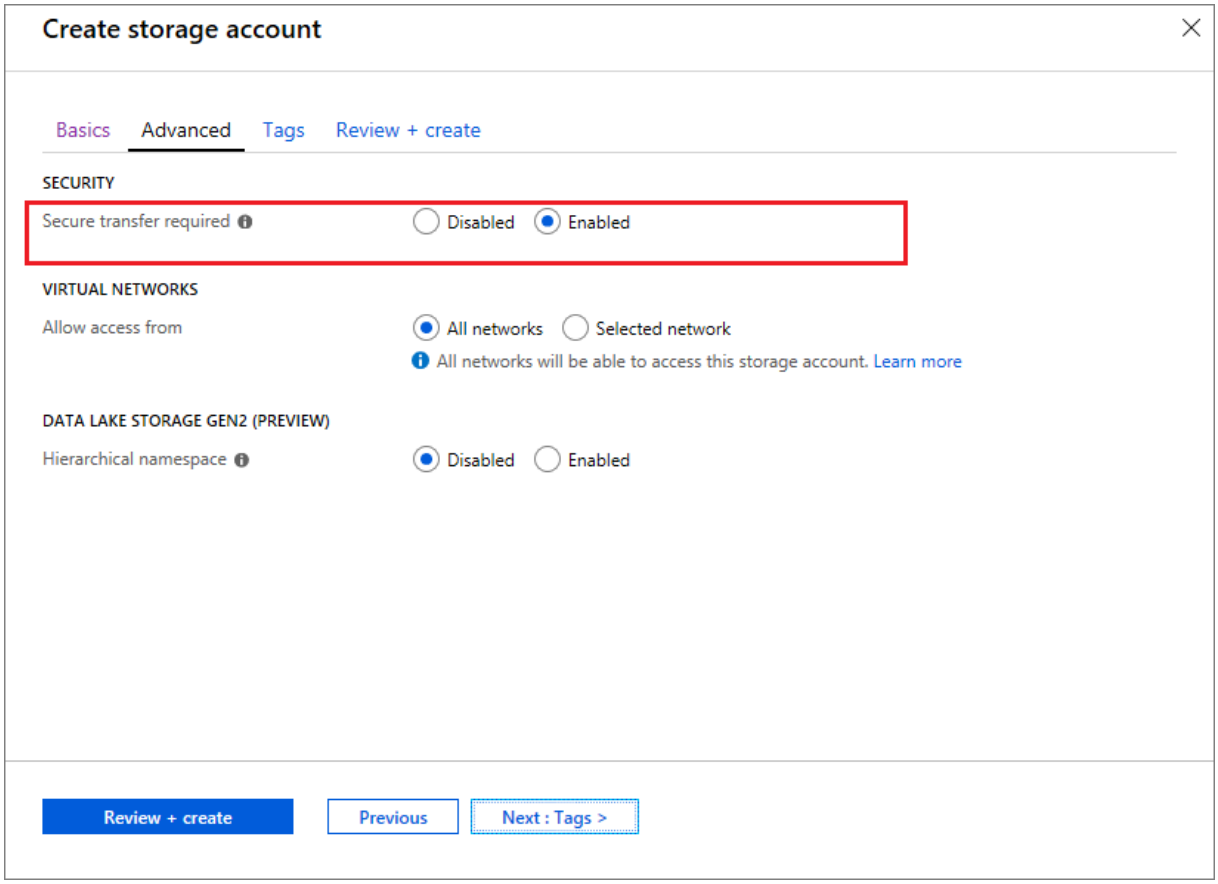
Mesures des machines cibles PVS. Citrix Monitor fournit désormais un panneau de mesures des machines cibles PVS sur la page Détails de la machine. Utilisez le panneau pour afficher l'état des machines cibles du provisioning pour les machines avec système d'exploitation mono-session et multi-session. Plusieurs mesures sont disponibles sur ce panneau : Réseau, Démarrage et Cache. Ces mesures vous aident à surveiller et à dépanner les machines cibles PVS pour vous assurer qu'elles sont opérationnelles. Pour plus d'informations, consultez la section Mesures de la machine cible PVS.

Capture des propriétés d'instance AWS. MCS lit désormais les propriétés de l'instance à partir de laquelle l'AMI a été prise et applique le rôle IAM 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. Pour plus d'informations, consultez la section Capture des propriétés d'instance AWS.

Balisage des ressources opérationnelles AWS. Cette version introduit une option permettant de baliser les ressources créées par les composants Citrix lors du provisioning. Chaque balise représente une étiquette composée d'une clé définie par le client et d'une valeur facultative qui améliore votre capacité à gérer, rechercher et filtrer les ressources. Pour plus d'informations, consultez la section Balisage des ressources opérationnelles AWS.

Transfert sécurisé dans le stockage Azure. Machine Creation Services (MCS) propose une amélioration pour les comptes de stockage créés par les catalogues provisionnés par MCS dans les environnements Azure Resource Manager. Cette amélioration active automatiquement la propriété requise pour un transfert sécurisé. Cette option améliore la sécurité du compte de stockage en autorisant uniquement les requêtes vers le compte à partir de connexions sécurisées. Pour plus d'informations, consultez Exiger un transfert sécurisé pour assurer la sécurité des connexions sur le site Microsoft.

Activez la propriété requise pour un **transfert sécurisé** lors de la création d'un compte de stockage dans Azure :



Prise en charge des disques gérés SSD Azure. Machine Creation Services (MCS) prend en charge les disques gérés SSD standard pour les machines virtuelles Azure. Ce type de disque offre des performances cohérentes et offre une meilleure disponibilité par rapport aux disques durs. Pour plus d'informations, consultez Disques SSD standard pour les charges de travail des machines virtuelles Azure.

Utilisez la propriété personnalisée `StorageAccountType` PowerShell dans la commande `New-ProvScheme` ou la commande `Set-ProvScheme` pour configurer cette fonctionnalité :

```
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"StandardSSD_LRS`" /><Property xsi:type=`"StringProperty`" Value=`"Windows_Server`" />
<!--NeedCopy-->
```

> **Remarque :**
>
> Cette fonctionnalité n'est disponible que lors de l'utilisation de disques gérés, c'est-à-dire lorsque la propriété personnalisée `UseManagedDisks` est définie sur **true**. Pour les disques non gérés, seuls le HDD standard et le SSD Premium sont pris en charge.

Janvier 2020

Fonctionnalités nouvelles et améliorées

Barre de langue dans Citrix Studio. À compter de cette version, Citrix Studio fournit une barre de langue pour faciliter le mappage correct du clavier.

- Si la langue de Citrix Cloud ou la langue d'affichage de votre navigateur est définie sur **Anglais** ou **Japonais**, la barre de langue n'apparaît pas.
- Si la langue de Citrix Cloud ou la langue d'affichage de votre navigateur est définie sur **Allemand**, **Espagnol** ou **Français**, la barre de langue apparaît après l'ouverture d'une session sur Citrix Studio. Il y a deux options de langue dans la liste de la barre de langue. Sélectionnez une option qui correspond à la langue la plus haute de votre navigateur.

  > **Conseil :**
  >
  > – Les paramètres que vous configurez pour la barre de langue peuvent ne pas prendre effet. Dans ce cas, déconnectez-vous et reconnectez-vous.
  > – Il se peut que vous ne puissiez pas saisir certains symboles et caractères localisés à l'aide de la barre de langue. Pour résoudre le problème, vous devez configurer la langue de Citrix Cloud, la langue d'affichage de votre navigateur et la disposition du clavier local. Pour plus d'informations, consultez l'article CTX310743 du centre de connaissances.

Délai maximal de programme de redémarrage (PowerShell uniquement). Si un redémarrage programmé des machines d'un groupe de mise à disposition ne commence pas en raison d'une panne de base de données de site, vous pouvez spécifier le délai d'attente au-delà de l'heure de démarrage planifiée. Si la connexion à la base de données est restaurée pendant cet intervalle, les redémarrages commencent. Si la connexion n'est pas restaurée pendant cet intervalle, les redémarrages ne commencent pas. Pour plus d'informations, voir Redémarrages programmés retardés en raison d'une panne de base de données.

Équilibrage de charge vertical (PowerShell uniquement). Auparavant, le service utilisait l'équilibrage de charge horizontal pour tous les lancements RDS, ce qui attribuait la charge entrante à la machine RDS la moins chargée. Ce comportement reste le comportement par défaut. Vous pouvez désormais utiliser PowerShell pour activer l'équilibrage de charge vertical en tant que paramètre à l'échelle du site.

Lorsque l'équilibrage de charge vertical est activé, le broker affecte la charge entrante à la machine RDS la plus chargée qui n'a pas atteint un niveau élevé. Ce processus sature les machines existantes avant de passer à de nouvelles machines. Lorsque les utilisateurs se déconnectent et libèrent les machines existantes, une nouvelle charge est attribuée à ces machines.

Par défaut, l'équilibrage de charge horizontal est activé. Pour afficher, activer ou désactiver l'équilibrage de charge vertical, les applets de commande `Get-BrokerSite` et `Set-BrokerSite` prennent désormais en charge le paramètre `UseVerticalScalingForRdsLaunches`. Pour plus d'informations, consultez la section Gérer la charge des machines dans les groupes de mise à disposition.

Décembre 2019

Fonctionnalités nouvelles et améliorées

Service pour Citrix Service Providers (CSP). Les CSP peuvent désormais intégrer des clients locataires au service Virtual Apps and Desktops, configurer un accès administrateur client au service et fournir des espaces de travail partagés ou dédiés aux utilisateurs des clients à l'aide de domaines fédérés. Pour plus d'informations, consultez Citrix Virtual Apps and Desktops Service pour les fournisseurs de services Citrix.

Possibilité de déterminer les raisons pour lesquelles une machine est en mode de maintenance (PowerShell uniquement). Avec PowerShell, vous pouvez désormais déterminer pourquoi une machine est en mode maintenance. Pour ce faire, utilisez le paramètre `-MaintenanceModeReason`. Cette fonctionnalité peut aider les administrateurs à résoudre les problèmes liés aux machines en mode maintenance. Pour plus de détails, consultez https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/Broker/Get-BrokerMachine/.

Autoscale. Autoscale permet désormais de créer des machines et de les supprimer dynamiquement. Vous pouvez optimiser cette fonctionnalité en utilisant un script PowerShell. Le script vous permet d'augmenter ou de réduire dynamiquement le nombre de machines dans le groupe de mise à disposition en fonction des conditions de charge actuelles. Pour plus d'informations, consultez Provisionner dynamiquement les machines avec Autoscale.

Novembre 2019

Fonctionnalités nouvelles et améliorées

GroomStartHour. Le service de surveillance prend désormais en charge **GroomStartHour** - une nouvelle configuration qui aide les administrateurs à déterminer l'heure de la journée à laquelle le nettoyage doit commencer à s'exécuter. Pour de plus amples informations, consultez la documentation de SDK Citrix Virtual Apps and Desktops.

Pagination OData. Le service de surveillance prend désormais en charge la **pagination OData**. Tous les points de terminaison OData v4 renvoient un maximum de 100 enregistrements par page avec un lien vers les 100 enregistrements suivants dans la réponse. Pour plus d'informations, consultez la section Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

Octobre 2019

Fonctionnalités nouvelles et améliorées

App-V. La fonctionnalité App-V est désormais disponible dans Citrix Cloud. Vous pouvez ajouter des packages App-V au Delivery Controller dans votre configuration Citrix Cloud, en mode administrateur simple ou double. Le *module de détection de package Virtual Apps and Desktops Service App-V*, disponible dans Téléchargements Citrix, vous permet d'importer des packages App-V et d'enregistrer des serveurs Microsoft App-V. Les applications qu'ils contiennent sont alors disponibles pour vos utilisateurs. Ce module PowerShell vous permet d'enregistrer les serveurs de gestion et de publication Microsoft App-V à l'aide d'URL DNS, évitant ainsi que les serveurs derrière des mécanismes d'équilibrage de charge soient enregistrés à l'aide de leur URL de machine réelle. Pour plus d'informations, consultez Module de détection du service Citrix Virtual Apps and Desktops pour les packages et les serveurs App-V.

Plate-forme Google Cloud. Le service Citrix Virtual Apps and Desktops ajoute désormais la prise en charge de l'utilisation de Machine Creation Services (MCS) pour provisionner des machines sur Google Cloud Platform (GCP). Pour plus d'informations, voir Environnements de virtualisation Google Cloud Platform.

Septembre 2019

Fonctionnalités nouvelles et améliorées

Prise en charge de VDA pour Azure Virtual Desktop. Pour connaître les systèmes d'exploitation et les versions de VDA pris en charge, consultez VDA dans un environnement Azure Virtual Desktop.

Stratégie d'alimentation améliorée. 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 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. Pour plus d'informations, consultez Gestion de l'alimentation des machines VDI qui passent à une période différente avec des sessions déconnectées.

Catalogues de machines : Balises. Vous pouvez désormais utiliser PowerShell pour appliquer des balises aux catalogues de machines. Pour plus d'informations, consultez la rubrique Appliquer des balises aux catalogues de machines.

Durée du démarrage de session. La fonction Surveiller affiche désormais la durée de démarrage de la session divisée en périodes de démarrage de la session de l'application Workspace et de démarrage de la session VDA. 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 les VDA 1903 ou version ultérieure. Pour plus d'informations, consultez Diagnostiquer les problèmes de démarrage de session.

Août 2019

Fonctionnalités nouvelles et améliorées

Reconnexion automatique de session. La page Sessions de l'onglet Tendances contient désormais des informations sur le nombre de reconnexions automatiques. Les reconnexions automatiques sont tentées lorsque les stratégies Fiabilité de session ou Reconnexion automatique du client sont en vigueur. Les informations de reconnexion automatique vous permettent d'afficher et de dépanner les connexions réseau rencontrant des interruptions, ainsi que d'analyser les réseaux offrant une expérience sans problème.

L'affichage des détails fournit des informations supplémentaires telles que la fiabilité de session ou la 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. 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 des VDA de version 1906 ou ultérieure. Pour plus d'informations, consultez :

- Sessions
- Paramètres de stratégie Reconnexion automatique des clients
- Paramètres de stratégie Fiabilité de session
- Reconnexion automatique de session

Juillet 2019

Fonctionnalités nouvelles et améliorées

Journalisation de la configuration. Vous pouvez désormais utiliser le SDK Remote PowerShell pour supprimer périodiquement le contenu de la base de données de journalisation de la configuration. Pour plus de détails, voir Planifier la suppression périodique des données.

Autoscale. Autoscale permet désormais de gérer l'alimentation uniquement d'un sous-ensemble de machines d'un groupe de mise à disposition. Cette fonctionnalité peut être utile dans les cas d'utilisation de poussée sur le cloud : vous souhaitez utiliser les ressources locales pour gérer les charges de travail avant que les ressources basées sur le cloud répondent à des demandes supplémentaires (c'est-à-dire, une poussée de charges de travail). Pour plus d'informations, consultez Restreindre Autoscale à certaines machines dans un groupe de mise à disposition.

Local App Access et redirection d'adresse URL. Citrix Studio vous permet désormais d'ajouter l'option Ajouter l'application Local App Access à l'interface utilisateur Studio de votre site à l'aide du kit SDK PowerShell. Pour plus d'informations, consultez la section Fournir uniquement l'accès aux applications publiées.

Changements de nom des systèmes d'exploitation. Les noms des systèmes d'exploitation dans les pages **Créer un catalogue de machines > Configuration du catalogue de machines > Système d'exploitation** et **Surveiller** ont changé :

- OS multi-session (anciennement OS de serveur) : le catalogue de machines avec OS à sessions multiples fournit des bureaux partagés hébergés adaptés au déploiement à grande échelle de machines avec OS Linux ou OS à sessions multiples Windows standardisées.
- OS mono-session (anciennement OS de bureau) : le catalogue de machines avec OS mono-session fournit des bureaux VDI adaptés à une variété d'utilisateurs.

Durée Citrix Profile Management dans Chargement du profil. Surveiller inclut désormais la durée du traitement du profil dans la barre Chargement du profil du graphique Durée d'ouverture de session. Il s'agit du temps que met Citrix Profile Management à traiter les profils utilisateur. Ces informations aident les administrateurs à résoudre avec plus de précision les durées de chargement de profil élevées. Cette amélioration est disponible sur les VDA 1903 et version ultérieure. Pour plus d'informations, voir Chargement du profil.

Analyse de bureaux. L'analyse des bureaux est une fonctionnalité du service Citrix Virtual Apps and Desktops. Elle automatise les contrôles d'intégrité des bureaux virtuels publiés dans un site, améliorant ainsi l'expérience utilisateur. Pour lancer l'analyse de bureaux, installez et configurez Citrix Probe Agent sur un ou plusieurs points de terminaison. L'analyse de bureaux est disponible pour les sites sous licence Premium. Cette fonctionnalité nécessite Citrix Probe Agent 1903 ou version ultérieure. Pour plus d'informations, consultez Analyse d'applications et de bureaux.

> **Remarque :**
>
> Citrix Probe Agent prend désormais en charge TLS 1.2.

June 2019

Fonctionnalités nouvelles et améliorées

Restreindre à l'aide de balises. Les balises sont des chaînes qui identifient les éléments tels que les machines, les applications, les bureaux, 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. Pour plus d'informations, consultez la section Groupes d'applications et Balises.

Notifications par e-mail. Le service Citrix Virtual Apps and Desktops envoie par courrier électronique des notifications liées aux alertes et aux sondages. Cela élimine la nécessité de configurer le serveur de messagerie SMTP. La zone **Préférences de notification** est activée par défaut ; Citrix Cloud envoie des notifications d'alerte à l'adresse e-mail fournie dans la section **Préférences de notification**. Assurez-vous que l'adresse e-mail `donotreplynotifications@citrix.com` est ajoutée à la liste blanche dans votre configuration de messagerie.

Mai 2019

Fonctionnalités nouvelles et améliorées

Autoscale. Autoscale est une fonctionnalité du service Citrix Virtual Apps and Desktops qui 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 intègre la technologie Smart Scale obsolète dans la solution de gestion de l'alimentation Studio. Pour plus d'informations, consultez la section Autoscale. Vous pouvez surveiller les indicateurs des machines gérées par AutoScale dans les pages Tendances de l'onglet **Surveiller**. Pour plus d'informations, consultez la section Surveiller les machines gérées par Autoscale.

Février 2019

Fonctionnalités nouvelles et améliorées

Surveillance des alertes d'hyperviseur. Les alertes de Citrix Hypervisor et VMware vSphere sont désormais affichées dans l'onglet **Surveiller** > **Alertes** pour vous aider à surveiller les états et paramètres suivants de l'intégrité de l'hyperviseur :

- Utilisation du processeur
- Utilisation de la mémoire
- Utilisation du réseau
- Connexion d'hyperviseur non disponible

- Utilisation du disque (vSphere uniquement)
- État de l'alimentation ou de la connexion de l'hôte (vSphere uniquement)

Pour plus d'informations, consultez la section Surveillance des alertes d'hyperviseur dans Alertes et notifications.

Communications via les versions TLS antérieures. Pour améliorer la sécurité du service, Citrix bloquera toute communication via TLS (Transport Layer Security) 1.0 et 1.1 à compter du 15 mars 2019 et autorisa uniquement les communications TLS 1.2. Pour plus d'informations, consultez la section Versions TLS. Pour obtenir des instructions supplémentaires, consultez le document CTX247067.

Groupes d'applications. Les groupes d'applications vous permettent de gérer des collections d'applications. Vous pouvez créer des groupes d'applications pour les applications partagées entre différents groupes de mise à disposition ou utilisées par un sous-ensemble d'utilisateurs dans des groupes de mise à disposition. Pour de plus amples informations, consultez l'article Créer des groupes d'applications.

Performances d'ouverture de session - Détails du profil. Le panneau **Durée d'ouverture de session** de la page **Détails de l'utilisateur** sur l'onglet **Surveiller** contient désormais des informations sur les détails de la **phase de chargement du profil** du processus de connexion. Les détails du profil fournissent des informations utiles sur les profils utilisateur de la session en cours, qui peuvent aider les administrateurs à résoudre les problèmes de charge de profil. Une info-bulle contenant les informations de profil utilisateur suivantes est affichée :

- Nombre de fichiers
- Taille du profil
- Nombre de fichiers volumineux

Une analyse détaillée fournit des informations sur les dossiers individuels, leur taille et le nombre de fichiers. Cette fonctionnalité est disponible sur la version 1811 et ultérieure des VDA. Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.

Intégrité des licences Microsoft RDS. L'onglet Surveiller affiche l'état de la licence Microsoft RDS (Remote Desktop Services) sur le panneau **Détails de la machine** de la page Détails de la machine et Détails de l'utilisateur pour les machines avec OS de serveur. Un message approprié s'affiche sur l'état de la licence. Vous pouvez survoler l'icône d'information pour voir plus de détails. Pour plus d'informations, consultez la section Intégrité des licences Microsoft RDS dans Dépanner les machines.

Analyse d'application. Cette fonctionnalité automatise l'évaluation de l'intégrité des applications virtuelles publiées sur un site.

Pour lancer l'analyse d'application :

- Sur une ou plusieurs machines de point de terminaison, installez Citrix Application Probe Agent.
- Configurez Citrix Application Probe Agent avec les informations d'identification de Citrix Workspace et Citrix Virtual Apps and Desktops Service.

- Configurez les applications à analyser, les machines de point de terminaison sur lesquelles exécuter l'analyse et l'heure d'analyse planifiée dans l'onglet **Surveiller** > **Configuration** de Citrix Virtual Apps and Desktops Service.

L'agent teste le lancement des applications sélectionnées via Citrix Workspace et indique les résultats de l'analyse dans l'onglet **Surveiller** de Citrix Virtual Apps and Desktops Service.

- Les résultats sont affichés sur la page Applications (données des dernières 24 heures) et la page **Tendances** > **Résultats de l'analyse d'application**.
- Les résultats incluent l'historique des analyses, ainsi que l'étape où l'échec d'analyse s'est produit : Accessibilité de Workspace, Authentification de Workspace, Énumération de Workspace, Téléchargement ICA ou Lancement d'applications.

Le rapport d'échec est envoyé par courrier électronique aux adresses configurées. Vous pouvez planifier l'exécution des analyses d'application pendant les heures creuses sur plusieurs zones géographiques. De cette façon, vous pouvez utiliser les résultats pour résoudre de manière proactive les problèmes liés aux applications provisionnées, aux machines d'hébergement ou aux connexions avant que les utilisateurs ne les rencontrent. Pour plus d'informations, consultez Analyse d'applications et de bureaux.

Janvier 2019

Fonctionnalités nouvelles et améliorées

Administration déléguée avec étendue personnalisée. La surveillance prend désormais en charge l'étendue personnalisée grâce à des rôles d'administrateur délégué intégrés. Pour plus d'informations sur les rôles intégrés disponibles pour la surveillance et comment les affecter, consultez Rôles d'administrateur délégué.

Décembre 2018

Fonctionnalités nouvelles et améliorées

La date après laquelle Citrix bloquera toute communication via TLS (Transport Layer Security) 1.0 et 1.1 est passée au 31 janvier 2019 (au lieu du 31 décembre 2018). Pour plus de détails, voir Fin de prise en charge des versions TLS.

Novembre 2018

Fonctionnalités nouvelles et améliorées

Données historiques de machine disponibles à l'aide de l'API OData : données historiques suivantes contenant des analyses de machine sont désormais disponibles via l'API OData. Ces données sont collectées toutes les heures et rassemblées pour la journée.

- Nombre de machines sous tension (pour les machines avec gestion de l'alimentation)
- Nombre de machines enregistrées
- Nombre de machines en mode maintenance
- Nombre total de machines

Les données sont agrégées pour la période pendant laquelle le service de surveillance est en cours d'exécution. Pour plus d'informations sur l'utilisation de l'API OData et des exemples, voir Citrix Monitor Service 7 1808. Le schéma de base de données est disponible dans Schéma de Monitor Service.

Performances d'ouverture de session - Détails de la session interactive : le panneau **Durée de connexion** de la vue **Détails de l'utilisateur et Détails de la session** contient des informations sur la phase **Session interactive** du processus de connexion. Le temps nécessaire pour chacune des trois sous-phases (**Pre-userinit**, **Userinit** et **Shell**) est affiché dans la barre de **session interactive** sous la forme d'une info-bulle. Cela permet un dépannage plus précis de cette phase de la connexion. Le délai cumulé entre les sous-phases et un lien vers la documentation sont également fournis. Cette fonctionnalité est disponible sur Delivery Controller version 7 1808 et version ultérieure. La barre de détail **Session interactive** affiche uniquement la durée de la session en cours. Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.

Performances d'ouverture de session - Détails GPO : le panneau **Durée de connexion** de la vue **Détails de l'utilisateur et de la session** contient la durée des objets de stratégie de groupe (GPO). Il s'agit du temps total nécessaire pour appliquer les objets de stratégie de groupe sur la machine virtuelle au cours du processus d'ouverture de session. À présent, vous pouvez voir les détails de chaque stratégie appliquée selon les CSE (extensions côté client) sous forme d'info-bulle sur la barre GPO. Pour chaque application de stratégie, le détail affiche l'état et le temps nécessaire. Ces informations supplémentaires facilitent le dépannage et la résolution des problèmes impliquant une durée de GPO élevée. Les durées indiquées dans le détail représentent uniquement la durée du traitement des CSE et ne correspondent pas à la durée totale du GPO. Cette fonctionnalité est disponible sur Delivery Controller version 7 1808 et version ultérieure. Pour de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion utilisateur.

Corrections

Les requêtes de rapport personnalisé enregistrées durant la surveillance ne sont pas disponibles après une mise à niveau du Cloud. [DNA-23420]

Octobre 2018

Fonctionnalités nouvelles et améliorées

Applications : limite par machine. Vous pouvez maintenant limiter le nombre d'instances d'application par machine. Cette limite s'applique à toutes les machines du site. Cette limite vient s'ajouter à la limite d'application existante pour tous les utilisateurs du groupe de mise à disposition et à la limite par utilisateur. Cette fonctionnalité est disponible uniquement via PowerShell, pas dans Studio. Pour plus de détails, consultez la section Configurer les limites d'application.

Windows Server 2019. Vous pouvez maintenant installer des VDA pour OS multi-session (anciennement VDA pour OS de serveur) sur des machines Windows Server 2019, comme indiqué dans la section Configuration système requise.

Septembre 2018

Fonctionnalités nouvelles et améliorées

Administration déléguée. L'administration déléguée de Citrix Cloud vous permet de configurer les autorisations d'accès requises par tous vos administrateurs conformément à leur rôle dans votre organisation. Pour de plus amples informations, veuillez consulter la section Administration déléguée. La surveillance prend en charge l'allocation de rôles intégrés. Les rôles intégrés sont disponibles avec l'étendue complète. Pour plus d'informations sur les rôles intégrés disponibles pour la surveillance et comment les affecter, consultez Rôles d'administrateur délégué.

Journalisation de la configuration. La journalisation de la configuration permet aux administrateurs de suivre les modifications de configuration et les activités administratives. Pour plus de détails, voir Journalisation de la configuration.

Plusieurs cmdlets PowerShell dans le SDK PowerShell distant qui étaient précédemment désactivées sont maintenant activées, à utiliser avec la journalisation de la configuration :

- Log:GetLowLevelOperation
- Log:GetHighLevelOperation
- Log:GetSummary
- Log:GetDataStore
- Log:ExportReport

Cache d'hôte local. Le cache d'hôte local est maintenant entièrement disponible. La fonctionnalité de cache d'hôte local permet de poursuivre les opérations de négociation de connexion lorsqu'un Cloud Connector dans un emplacement de ressources ne peut pas communiquer avec Citrix Cloud. Pour plus d'informations, veuillez consulter Cache d'hôte local.

Citrix Provisioning. Pour provisionner les VDA, vous pouvez maintenant utiliser Citrix Provisioning ou les Machine Creation Services existants. Pour des informations Citrix Provisioning spécifiques à l'environnement cloud, voir Citrix Provisioning géré par Citrix Cloud.

Corrections

Dans les versions antérieures, lors de l'utilisation du provisioning Azure à la demande, toutes les VM étaient supprimées lors de la mise hors tension. Désormais, seules les VM regroupées sont supprimées. Les VM persistantes (dédiées) ne sont pas supprimées lors de leur mise hors tension.

Août 2018

- **Nouveaux noms de produits**

  Si vous êtes client ou partenaire Citrix depuis un certain temps, vous remarquerez de nouveaux noms dans nos produits et dans la documentation de ces produits. Si vous découvrez ce produit Citrix, vous pourrez parfois rencontrer des noms différents pour un produit ou un composant.

  Les nouveaux noms de produits et de composants représentent mieux le portefeuille toujours croissant de Citrix et sa stratégie cloud. Les articles de cette documentation utilisent les noms suivants.

  - **Citrix Virtual Apps and Desktops :** Citrix Virtual Apps and Desktops offre une solution de bureaux et d'applications virtuels, fournie sous la forme d'un service cloud et d'un produit sur site, donnant aux employés la liberté de travailler n'importe où et sur n'importe quel appareil, tout en réduisant les coûts informatiques. Mettez à disposition des applications Windows, Linux, Web et SaaS ou des bureaux virtuels complets à partir de n'importe quel cloud : public, local ou hybride. La solution Virtual Apps and Desktops s'appelait auparavant XenApp et XenDesktop.
  - **Application Citrix Workspace :** l'application Citrix Workspace intègre la technologie Citrix Receiver existante ainsi que les autres technologies clientes de Citrix Workspace. Elle a été améliorée pour offrir des fonctionnalités supplémentaires afin de proposer aux utilisateurs finaux une expérience contextuelle unifiée qui leur permet d'interagir avec toutes les applications professionnelles, les fichiers et les appareils dont ils ont besoin pour travailler efficacement. Pour plus d'informations, consultez ce billet de blog.

- **Citrix SD-WAN :** NetScaler SD-WAN, une technologie essentielle pour nos clients et partenaires qui transforment leurs réseaux de succursales et leurs réseaux WAN avec la technologie cloud, s'appelle désormais Citrix SD-WAN.
- **Citrix Secure Web Gateway :** dans le cadre de notre portefeuille Citrix Networking toujours croissant, nous sommes fiers d'offrir notre robuste service Citrix Secure Web Gateway, précédemment appelé NetScaler Secure Web Gateway.
- **Citrix Gateway :** NetScaler Unified Gateway, notre solution robuste qui permet un accès sécurisé et contextuel aux applications et aux données dont vous avez besoin pour travailler efficacement, s'appelle désormais Citrix Gateway.
- **Citrix Content Collaboration et Citrix Files pour Windows :** les fonctionnalités avancées d'accès, de collaboration, de workflow, de gestion des droits et d'intégration de ShareFile sont désormais disponibles dans le composant Citrix Content Collaboration de Citrix Workspace, notre solution intégrée, contextuelle et sécurisée. Citrix Files pour Windows vous permet d'accéder directement à vos fichiers Content Collaboration via un lecteur mappé, offrant ainsi une expérience identique à l'Explorateur de fichiers Windows natif.
- **Citrix Hypervisor :** la technologie XenServer pour l'infrastructure de virtualisation, basée sur l'hyperviseur XenProject, est désormais Citrix Hypervisor.

Voici un résumé rapide :

Est	Était
Citrix Virtual Apps and Desktops	XenApp et XenDesktop
Application Citrix Workspace	Intègre Citrix Receiver et d'importantes améliorations
Citrix SD-WAN	NetScaler SD-WAN
Citrix Secure Web Gateway	NetScaler Secure Web Gateway
Citrix Gateway	NetScaler Unified Gateway
Citrix Content Collaboration	ShareFile
Citrix Files pour Windows	ShareFile Desktop App, ShareFile Sync, ShareFile Drive Mapper
Citrix Hypervisor	XenServer
Citrix Provisioning	Citrix Provisioning Services

L'implémentation de cette transition dans nos produits et leur documentation est en cours.

- Le contenu intégré au produit peut encore contenir les anciens noms. Par exemple, vous pouvez voir des instances des anciens noms dans le texte de la console, les messages et les noms de répertoire/fichier.

- Il est possible que certains éléments (tels que les commandes et les MSI) continuent à conserver leurs anciens noms pour éviter de casser les scripts clients existants.
- La documentation produit associée et les autres ressources (telles que les vidéos et les billets de blog) auxquelles la documentation de ce produit renvoie peuvent toujours contenir des noms anciens.
- Pour Citrix Hypervisor : le nouveau nom est utilisé sur le site Web de Citrix et dans les informations produit à partir de septembre 2018. Vous verrez également le nouveau nom dans les consoles d'administration de certains produits Citrix, tels que Citrix Virtual Apps and Desktops. Le produit XenServer et la documentation technique continuent à utiliser XenServer 7.x jusqu'au début de 2019.

Nous vous remercions de votre patience pendant cette transition.

Pour plus de détails sur les nouveaux noms, reportez-vous à https://www.citrix.com/about/citrix-product-guide/.

- **Changements de numéros de version des produits et composants**

  Citrix installe et gère la plupart des composants Citrix Virtual Apps and Desktops, vous ne serez donc pas concerné par ces numéros de version. Cependant, vous pouvez voir les numéros de version lors de l'installation de Cloud Connectors, ainsi que lors de l'installation ou de la mise à niveau de VDA dans des emplacements de ressources.

  Les numéros de version des produits et composants Citrix Virtual Apps and Desktops sont affichés au format suivant : **AAMM.*c.m.b***

  - AAMM = Année et mois de publication du produit ou du composant. Par exemple, une version sortie en septembre 2018 apparaît comme 1809.
  - c = Numéro de version de Citrix Cloud pour le mois.
  - m = Version de maintenance (le cas échéant).
  - b = Numéro de compilation. Ce champ s'affiche uniquement sur la page À propos du composant et dans la fonctionnalité du système d'exploitation permettant de supprimer ou de modifier des programmes.

  Par exemple, **Citrix Virtual Apps and Desktops 1809.1.0** indique que le composant est sorti en septembre 2018. Il est associé à Citrix Cloud version 1 ce mois-là et n'est pas une version de maintenance. Certains écrans affichent uniquement l'année et le mois de la version : par exemple, **Citrix Virtual Apps and Desktops 1809**.

  Dans les versions antérieures (7.18 et versions antérieures), les numéros de version étaient affichés au format : 7.*version*, où la valeur augmentait de 1 pour chaque version. Par exemple, la version VDA suivant XenApp and XenDesktop 7.17 était 7.18. Les versions antérieures (7.18 et antérieures) ne seront pas mises à jour avec le nouveau format de numérotation.

- **Fin de prise en charge des versions TLS.** Pour améliorer la sécurité de Citrix Virtual Apps and Desktops Service, Citrix bloquera toute communication via TLS (Transport Layer Security) 1.0 et 1.1 à compter du 31 décembre 2018. Pour plus de détails, voir Fin de prise en charge des versions TLS.
- **Environnement de virtualisation Google Cloud Platform.** Citrix Virtual Apps and Desktops Service prend en charge la possibilité de mettre manuellement hors/sous tension les VM Virtual Apps and Desktops sur Google Cloud Platform (GCP). Pour plus d'informations, voir Environnements de virtualisation Google Cloud Platform.

Juillet 2018

- **Exportation de données de filtres.** Vous pouvez désormais exporter les données de surveillance en temps réel sur l'onglet **Surveiller** > **Filtres** vers des fichiers au format CSV. La fonction d'exportation est disponible à partir des pages Filtres de Machines, Sessions, Connexions et Instances d'application. Vous pouvez sélectionner un filtre personnalisé prédéfini ou sélectionner des critères de filtre appropriés, choisir les colonnes requises dans le tableau et exporter les données. Des données pouvant atteindre 100 000 enregistrements peuvent être exportées. Les fichiers CSV exportés offrent une vue complète des données en temps réel et facilitent l'analyse des grands ensembles de données.

Juin 2018

- **Connexions à Azure Resource Manager.** Dans l'assistant de création de connexion de Studio, la sélection de l'environnement Azure sur la page **Connexion** inclut tous les clouds Azure valides pour votre abonnement Azure. La disponibilité générale pour Azure US Government Cloud et Azure Germany Cloud remplace les versions préliminaires de ces deux environnements dans les versions antérieures.

Mai 2018

- **Déploiement rapide d'Azure.** Lorsque votre emplacement de ressources utilise des machines Azure Resource Manager pour fournir des applications et des postes de travail, vous pouvez maintenant choisir une méthode de déploiement :
  - Configuration complète : cette méthode existante utilise la console de gestion Studio, qui vous guide dans la création d'un catalogue de machines et d'un groupe de mise à disposition.
  - Déploiement rapide d'Azure : cette nouvelle option fournit une interface plus simple qui permet un déploiement plus rapide des applications et des postes de travail.

- **Lien Citrix Health Assistant.** La page Détails de la machine d'une machine non enregistrée dans la console de surveillance contient désormais un bouton **Health Assistant**. Le lien pointe actuellement vers l'article Dépanner les machines et vers l'article du Centre de connaissances, Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch, à partir duquel vous pouvez télécharger l'outil. Citrix Health Assistant est un outil qui permet de résoudre les problèmes de configuration dans les VDA non enregistrés. L'outil automatise plusieurs vérifications de l'état pour identifier les causes possibles des problèmes courants d'enregistrement de VDA, de lancement de session et de configuration de la redirection de fuseau horaire.
- **Détails de la session interactive.** Dans la console de surveillance, le panneau de la vue **Détails de l'utilisateur > Durée de connexion** contient maintenant des informations sur l'étape **Session interactive** du processus de connexion. Pour permettre une résolution et un dépannage plus précis de cette phase de la connexion, **Session interactive** comporte désormais trois sous-phases : **Pre-userinit**, **Userinit** et **Shell**. Dans cette version, placer le curseur sur **Session interactive** permet d'afficher une info-bulle montrant les sous-phases et un lien vers la documentation. Pour une description des sous-phases et savoir comment améliorer les performances de chaque phase, voir Diagnostiquer les problèmes de connexion utilisateur.

Mars 2018

- **Prédiction d'instances d'applications (fonctionnalité préliminaire).** Il s'agit de la première fonction de surveillance basée sur l'analyse prédictive. La prévision de modèles d'utilisation des ressources est importante pour les administrateurs afin d'organiser les ressources et le nombre requis de licences sur chaque ressource. La fonction de prédiction d'instances d'applications indique le nombre d'instances d'applications hébergées susceptibles d'être lancées par site ou groupe de mise à disposition au cours d'une période donnée. Des algorithmes d'apprentissage automatique basés sur des modèles de données créés avec des données historiques existantes sont utilisés pour effectuer la prédiction. Le niveau de tolérance indique la qualité de la prédiction.

  Pour de plus amples informations, consultez la section Prédiction d'instances d'applications dans Director. Partagez vos commentaires sur l'utilité de cette fonctionnalité dans le forum de discussion Citrix Cloud.

- **API de groupes de mise à disposition - Version préliminaire**

  La version préliminaire des API de groupes de mise à disposition fournit un ensemble d'API REST que vous pouvez utiliser pour automatiser la gestion des groupes de mise à disposition. L'ensemble complet des API disponibles peut être consulté et testé dans la documentation Citrix Cloud API sur https://developer.cloud.com/.

- **Authentification Web Studio**

La console de gestion du service sur Citrix Cloud utilise désormais un jeton du porteur pour authentifier les clients. Le jeton du porteur est nécessaire pour authentifier l'accès à l'API REST Delivery Groups.

- **Accès aux données de Monitor Service à l'aide de la version 4 de l'API OData (fonctionnalité préliminaire)**

  Vous pouvez créer des tableaux de bord de surveillance et de reporting personnalisés en fonction des données du Monitor Service à l'aide du point de terminaison OData V.4. OData V.4 est basé sur l'API Web ASP.NET et prend en charge les requêtes d'agrégation. Utilisez votre nom d'utilisateur et votre jeton du porteur Citrix Cloud pour accéder aux données avec le point de terminaison V4. Pour plus d'informations et d'exemples, consultez la section Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

  Partagez vos commentaires sur l'utilité de cette fonctionnalité dans le forum de discussion Citrix Cloud.

Corrections

- Vous pouvez renommer, déplacer ou supprimer des dossiers d'applications. [#STUD-2376]

Janvier 2018

- **Vérification des licences RDS.** La création de catalogues de machines contenant des machines avec OS de serveur Windows comprend désormais une vérification automatique de licence RDS. Tous les problèmes de licence RDS détectés sont affichés, afin que vous puissiez prendre les mesures appropriées pour éviter une interruption du service. Pour de plus amples informations, consultez la section Créer des catalogues de machines.
- **Accès à la console de la machine à partir de Surveiller.** Le panneau Détails de la machine de Surveiller permet désormais d'accéder aux consoles de machines hébergées sur la version 7.3 de l'hyperviseur XenServer. Vous pouvez maintenant résoudre les problèmes rencontrés dans les VDA directement à partir de Surveiller. Pour obtenir davantage d'informations, veuillez consulter la section Accès à la console machine dans Dépanner les machines.

Décembre 2017

Fonctionnalités nouvelles et améliorées

- **Citrix Workspace.** Citrix Workspace est maintenant disponible pour les **nouveaux** clients de XenApp and XenDesktop Service. Pour plus d'informations, consultez la section Configuration de l'espace de travail.

- **Analyse des applications.** Vous pouvez maintenant analyser et surveiller les performances des applications de manière efficace avec la nouvelle page Analyse des applications disponible dans l'onglet **Surveiller** > **Applications**. La page fournit une vue consolidée de l'état et de l'utilisation de toutes les applications publiées sur votre site. Il affiche des métriques telles que le nombre d'instances par application et les défaillances et erreurs associées aux applications publiées. Cette fonctionnalité requiert des VDA de version 7.15 ou ultérieure.

  Pour obtenir davantage d'informations, veuillez consulter la section Analyses des applications dans la rubrique Surveillance.

Novembre 2017

Fonctionnalités nouvelles et améliorées

- **Cache d'hôte local.** La fonctionnalité de cache d'hôte local permet de poursuivre les opérations de négociation de connexion lorsqu'un Cloud Connector dans un emplacement de ressources ne peut pas communiquer avec Citrix Cloud. Pour plus d'informations, veuillez consulter Cache d'hôte local.
- **Azure Managed Disks.** Azure Managed Disks sont maintenant utilisés par défaut pour les VM provisionnées avec MCS dans les environnements Azure Resource Manager. Si vous le souhaitez, vous pouvez utiliser des comptes de stockage conventionnels. Pour de plus amples informations, consultez la section Environnements de virtualisation Microsoft Azure Resource Manager.
- **Administrateur du service d'assistance.** Lors de la gestion des administrateurs du service pour un compte client Citrix Cloud, vous disposez désormais d'un nouveau choix : Administrateur du service d'assistance. Un administrateur du service d'assistance peut accéder aux fonctions de surveillance du service. Pour de plus amples informations, consultez la section Gérer.

Corrections

- Vous pouvez désormais utiliser l'assistant de la console de gestion du service pour créer un catalogue de machines Remote PC Access. Dans les versions antérieures, vous deviez utiliser une applet de commande PowerShell pour créer un catalogue (tel que documenté dans l'article CTX220737). Ensuite, vous deviez revenir sur la console de gestion pour créer un groupe de mise à disposition. Désormais, vous créez le catalogue et le groupe de mise à disposition de manière séquentielle sur la console de gestion.
- Les catalogues créés avec MCS peuvent utiliser des comptes d'ordinateurs Active Directory existants. [#DNA-24566]
- Lors de la surveillance d'un déploiement, le défilement dans un tableau **Tendances > Sessions** trié affiche des résultats précis. [DNA-51257]

Informations supplémentaires

- Problèmes connus.
- Pour plus d'informations sur les logiciels tiers inclus dans le service, consultez la section Avis de tiers.

Problèmes connus

May 17, 2024

Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) présente les problèmes connus suivants :

- Dans un environnement VMware hébergé sur AWS, la création du catalogue de machines MCS échoue si le vTPM est activé sur l'image principale. Pour obtenir de l'assistance VMware, consultez la section Obtenir de l'assistance. [PMCS-37603]
- Les écrans du moniteur risquent de ne pas se charger si l'URL de Pendo, `https://citrix-cloud-content.customer.pendo.io/`, est bloquée.
  [DIR-18482]
- Un message d'erreur s'affiche si vous exécutez une commande `XDHyp:\` dans Remote PowerShell SDK. Pour résoudre ce problème :

  1. Exécutez une commande avec `Hyp`. Par exemple : `Get-HypServiceStatus`
  2. Exécutez une commande avec `XDHyp:\`. Par exemple : `Get-ChildItem XDHyp:\Connections\`

  [BRK-13723]
- Suite aux modifications apportées à l'architecture de Citrix DaaS dans la version 2209, les icônes par défaut des applications et des bureaux Windows déployés avant cette version sont maintenant des icônes de bureau génériques. Cette modification s'applique uniquement aux bureaux et aux applications qui pointent vers l'icône par défaut. Si vous souhaitez revenir aux icônes par défaut des applications Windows, exécutez le script suivant à l'aide du SDK Remote PowerShell :
  `Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0`.
- Dans **Gérer > Configuration complète**, les tentatives de modification du type de système d'exploitation pour les catalogues Azure échouent et un message d'erreur s'affiche. La modification du type de système d'exploitation pour les catalogues Azure n'est plus prise en charge, même si vous utilisez PowerShell. [STUD-19819]

- Dans les environnements Microsoft Azure, l'activation simultanée du disque d'OS éphémère Azure et des E/S de MCS ne parvient pas à créer un catalogue de machines. Toutefois, pour les catalogues de machines existants, vous pouvez toujours mettre à jour un catalogue de machines, ajouter ou supprimer des machines virtuelles et supprimer un catalogue de machines. [PMCS-21698]
- L'icône de flèche déroulante des boutons Nbre moyen d'E/S par seconde, Contrôle de la session et Contrôle de l'alimentation peut ne pas apparaître dans les pages **Détails utilisateur** et **Détails de la machine**. Cependant, la fonctionnalité fonctionne comme prévu. Pour afficher tous les éléments du menu, cliquez n'importe où sur le bouton. [DIR-11875]
- Si vous utilisez Azure AD Domain Services : les noms UPN de connexion à Workspace (ou StoreFront) doivent contenir le nom de domaine qui a été spécifié lors de l'activation de Azure AD Domain Services. Les connexions ne peuvent pas utiliser les noms UPN d'un domaine personnalisé que vous créez, même si ce domaine personnalisé est désigné comme le domaine principal.
- Lors du déploiement sur Azure et de la création d'un catalogue MCS version 7.9 ou ultérieure avec le cache en écriture activé et le VDA installé sur l'image principale de version 1811 ou antérieure, une erreur se produit. En outre, vous ne pouvez rien créer qui soit lié à Personal vDisk pour Microsoft Azure. Pour contourner le problème, sélectionnez une autre version de catalogue à déployer sur Azure ou désactivez le cache en écriture différée. Pour désactiver le cache en écriture différée lorsque vous créez un catalogue, décochez les cases **Mémoire allouée au cache** et **Taille du cache disque** sur la page **Machines**.
- Le lien **Console** sur **Surveiller > Détails de la machine** ne lance pas la console Machine dans les navigateurs Microsoft Edge 44 et Firefox 68 ESR. [DIR-8160]
- Lorsque vous essayez d'utiliser l'option « Redémarrer » dans l'application Workspace sur le Web ou le bureau, la boîte de dialogue « Redémarrer » ne se ferme jamais et ne signale jamais que l'opération a réussi. L'hyperviseur indique que la machine s'est arrêtée, mais n'a pas démarré. Pour contourner ce problème, après un certain temps, l'utilisateur peut fermer la boîte de dialogue « Redémarrage » et lancer le bureau. Le bureau devrait démarrer. [BRK-5564]

Pour les problèmes liés aux VDA actuels, consultez la section Problèmes connus.

Fin de prise en charge

March 7, 2024

Cet article vous informe à l'avance des fonctionnalités de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) qui vont disparaître pour que vous puissiez prendre les décisions appro-

priées. Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand retirer les fonctionnalités. 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 Product Lifecycle Support Policy.

> **Remarque :**
>
> Les fins de prise en charge et suppressions de Citrix Virtual Apps and Desktops sont décrites dans l'article Fin de prise en charge correspondant.

Fins de prise en charge et retraits

La liste suivante présente les fonctionnalités Citrix DaaS qui sont obsolètes ou ont été retirées.

Les éléments *obsolètes* ne sont pas retirés immédiatement. Citrix continue de les prendre en charge, mais ils seront retirés dans le futur.

Les éléments *retirés* sont retirés, ou ne sont plus pris en charge, dans Citrix DaaS. Les dates en **caractères gras** indiquent les mises à jour les plus récentes.

Élément	Fin de prise en charge annoncée dans la version	Supprimé dans la version	Solution alternative
Prise en charge de la configuration du cache en écriture différée pour inclure uniquement un cache disque et aucun cache mémoire	Février 2024		Utilisez l'option de configuration de la taille du cache mémoire et indiquez une taille différente de zéro.
Prise en charge des catalogues Azure créés avant la fonctionnalité de provisioning à la demande (catalogues « d'ancienne génération »)	Février 2024		Recréez les machines virtuelles du catalogue Azure d'ancienne génération. Les catalogues sont fournis à la demande et permettent de réduire les coûts de stockage.

Élément	Fin de prise en charge annoncée dans la version	Supprimé dans la version	Solution alternative
Support pour Citrix Connector 3.1 pour System Center Configuration Manager	Décembre 2023		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	Décembre 2023		Utilisez Azure Compute Gallery pour répliquer l'image principale dans la région souhaitée.
Prise en charge du travailleur de volume AWS	Novembre 2023		Utiliser le chargement et le téléchargement directs sur disque. Voir Chargement et téléchargement directs sur disque.
Prise en charge de l'option `Leave user management to Citrix Cloud` utilisée pour créer des groupes de mise à disposition	Septembre 2023	Septembre 2023	
Prise en charge de `AwsCaptureInstanceProperties` utilisé dans les environnements AWS	Août 2023		Utilisez un profil de machine. Reportez-vous à la section Créer un catalogue à l'aide d'un profil de machine.
Prise en charge de VMware vSphere 6.7		Juin 2023	Utilisez des versions supérieures pour VMware vSphere.

Élément	Fin de prise en charge annoncée dans la version	Supprimé dans la version	Solution alternative
Commande Powershell `Schedule-ProvVMUpdate`	Avril 2023		Utilisez la commande `Set-ProvVMUpdateTimeWindow`.
Commande Powershell `Request-ProvVMUpdate`	Avril 2023		Utilisez la commande `Set-ProvVMUpdateTimeWindow` avec les paramètres `-StartsNow` et `-DurationInMinutes -1`.
Commande Powershell `Cancel-ProvVMUpdate`	Avril 2023		Utilisez la commande `Clear-ProvVMUpdateTimeWindow`.
Paramètre `DedicatedTenancy` utilisé dans la commande `New-ProvScheme`	Mars 2023		Utilisez le paramètre `TenancyType`.
Disque non géré pour créer une machine virtuelle dans l'environnement Azure	Juin 2022		

Élément	Fin de prise en charge annoncée dans la version	Supprimé dans la version	Solution alternative
Prise en charge de quatre commandes spécifiques à AWS : `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` et `Grant-HypSecurityGroupIngress`	Mai 2022		
Paramètre `StorageAccountType` utilisé dans les environnements Azure	Avril 2022		Utilisez `StorageType`.
Ancienne console (console MMC)	Juillet 2021	Novembre 2021	Utilisez **Gérer > Configuration complète** pour accéder à la gamme complète des actions de configuration et de gestion.
Déploiement rapide d'Azure	Septembre 2020		Utilisez Déploiement rapide.

Élément	Fin de prise en charge annoncée dans la version	Supprimé dans la version	Solution alternative
Possibilité d'importer des machines cibles Citrix Provisioning pour créer des catalogues dans Citrix Studio.	Août 2020	Février 2021	Utilisez l'Assistant d'exportation de machines Citrix Provisioning pour transférer les machines virtuelles Citrix Provisioning dans des Delivery Controllers/MCS pour la création de catalogue. Consultez la section Assistant d'exportation de machines.

Configuration système requise

June 12, 2024

Introduction

La configuration système requise des composants non couverts dans ce document (telles que l'application Citrix Workspace et Citrix Provisioning) est décrite dans leur documentation respective.

Nous ne pouvons pas fournir de recommandations relatives au dimensionnement des VM chargées de mettre à disposition des applications et postes de travail en raison de la nature complexe et dynamique des offres de matériel. Chaque déploiement a des besoins uniques. En général, le dimensionnement d'une VM est basé sur le matériel et non pas sur les charges de travail de l'utilisateur (à l'exception de la RAM, vous aurez besoin de RAM supplémentaire pour les applications qui consomment davantage). La Citrix Tech Zone contient les dernières recommandations sur le dimensionnement des VDA.

> **Important :**
>
> Les versions de VDA mentionnées dans cet article sont soumises au cycle de vie du produit Citrix. Pour plus d'informations, consultez le tableau des produits sur le site Web de Citrix.
>
> Pour plus d'informations sur l'utilisation de VDA LTSR avec Citrix DaaS, consultez CTX205549.

Rappel : dans un déploiement Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), vous n'avez pas besoin d'installer ni de gérer les composants principaux (Delivery Controller, la base de données de site ou consoles de gestion et de surveillance). Pour obtenir des conseils d'installation de Virtual Delivery Agent (VDA), voir :

- Installer des VDA
- Installez des VDA à l'aide de la ligne de commande.

Cloud Connector

Pour plus d'informations, consultez la section Détails techniques sur Cloud Connector.

VDA dans un environnement Azure

Systèmes d'exploitation pris en charge :

- Windows 11 sessions multiples
- Windows 11 Mode session unique
- Windows 10 sessions multiples
- Windows 10 session unique
- Windows Server 2022 (nécessite un VDA 2106 minimum)
- Windows Server 2019
- Windows Server 2016

Tous les VDA qui n'ont pas atteint leur fin de vie sont pris en charge pour une utilisation avec Citrix DaaS. Nous vous recommandons d'utiliser les VDA LTSR avec la dernière mise à jour cumulative. Pour plus d'informations sur le cycle de vie des VDA, consultez le Tableau des produits Citrix.

Windows Server 2012 R2 est uniquement pris en charge avec VDA 1912 (et versions ultérieures).

Windows Server nécessite des licences Microsoft RDS.

Pour plus d'informations sur Azure Virtual Desktop, consultez la documentation Microsoft.

VDA pour OS mono-session

Les informations suivantes s'appliquent à la dernière version de VDA.

Systèmes d'exploitation pris en charge :

- Windows 11
- Windows 10
  - Pour connaître les éditions prises en charge, voir l'article CTX224843. Cet article contient également des liens vers les problèmes connus de Citrix avec les versions de Windows prises en charge.
  - La redirection de la composition du bureau et le mode graphique d'ancienne génération ne sont pas pris en charge sur Windows 10.

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.
  - Si la machine contient une version antérieure de ce composant d'exécution (telle que 2015-2017), 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.

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.

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 de bureau Windows prises en charge, la prise en charge Media Foundation est déjà installée et ne peut pas être supprimée. Cependant, les éditions N n'incluent pas certaines technologies multimédia. Vous pouvez obtenir ce logiciel auprès de Microsoft ou d'un tiers.

Informations complémentaires :

- Pour obtenir des informations sur le Linux VDA, consultez la documentation du produit Linux Virtual Delivery Agent.

- Pour utiliser la fonctionnalité Server VDI, vous pouvez utiliser l'interface de ligne de commande pour l'installation d'un VDA mono-session 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 de version plus ancienne, voir Systèmes d'exploitation antérieurs.
- Voir aussi VDA dans un environnement Azure Virtual Desktop.

VDA pour OS multi-session

Les informations suivantes s'appliquent à la dernière version de VDA.

Systèmes d'exploitation pris en charge :

- Windows Server 2022 (nécessite un VDA 2106 minimum)
- Windows Server 2019, éditions Standard et Datacenter
- Windows Server 2016, édition Standard et Datacenter
- Windows 11
- Windows 10 (64 bits) : toutes les versions prises en charge

Le programme d'installation déploie automatiquement les composants suivants :

- 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.
  - Si la machine contient une version antérieure de ce composant d'exécution (telle que 2015-2017), 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.

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. Cela déclenche un redémarrage.

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 versions de Windows Server, la fonctionnalité Media Foundation est installée via le Gestionnaire de serveur. Cependant, les éditions N n'incluent pas certaines technologies multimédia. Vous pouvez obtenir ce logiciel auprès de Microsoft ou d'un tiers.

Si Media Foundation n'est pas présente sur le VDA, ces fonctionnalités multimédias ne fonctionnent pas :

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

Informations complémentaires :

- 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 un système d'exploitation Windows qui n'est plus pris en charge, consultez la section Systèmes d'exploitation antérieurs.
- Voir aussi VDA dans un environnement Azure Virtual Desktop.

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 CTX131239 contient des informations sur la version la plus récente de l'hyperviseur, ainsi que des liens vers les problèmes connus.

- **Amazon Web Services (AWS)**
  - Vous pouvez configurer des applications et des bureaux sur les systèmes d'exploitation Windows pris en charge.
  - Le service Amazon de la base de données relationnelle (RDS) n'est pas pris en charge.

  Pour plus d'informations, consultez la section Environnements de cloud AWS.
- **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.
- **Google Cloud Platform**

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

  Pour plus d'informations, consultez la section Environnements de virtualisation HPE Moonshot.

- **Microsoft Azure Resource Manager**

  Pour de plus amples informations, consultez Environnements de cloud Microsoft Azure Resource Manager.

- **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 Cloud on AWS**

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

  Pour plus d'informations, consultez Cloud VMware sur Amazon Web Services (AWS).

- **Azure VMware Solution (AVS)**

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

  Pour plus d'informations, consultez Intégration de la solution Azure VMware (AVS).

- **Google Cloud VMware Engine**

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

  Pour plus d'informations, consultez Google Cloud VMware Engine.

- **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.

> **Remarque :**
>
> Vous ne devez pas installer le logiciel VDA sur un serveur Citrix DDC ou StoreFront. Le VDA doit être un système autonome. L'installation de plusieurs composants sur une seule machine virtuelle n'est autorisée que lors du développement d'une preuve de concept ou lors de la publication de la console d'administration Studio auprès d'administrateurs uniquement. Dans ce cas, vous devez vous assurer que les utilisateurs non administrateurs n'ont pas accès aux machines virtuelles DDC/StoreFront.

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

Pour plus d'informations sur Active Directory, consultez la section Joint à Active Directory.

Technologies HDX

Pour accéder aux informations de prise en charge et de configuration requise pour les fonctionnalités HDX, consultez la section HDX.

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 2019
- Windows Server 2016

Exigences :

- Microsoft .NET Framework 4.8 (minimum)
- Microsoft Visual C++ 2015-2022 Redistributable.
  - Si la machine contient une version antérieure de ce composant d'exécution (telle que 2015-2017), 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.

Pour les VDA multi-session, 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.

Connectivité du service

Consultez la section Configuration requise pour le système et la connectivité pour obtenir des informations sur la connexion Internet. Ces informations incluent les exigences communes à la plupart des services Citrix Cloud, plus la configuration requise pour Citrix DaaS.

Autre

- 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. Visual Studio 2015 runtime doit être installé sur la machine sur laquelle vous installez `CitrixGroupPolicyManagement_x64.msi`. Pour plus d'informations, consultez la documentation de Microsoft.
- Ce produit prend en charge les versions 3 à 5 de PowerShell.
- Les composants et les fonctionnalités qui peuvent être installés sur des serveurs Windows, ne peuvent pas être installés sur des serveurs Server Core et Nano Server, sauf indication contraire.
- Pour plus d'informations sur les limites de ressources dans un déploiement, reportez-vous à la section Limites.
- Pour connaître les versions StoreFront prises en charge, consultez la configuration système requise pour StoreFront.
- Pour obtenir davantage d'informations sur la globalisation, veuillez consulter l'article CTX119253.
- Pour plus d'informations sur les ports utilisés par Citrix DaaS, consultez Ports de communication utilisés par les technologies Citrix.
- Pour plus d'informations sur les conditions requises lorsque vous utilisez l'interface de gestion Déploiement rapide, reportez-vous aux exigences.

Limites

June 12, 2024

Les valeurs de cet article indiquent les limites d'une instance Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) unique. Ces limites sont testées de manière approfondie par Citrix et recommandées pour une expérience optimale pour les utilisateurs et les administrateurs. Il s'agit de limites souples qui ne sont pas appliquées techniquement (à l'exception du nombre total de VDA par emplacement de ressources). Lorsque le nombre d'utilisateurs simultanés dépasse 125 000, Citrix peut monter en charge et combiner plusieurs instances Citrix DaaS afin d'offrir une expérience unifiée à n'importe quelle échelle.

Les informations contenues dans cet article sont dynamiques. Revenez fréquemment pour vérifier si elles ont été mises à jour. Si vos besoins actuels ne sont pas traités dans cette publication, contactez dès que possible votre représentant Citrix pour obtenir de l'aide.

Limites de configuration

Si les stratégies dépassent la limite, Citrix recommande d'utiliser le service Workspace Environment Management ou les objets de stratégie de groupe (GPO) Active Directory.

Ressource	Limites
Domaines Active Directory	100
Dossiers d'application	1 000
Groupes d'applications	250
Applications	5 000
Catalogues	2 000
Groupes de mise à disposition	2 000
Connexions hôte	200
Emplacements des ressources	100
Stratégies de console de gestion (Configuration complète)	200
Balises	10 000
VDA	100 000

Limites d'emplacement des ressources

Le tableau suivant répertorie les limites pour chaque emplacement de ressources.

Si vos besoins dépassent ces limites, Citrix recommande d'utiliser des emplacements de ressources supplémentaires.

Ressource	Limites
Nombre total de VDA (limite stricte)	10 000
Nombre total de sessions	25 000
Domaines Active Directory	1
Connexions hôte	40

Les Citrix Cloud Connector sont attribués à des emplacements de ressources et lient les charges de travail à Citrix DaaS. Pour plus d'informations sur les limites de Cloud Connector, consultez Considérations sur le dimensionnement et la scalabilité des Cloud Connector.

Limites de provisioning

Les limites de provisioning indiquées dans le tableau suivant sont les valeurs maximales recommandées par Citrix pour un abonnement à un seul fournisseur public.

Vous êtes susceptible d'atteindre les limites de quota de votre fournisseur de cloud public à des niveaux inférieurs. Dans ce cas, contactez le fournisseur pour augmenter le quota de votre abonnement. Pour les déploiements à plus grande échelle, Citrix recommande un modèle hub-and-spoke (modèle en étoile), où les VDA sont distribués sur plusieurs abonnements et connexions hôtes.

Pour plus d'informations, consultez les architectures de référence suivantes :

- Citrix DaaS sur AWS
- Virtualisation Citrix sur Google Cloud
- Citrix DaaS sur Azure

Ressource	Limites
VDA par compte Amazon Web Services par région	3 000
VDA par projet Google Cloud Platform	3 000
VDA par abonnement Microsoft Azure par région	5 000

> **Remarque :**
>
> Ces limites sont recommandées par Citrix.

Limites d'utilisation

Pour plus d'informations sur les rôles d'administrateur et les différences entre ces rôles, voir :

- Administrateurs de gestion (Configuration complète)
- Administrateurs de surveillance (Director)

Ressource	Limites
Administrateurs complets de surveillance (Director) simultanés	40
Administrateurs du centre d'assistance de surveillance (Director) simultanés	200
Administrateurs de sessions de surveillance (Director) simultanés	50
Administrateurs cloud de gestion (Configuration complète) simultanés	100
Administrateurs du service d'assistance de gestion (Configuration complète) simultanés	60
Utilisateurs finaux simultanés	125 000
Ressources publiées pour un seul utilisateur	250
Lancements de session par minute	3 000

- L'onglet Surveiller (Director) prend en charge l'agrégation d'un maximum de quatre locataires Citrix DaaS (« spokes ») sous un seul locataire (« hub »).
- Un administrateur du centre d'assistance sur l'instance hub peut surveiller et dépanner les utilisateurs, les machines, les points de terminaison et les transactions de toutes les instances agrégées (hub et spokes) conformément à la configuration de l'administration déléguée sur l'instance spécifique.
- Le nombre d'administrateurs simultanés par instance Citrix DaaS est conforme au tableau Limites d'utilisation.

Journal des modifications des limites

Le tableau suivant répertorie la modification des limites de configuration :

Date	Ressource	Description
22 Nov 2023	Domaines Active Directory	La limite a été augmentée de 85 à 100.
	Catalogues	La limite a été augmentée de 1 000 à 2 000.
	Groupes de mise à disposition	La limite a été augmentée de 1 000 à 2 000.
	Emplacements des ressources	La limite a été augmentée de 85 à 100.
	Emplacement des ressources -> Nombre total de sessions	La limite a été augmentée de 20 000 à 25 000.
07 Dec 2023	Limites de provisioning -> VDA par abonnement Microsoft Azure par région	La limite a été augmentée de 2 500 à 5 000.

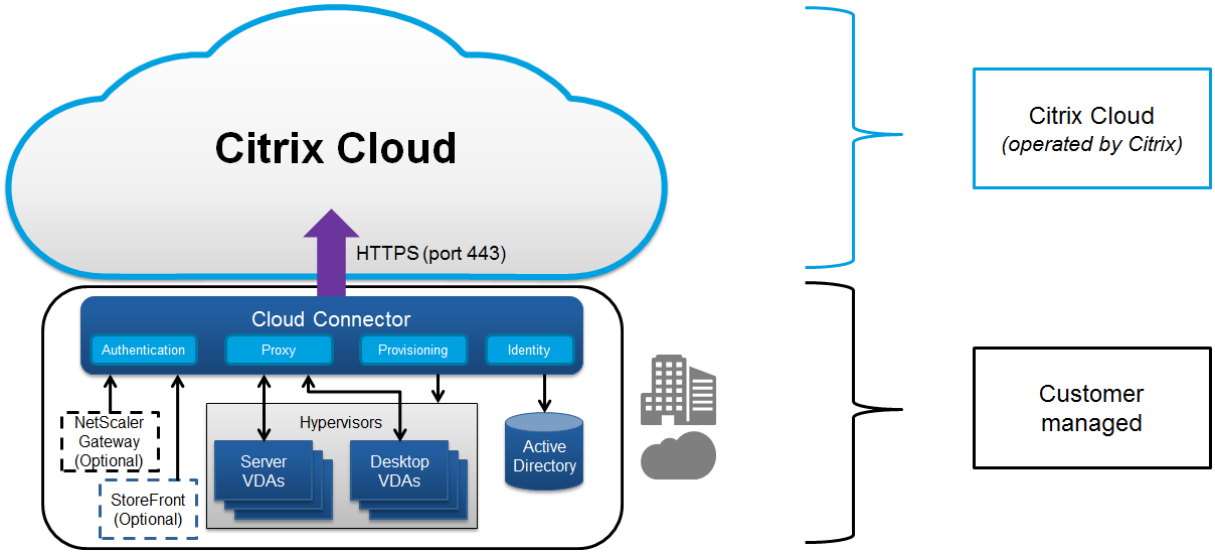
Vue d'ensemble de la sécurité technique

May 17, 2024

Vue d'ensemble de la sécurité technique

Ce document s'applique aux services Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) hébergés dans Citrix Cloud. Ces informations incluent Citrix Virtual Apps Essentials et Citrix Virtual Desktops Essentials.

Citrix Cloud permet de gérer le fonctionnement du plan de contrôle pour les environnements Citrix DaaS. Le plan de contrôle comprend les Delivery Controller, les consoles de gestion, la base de données SQL, le serveur de licences et éventuellement StoreFront et Citrix Gateway (anciennement NetScaler Gateway). Les Virtual Delivery Agents (VDA) hébergeant les bureaux et applications restent sous le contrôle du client dans le datacenter de leur choix, sur cloud ou sur site. Ces composants sont connectés au service de cloud à l'aide d'un agent appelé le Citrix Cloud Connector. Si les clients choisissent d'utiliser Citrix Workspace, ils peuvent également choisir d'utiliser Citrix Gateway Service au lieu d'exécuter Citrix Gateway dans leur datacenter. Le diagramme suivant illustre Citrix DaaS et ses limites de sécurité.



Conformité cloud de Citrix

L'utilisation de Citrix Managed Azure Capacity avec diverses éditions de Citrix DaaS et Workspace Premium Plus n'a pas été évaluée pour Citrix SOC 2 (Type 1 ou 2), ISO 27001, HIPAA ou d'autres exigences de conformité cloud. (Janvier 2021). Visitez le Citrix Trust Center pour en savoir plus sur les certifications Citrix Cloud et consultez-le fréquemment pour obtenir les informations les plus récentes.

Flux de données

Citrix DaaS n'héberge pas les VDA, de sorte que les données d'application du client et les images requises pour le provisioning sont toujours hébergées dans la configuration du client. Le plan de contrôle a accès aux métadonnées, telles que les noms d'utilisateur, les noms de machines et les raccourcis d'application, ce qui limite l'accès à la propriété intellectuelle du client à partir du plan de contrôle.

Les données qui transitent entre le cloud et les locaux du client utilisent une connexion sécurisée TLS sur le port 443.

Isolation des données

Citrix DaaS stocke uniquement les métadonnées requises pour la communication et le contrôle des applications et bureaux du client. Les informations sensibles, y compris les images, les profils utilisateur et d'autres données applicatives restent dans les locaux du client ou dans leur abonnement avec un fournisseur de cloud public.

Éditions de service

Les fonctionnalités de Citrix DaaS varient selon les éditions. Par exemple, Citrix Virtual Apps Essentials ne prend en charge que Citrix Gateway Service et Citrix Workspace. Consultez la documentation Produit pour en savoir plus sur les fonctionnalités prises en charge.

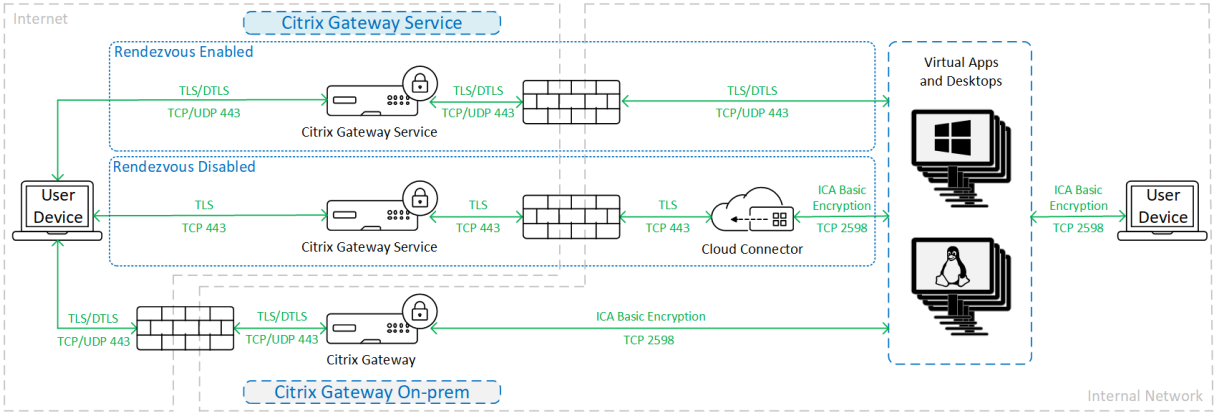
Sécurité ICA

Citrix DaaS offre plusieurs options pour sécuriser le trafic ICA en transit. Les options disponibles sont les suivantes :

- **Cryptage de base :** paramètre par défaut.
- **SecureICA :** permet de chiffrer les données de session à l'aide du chiffrement RC5 (128 bits).
- **VDA TLS/DTLS :** permet d'utiliser le chiffrement au niveau du réseau à l'aide de TLS/DTLS.
- **Protocole Rendezvous :** disponible uniquement lors de l'utilisation du Citrix Gateway Service. Lorsque vous utilisez le protocole Rendezvous, les sessions ICA sont chiffrées de bout en bout à l'aide de TLS/DTLS.

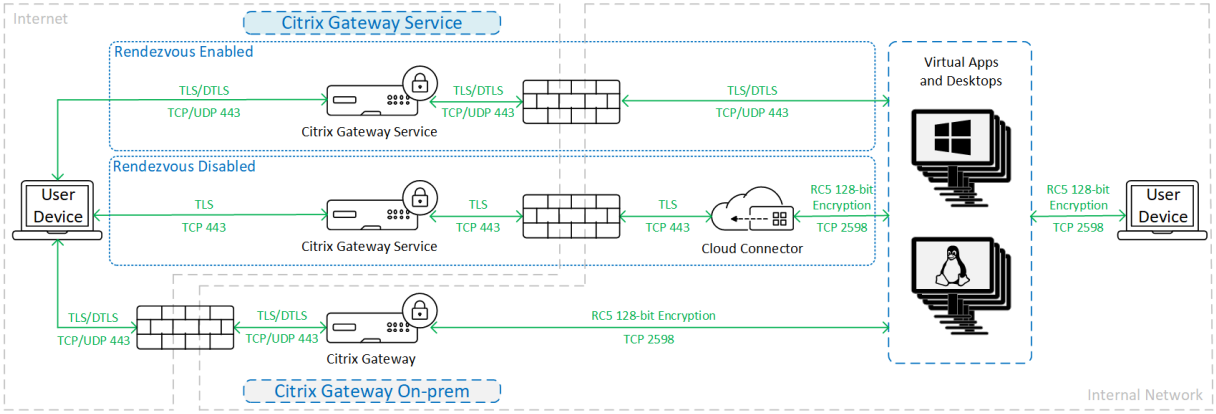
Cryptage de base

Lors de l'utilisation du cryptage de base, le trafic est chiffré comme indiqué dans le graphique suivant.



Secure ICA

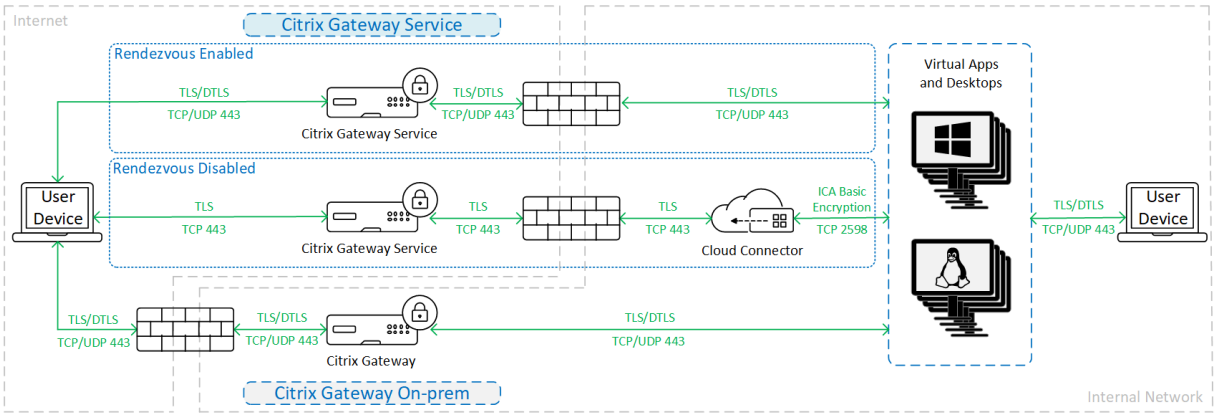
Lorsque vous utilisez SecureICA, le trafic est chiffré comme indiqué dans le graphique suivant.



> **Remarque :**
>
> SecureICA n'est pas pris en charge lors de l'utilisation de l'application Workspace pour HTML5.

VDA TLS/DTLS

Lors de l'utilisation du cryptage VDA TLS/DTLS, le trafic est chiffré comme indiqué dans le graphique suivant.



> **Remarque :**
>
> Lorsque vous utilisez le service Gateway sans Rendezvous, le trafic entre le VDA et le Cloud Connector n'est pas chiffré par TLS, car le Cloud Connector ne prend pas en charge la connexion au VDA avec un cryptage au niveau du réseau.

Plus de ressources

Pour plus d'informations sur les options de sécurité ICA et sur la façon de les configurer, voir :

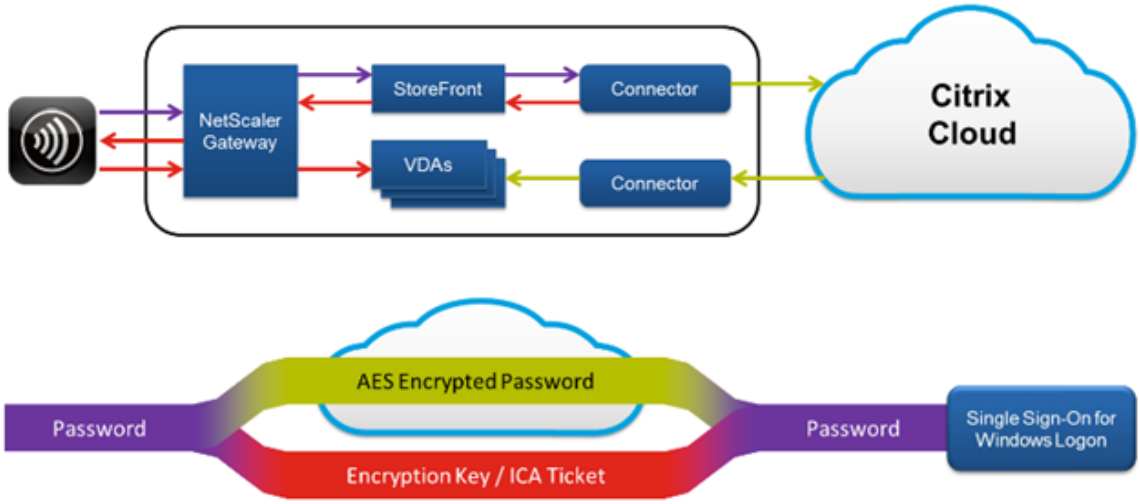
- SecureICA : Paramètres de stratégie Sécurité
- TLS/DTLS VDA : Transport Layer Security
- Protocole Rendezvous : Protocole Rendezvous

Gestion des informations d'identification

Citrix DaaS gère quatre types d'informations d'identification :

- Informations d'identification de l'utilisateur : lors de l'utilisation d'un StoreFront géré par le client, les informations d'identification utilisateur sont cryptées par le Cloud Connector à l'aide du cryptage AES-256 et d'une clé à usage unique générée aléatoirement pour chaque démarrage. La clé n'est jamais transmise au cloud et elle est uniquement renvoyée à l'application Citrix Workspace. Cette clé est ensuite transmise au VDA directement par l'application Citrix Workspace afin de décrypter le mot de passe utilisateur lors du lancement de session pour une expérience SSO. Le flux est illustré dans la figure suivante.

  Par défaut, les informations d'identification des utilisateurs ne sont pas transmises au-delà des limites de domaines non fiables. Si un VDA et StoreFront sont installés dans un domaine et qu'un utilisateur d'un autre domaine tente de se connecter au VDA, la tentative d'ouverture de session échoue à moins qu'une confiance ne soit établie entre les domaines. Vous pouvez désactiver ce comportement et autoriser le transfert des informations d'identification entre des domaines non fiables à l'aide du DaaS PowerShell SDK. Pour plus d'informations, consultez Set-Brokersite.



- Informations d'identification d'administrateur : les administrateurs s'authentifient auprès de Citrix Cloud. L'authentification génère un jeton Web signé JSON (JWT) à usage unique qui donne à l'administrateur l'accès à Citrix DaaS.
- Mots de passe d'hyperviseur : les hyperviseurs sur site qui requièrent un mot de passe pour l'authentification disposent d'un mot de passe généré par l'administrateur et stocké et crypté directement dans la base de données SQL dans le cloud. Citrix gère les clés d'homologue pour s'assurer que les informations d'identification de l'hyperviseur sont uniquement disponibles pour les processus authentifiés.
- Informations d'identification Active Directory (AD) : Machine Creation Services utilise le Cloud

Connector pour créer des comptes de machines dans l'Active Directory d'un client. Étant donné que le compte de machine du Cloud Connector possède uniquement un accès en lecture à Active Directory, l'administrateur est invité à entrer des informations d'identification pour chaque opération de création ou de suppression de machine. Ces informations d'identification sont uniquement stockées en mémoire et conservées pour un seul événement de provisioning.

Considérations de déploiement

Citrix recommande aux utilisateurs de consulter la documentation sur les meilleures pratiques pour le déploiement d'applications et de VDA Citrix Gateway dans leurs environnements.

Exigences d'accès au réseau de Citrix Cloud Connector

Les Citrix Cloud Connector requièrent uniquement le trafic sortant vers Internet sur le port 443 et peuvent être hébergés derrière un proxy HTTP.

- Le protocole de communication utilisé dans Citrix Cloud pour HTTPS est TLS. (Voir Fin de prise en charge des versions TLS)
- Dans le réseau interne, le Cloud Connector doit avoir accès aux composants suivants pour Citrix DaaS :
  - VDA : port 80, entrant et sortant, ainsi que 1494 et 2598 entrants si vous utilisez Citrix Gateway Service
  - Serveurs StoreFront : port 80 entrant.
  - Citrix Gateway, si configuré comme une STA : port 80 entrant.
  - Contrôleurs de domaine Active Directory
  - Hyperviseurs : sortant uniquement. Consultez Ports de communication utilisés par les technologies Citrix pour connaître les ports spécifiques.

Le trafic entre les VDA et les connecteurs cloud est crypté à l'aide de la sécurité au niveau du message de Kerberos.

StoreFront géré par le client

Un StoreFront géré par le client offre davantage d'options de configuration de sécurité et une plus grande flexibilité pour l'architecture de déploiement, y compris la possibilité de gérer les informations d'identification utilisateur sur site. StoreFront peut être hébergé derrière Citrix Gateway afin de fournir un accès à distance sécurisé, appliquer une authentification multi-facteurs et ajouter d'autres fonctionnalités de sécurité.

Citrix Gateway Service

L'utilisation de Citrix Gateway Service évite le besoin de déployer Citrix Gateway dans les datacenters des clients.

Pour plus de détails, consultez Citrix Gateway Service.

Toutes les connexions TLS entre le Cloud Connector et Citrix Cloud sont initiées du Cloud Connector vers Citrix Cloud. Aucun mappage de port de pare-feu entrant n'est requis.

Approbation XML

Ce paramètre est disponible dans **Configuration complète > Paramètres > Activer l'approbation XML** et il est désactivé par défaut. Vous pouvez également utiliser le SDK Citrix DaaS Remote PowerShell pour gérer l'approbation XML.

L'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 de l'approbation XML permet aux utilisateurs de s'authentifier avec succès, puis de démarrer les applications. Cloud Connector approuve les informations d'identification envoyées à partir de StoreFront. Activez le paramètre d'approbation XML uniquement lorsque vous avez sécurisé les communications entre vos Citrix Cloud Connectors et StoreFront (à l'aide de pare-feu, d'IPsec ou d'autres recommandations de sécurité).

Cette option est désactivée par défaut.

Utilisez le SDK Remote PowerShell Citrix DaaS pour gérer l'approbation XML.

- Pour vérifier la valeur actuelle de l'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`.

Appliquer le trafic HTTPS ou HTTP

Pour appliquer le trafic HTTPS ou HTTP via le service XML, configurez l'un des jeux de valeurs de registre suivants sur chacun de vos Cloud Connectors.

Après avoir configuré les paramètres, redémarrez le Remote Broker Provider Service sur chaque Cloud Connector.

Dans `HKLM\Software\Citrix\DesktopServer\` :

- Pour appliquer le trafic HTTPS (ignorer HTTP) : Définissez `XmlServicesEnableSsl` sur `1` et `XmlServicesEnableNonSsl` sur `0`.
- Pour appliquer le trafic HTTP (ignorer HTTPS) : Définissez `XmlServicesEnableNonSsl` sur `1` et `XmlServicesEnableSsl` sur `0`.

Fin de prise en charge des versions TLS

Pour améliorer la sécurité de Citrix DaaS, Citrix a commencé à bloquer toute communication via TLS (Transport Layer Security) 1.0 et 1.1, à compter du 15 mars 2019.

Toutes les connexions aux services Citrix Cloud à partir de Citrix Cloud Connector nécessitent TLS 1.2.

Pour garantir la réussite de la connexion à Citrix Workspace à partir des périphériques utilisateur, la version de Citrix Receiver installée doit être égale ou supérieure aux versions suivantes.

Receiver	Version
Windows	4.2.1000
Mac	12.0
Linux	13.2
Android	3.7
iOS	7.0
Chrome/HTML5	Version la plus récente (le navigateur doit prendre en charge TLS 1.2)

Pour effectuer une mise à niveau vers la dernière version de Citrix Receiver, accédez à https://www.citrix.com/products/receiver/.

Vous pouvez également effectuer une mise à niveau vers l'application Citrix Workspace, qui utilise TLS 1.2. Pour télécharger l'application Citrix Workspace, accédez à https://www.citrix.com/downloads/workspace-app/.

Si vous devez continuer à utiliser TLS 1.0 ou 1.1 (par exemple, si vous utilisez un client léger basé sur une version antérieure de Receiver pour Linux), installez StoreFront dans votre emplacement de ressources. Ensuite, faites pointer tous les Citrix Receivers vers ce StoreFront.

Informations supplémentaires

Les ressources suivantes contiennent des informations sur la sécurité :

- Vue d'ensemble de la sécurité technique pour Azure géré par Citrix.
- Site de sécurité de Citrix.
- Informations sur la sécurité et la conformité : le centre de sécurité et de conformité contient des bulletins de sécurité qui peuvent vous aider à rester informé. Le centre propose également une documentation sur les normes et les certifications qui sont importantes pour maintenir un environnement informatique sécurisé et conforme.
- Guide de déploiement sécurisé de la plate-forme Citrix Cloud : ce guide fournit une vue d'ensemble des recommandations en matière de sécurité lors de l'utilisation de Citrix Cloud et décrit les informations recueillies et gérées par Citrix Cloud. Ce guide contient également des liens vers des informations complètes sur Citrix Cloud Connector.
- Configuration requise pour le système et la connectivité.
- Considérations de sécurité et meilleures pratiques.
- Cartes à puce.
- Transport Layer Security (TLS).

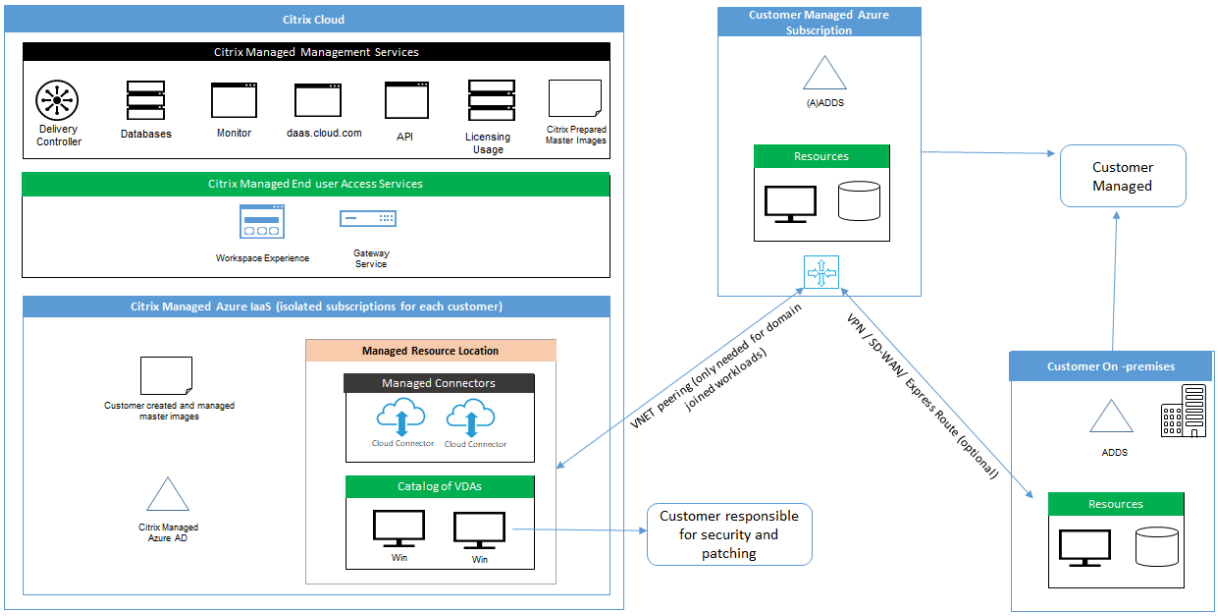
> **Remarque :**
>
> Ce document vise à fournir au lecteur une introduction et un aperçu des fonctionnalités de sécurité de Citrix Cloud et à définir le partage des responsabilités entre Citrix et les clients en ce qui concerne la sécurisation du déploiement de Citrix Cloud. Il n'est pas conçu pour servir de manuel de configuration et d'administration de Citrix Cloud ou de l'un de ses composants ou services.

Vue d'ensemble de la sécurité technique pour Azure géré par Citrix

May 17, 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.

Le diagramme suivant illustre les composants d'un déploiement Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) qui utilise Azure géré par Citrix. Cet exemple utilise une connexion d'appairage de réseaux virtuels.



Avec Azure géré par Citrix, les Virtual Delivery Agent (VDA) du client qui fournissent des bureaux et des applications, ainsi que des Citrix Cloud Connector, sont déployés dans un abonnement Azure et un locataire gérés par Citrix.

Conformité cloud de Citrix

L'utilisation de Citrix Managed Azure Capacity avec diverses éditions de Citrix DaaS et Workspace Premium Plus n'a pas été évaluée pour Citrix SOC 2 (Type 1 ou 2), ISO 27001, HIPAA ou d'autres exigences de conformité cloud. (Janvier 2021). Visitez le Citrix Trust Center pour en savoir plus sur les certifications Citrix Cloud et consultez-le fréquemment pour obtenir les informations les plus récentes.

Responsabilité de Citrix

Citrix Cloud Connector pour catalogues non joints à un domaine

Lorsque vous utilisez un abonnement Azure géré par Citrix, Citrix DaaS déploie au moins deux Cloud Connector dans chaque emplacement de ressources. Certains catalogues peuvent partager un emplacement de ressources s'ils se trouvent dans la même région que d'autres catalogues pour le même client.

Citrix est responsable des opérations de sécurité suivantes sur les Cloud Connector de catalogues non joints à un domaine :

- Installation des mises à jour du système d'exploitation et des correctifs
- Installation et maintenance d'un logiciel antivirus
- Installation des mises à jour logicielles des Cloud Connector

Les clients n'ont pas accès aux Cloud Connector. Citrix est donc entièrement responsable des performances des Cloud Connector de catalogues qui ne sont pas joints à un domaine.

Abonnement Azure et Azure Active Directory

Citrix est responsable de la sécurité de l'abonnement Azure et d'Azure Active Directory (AAD) créés pour le client. Citrix garantit l'isolation des locataires, de sorte que chaque client dispose de son propre abonnement Azure et AAD, et les échanges croisés entre différents locataires sont évités. Citrix limite également l'accès à AAD à Citrix DaaS et au personnel des opérations Citrix uniquement. L'accès de Citrix à l'abonnement Azure de chaque client est vérifié.

Les clients utilisant des catalogues non joints à un domaine peuvent utiliser AAD géré par Citrix comme moyen d'authentification pour Citrix Workspace. Pour ces clients, Citrix crée des comptes utilisateurs à privilèges limités dans AAD géré par Citrix. Toutefois, ni les utilisateurs ni les administrateurs des clients ne peuvent exécuter d'actions sur AAD géré par Citrix. Si ces clients choisissent plutôt d'utiliser leur propre AAD, ils sont entièrement responsables de sa sécurité.

Infrastructure et réseaux virtuels

Au sein de l'abonnement Azure géré par Citrix du client, Citrix crée des réseaux virtuels pour isoler les emplacements de ressources. Au sein de ces réseaux, Citrix crée des machines virtuelles pour les VDA, les Cloud Connector et les machines de création d'images, en plus des comptes de stockage, des coffres de clés et d'autres ressources Azure. Citrix, en partenariat avec Microsoft, est responsable de la sécurité des réseaux virtuels, y compris des pare-feu de réseau virtuel.

Citrix garantit que la stratégie de pare-feu Azure par défaut (groupes de sécurité réseau) est configurée de façon à limiter l'accès aux interfaces réseau dans l'appairage de réseau virtuel et les connexions SD-WAN. En règle générale, cela contrôle le trafic entrant vers les VDA et Cloud Connector. Pour plus de détails, consultez :

- Stratégie de pare-feu pour les connexions d'appairage de réseaux virtuels Azure
- Stratégie de pare-feu pour les connexions SD-WAN

Les clients ne peuvent pas modifier cette stratégie de pare-feu par défaut, mais ils peuvent déployer des règles de pare-feu supplémentaires sur des machines VDA créées par Citrix. Par exemple, pour limiter partiellement le trafic sortant. Les clients qui installent des clients de réseau privé virtuel, ou d'autres logiciels capables de contourner les règles de pare-feu, sur des machines VDA créées par Citrix sont responsables de tous les risques de sécurité pouvant en découler.

Lorsque le générateur d'images dans Citrix DaaS est utilisé pour créer et personnaliser une nouvelle image de machine, les ports 3389-3390 sont ouverts temporairement dans le réseau virtuel géré par

Citrix, de sorte que le client peut utiliser le Remote Desktop Protocol vers la machine contenant la nouvelle image de machine, pour la personnaliser.

Responsabilité de Citrix lors de l'utilisation de connexions d'appairage de réseaux virtuels Azure

Pour que les VDA de Citrix DaaS contactent des contrôleurs de domaine locaux, des partages de fichiers ou d'autres ressources intranet, Citrix DaaS fournit un flux de travail d'appairage de réseaux virtuels comme option de connectivité. Le réseau virtuel géré par Citrix du client est associé à un réseau virtuel Azure géré par le client. Le réseau virtuel géré par le client peut permettre la connectivité avec les ressources locales du client à l'aide de la solution de connectivité cloud vers site de son choix, comme Azure ExpressRoute ou les tunnels IPSec.

La responsabilité de Citrix pour l'appairage de réseaux virtuels se limite à la prise en charge du flux de travail et de la configuration des ressources Azure associée pour établir une relation d'appairage entre Citrix et les réseaux virtuels gérés par le client.

Stratégie de pare-feu pour les connexions d'appairage de réseaux virtuels Azure Citrix ouvre ou ferme les ports suivants pour le trafic entrant et sortant qui utilise une connexion d'appairage de réseaux virtuels.

Réseau virtuel géré par Citrix avec des machines non jointes à un domaine

- Règles du trafic entrant
  - Autorisez les ports 80, 443, 1494 et 2598 entrants des VDA vers les Cloud Connector et des Cloud Connector vers les VDA.
  - Autorisez les ports 49152-65535 entrants vers les VDA à partir d'une plage IP utilisée par la fonction d'observation de Gérer. Consultez Ports de communication utilisés par les technologies Citrix.
  - Refusez tout autre trafic entrant. Cela inclut le trafic intra-réseau virtuel depuis VDA vers VDA et VDA vers Cloud Connector.
- Règles du trafic sortant
  - Autorisez tout le trafic sortant.

Réseau virtuel géré par Citrix avec des machines jointes à un domaine

- Règles du trafic entrant
  - Autorisez les ports 80, 443, 1494 et 2598 entrants des VDA vers les Cloud Connector et des Cloud Connector vers les VDA.

  - Autorisez les ports 49152-65535 entrants vers les VDA à partir d'une plage IP utilisée par la fonction d'observation de Gérer. Consultez Ports de communication utilisés par les technologies Citrix.
  - Refusez tout autre trafic entrant. Cela inclut le trafic intra-réseau virtuel depuis VDA vers VDA et VDA vers Cloud Connector.

- Règles du trafic sortant
  - Autorisez tout le trafic sortant.

Réseau virtuel géré par le client avec des machines jointes à un domaine

- Il appartient au client de configurer correctement son réseau virtuel. Cela inclut l'ouverture des ports suivants pour rejoindre un domaine.
- Règles du trafic entrant
  - Autorisez le trafic entrant sur 443, 1494 et 2598 à partir des adresses IP clientes pour les lancements internes.
  - Autorisez le trafic entrant sur 53, 88, 123, 135-139, 389, 445, 636 à partir de réseau virtuel Citrix (plage IP spécifiée par le client).
  - Autorisez le trafic entrant sur les ports ouverts avec une configuration proxy.
  - Autres règles créées par le client.
- Règles du trafic sortant
  - Autorisez le trafic entrant sur 443, 1494 et 2598 vers un réseau virtuel Citrix (plage IP spécifiée par le client) pour les lancements internes.
  - Autres règles créées par le client.

Responsabilité Citrix lors de l'utilisation de la connectivité SD-WAN

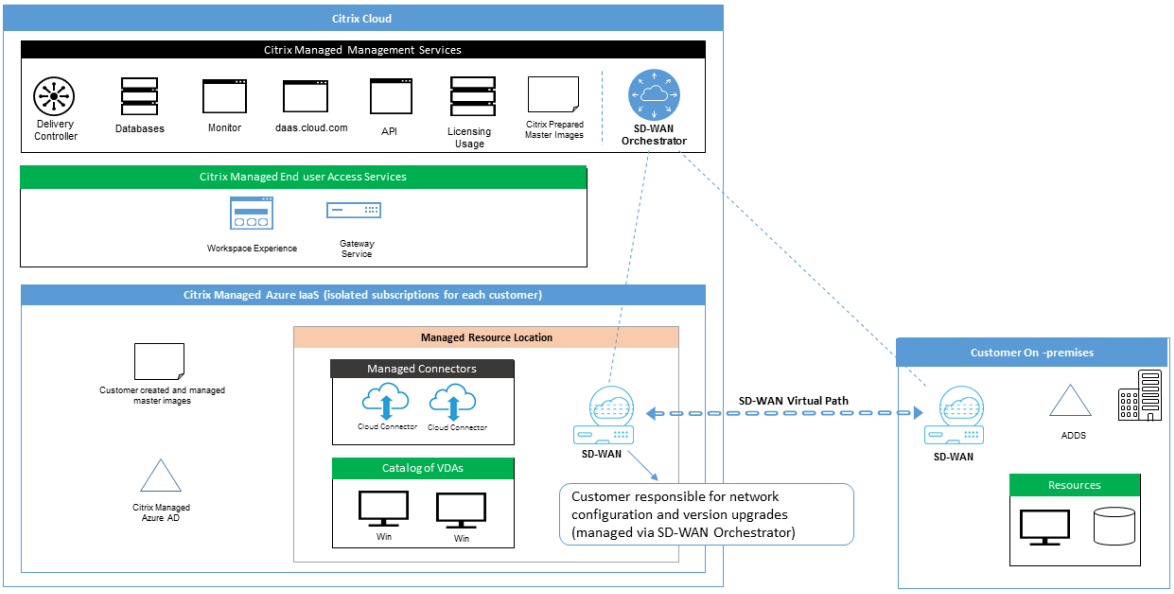
Citrix prend en charge une méthode entièrement automatisée pour déployer des instances virtuelles de Citrix SD-WAN pour permettre la connectivité entre Citrix DaaS et les ressources locales. La connectivité Citrix SD-WAN présente plusieurs avantages par rapport à l'appairage de réseaux virtuels, notamment :

Fiabilité et sécurité élevées des connexions VDA vers centre de données et VDA vers branche (ICA).

- Meilleure expérience utilisateur final pour les employés de bureau, avec des capacités QoS avancées et des optimisations VoIP.
- Possibilité intégrée d'inspecter, de hiérarchiser et de générer des rapports sur le trafic réseau Citrix HDX et l'utilisation d'autres applications.

Citrix exige que les clients qui souhaitent tirer parti de la connectivité SD-WAN pour Citrix DaaS utilisent SD-WAN Orchestrator pour gérer leurs réseaux Citrix SD-WAN.

Le diagramme suivant montre les composants ajoutés dans un déploiement Citrix DaaS utilisant un abonnement Azure géré par Citrix et une connectivité SD-WAN.



Le déploiement Citrix SD-WAN pour Citrix DaaS est similaire à la configuration du déploiement Azure standard pour Citrix SD-WAN. Pour plus d'informations, consultez Déployer une instance Citrix SD-WAN Standard Edition sur Azure. Dans une configuration haute disponibilité, une paire d'instances SD-WAN active/en veille avec des équilibreurs de charge Azure est déployée en tant que passerelle entre le sous-réseau contenant des VDA et des Cloud Connector, et Internet. Dans une configuration sans haute disponibilité, seule une seule instance SD-WAN est déployée en tant que passerelle. Les interfaces réseau des appliances SD-WAN virtuelles se voient attribuer des adresses provenant d'une petite plage d'adresses distincte divisée en deux sous-réseaux.

Lors de la configuration de la connectivité SD-WAN, Citrix apporte quelques modifications à la configuration réseau des bureaux gérés décrite ci-dessus. En particulier, tout le trafic sortant du réseau virtuel, y compris le trafic vers les destinations Internet, est acheminé via l'instance Cloud SD-WAN. L'instance SD-WAN est également configurée pour être le serveur DNS du réseau virtuel géré par Citrix.

L'accès de gestion aux instances SD-WAN virtuelles nécessite un identifiant et un mot de passe administrateur. Chaque instance SD-WAN se voit attribuer un mot de passe sécurisé unique et aléatoire qui peut être utilisé par les administrateurs SD-WAN pour la connexion et le dépannage à distance via l'interface utilisateur SD-WAN Orchestrator, l'interface utilisateur de gestion des appliances virtuelles et l'interface de ligne de commande.

Tout comme les autres ressources spécifiques au locataire, les instances SD-WAN virtuelles déployées dans un réseau virtuel client spécifique sont complètement isolées de tous les autres réseaux virtuels.

Lorsque le client active la connectivité Citrix SD-WAN, Citrix automatise le déploiement initial des instances SD-WAN virtuelles utilisées avec Citrix DaaS, gère les ressources Azure sous-jacentes (machines virtuelles, équilibreurs de charge, etc.), fournit une solution prête à l'emploi sécurisée et efficace pour la configuration initiale des instances SD-WAN virtuelles, et permet la maintenance continue et le dépannage via SD-WAN Orchestrator. Citrix prend également des mesures raisonnables pour effectuer une validation automatique de la configuration réseau SD-WAN, vérifier les risques de sécurité connus et afficher les alertes correspondantes via SD-WAN Orchestrator.

Stratégie de pare-feu pour les connexions SD-WAN Citrix utilise des stratégies de pare-feu Azure (groupes de sécurité réseau) et l'attribution d'adresses IP publiques pour limiter l'accès aux interfaces réseau des appliances SD-WAN virtuelles :

- Seules les interfaces WAN et de gestion se voient attribuer des adresses IP publiques et permettent la connectivité sortante à Internet.
- Les interfaces LAN, agissant comme passerelles pour le réseau virtuel géré par Citrix, sont uniquement autorisées à échanger du trafic réseau avec des machines virtuelles sur le même réseau virtuel.
- Les interfaces WAN limitent le trafic entrant au port UDP 4980 (utilisé par Citrix SD-WAN pour la connectivité des chemins virtuels) et refusent le trafic sortant vers le réseau virtuel.
- Les ports de gestion autorisent le trafic entrant vers les ports 443 (HTTPS) et 22 (SSH).
- Les interfaces haute disponibilité ne sont autorisées qu'à échanger le trafic de contrôle entre elles.

Accès à l'infrastructure

Citrix peut accéder à l'infrastructure gérée par Citrix (Cloud Connector) du client pour effectuer certaines tâches administratives telles que la collecte des journaux (y compris l'Observateur d'événements Windows) et le redémarrage des services sans en avertir le client. Citrix est responsable de l'exécution de ces tâches en toute sécurité, avec un impact minimal sur le client. Citrix est également responsable de s'assurer que tous les fichiers journaux sont récupérés, transportés et traités en toute sécurité. Les VDA clients ne sont pas accessibles de cette façon.

Sauvegardes pour catalogues non joints à un domaine

Citrix n'est pas responsable des sauvegardes de catalogues non joints à un domaine.

Sauvegardes d'images de machine

Citrix est responsable de la sauvegarde de toutes les images de machine chargées sur Citrix DaaS, y compris les images créées avec le générateur d'images. Citrix utilise un stockage redondant localement pour ces images.

Bastions pour catalogues non joints à un domaine

Le personnel des opérations Citrix a la capacité de créer un bastion, si nécessaire, pour accéder à l'abonnement Azure géré par Citrix du client pour diagnostiquer et réparer les problèmes des clients, potentiellement avant que le client ne soit conscient d'un problème. Citrix n'a pas besoin du consentement du client pour créer un bastion. Lorsque Citrix crée le bastion, Citrix crée un mot de passe fort généré aléatoirement pour le bastion et restreint l'accès RDP aux adresses IP NAT Citrix. Lorsque le bastion n'est plus nécessaire, Citrix le retire et le mot de passe n'est plus valide. Le bastion (et les règles d'accès RDP qui l'accompagnent) est retiré lorsque l'opération est terminée. Citrix peut accéder uniquement aux Cloud Connector non joints à un domaine du client avec le bastion. Citrix ne dispose pas du mot de passe nécessaire pour se connecter à des VDA non joints à un domaine ou à des Cloud Connector et VDA appartenant à un domaine.

Stratégie de pare-feu lors de l'utilisation d'outils de dépannage

Lorsqu'un client demande la création d'une machine bastion à des fins de dépannage, les modifications suivantes du groupe de sécurité sont apportées au réseau virtuel géré par Citrix :

- Autorisez temporairement le trafic entrant 3389 de la plage IP spécifiée par le client vers le bastion.
- Autorisez temporairement le trafic entrant 3389 depuis l'adresse IP du bastion vers n'importe quelle adresse du réseau virtuel (VDA et Cloud Connector).
- Continuez à bloquer l'accès RDP entre les Cloud Connector, les VDA et les autres VDA.

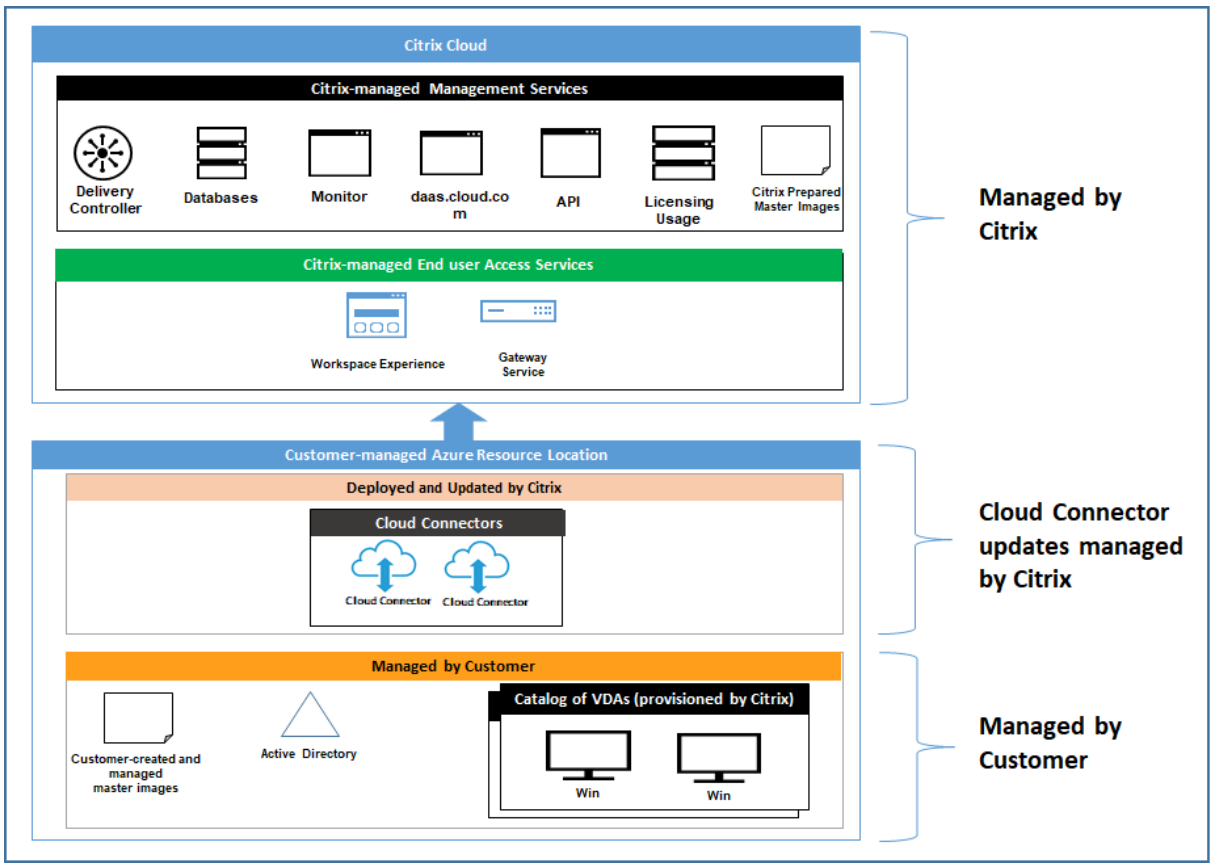
Lorsqu'un client autorise l'accès RDP à des fins de dépannage, les modifications suivantes du groupe de sécurité sont apportées au réseau virtuel géré par Citrix :

- Autorisez temporairement le trafic entrant 3389 depuis la plage IP spécifiée par le client vers n'importe quelle adresse du réseau virtuel (VDA et Cloud Connector).
- Continuez à bloquer l'accès RDP entre les Cloud Connector, les VDA et les autres VDA.

Abonnements gérés par le client

Pour les abonnements gérés par le client, Citrix adhère aux responsabilités ci-dessus lors du déploiement des ressources Azure. Après le déploiement, tout ce qui précède relève de la responsabilité

du client, car le client est propriétaire de l'abonnement Azure.



Responsabilité du client

VDA et images de machine

Le client est responsable de tous les aspects du logiciel installé sur les machines VDA, y compris :

- mises à jour du système d'exploitation et correctifs de sécurité
- antivirus et antimalware
- mises à jour logicielles VDA et correctifs de sécurité
- règles de pare-feu logiciel supplémentaires (en particulier le trafic sortant)
- suivre les considérations de sécurité et les meilleures pratiques Citrix

Citrix fournit une image préparée destinée à servir de point de départ. Les clients peuvent utiliser cette image à des fins de preuve de concept ou de démonstration ou comme base pour créer leur propre image de machine. Citrix ne garantit pas la sécurité de cette image préparée. Citrix tentera de maintenir à jour le système d'exploitation et le logiciel VDA de l'image préparée et activera Windows Defender sur ces images.

Responsabilité du client lors de l'utilisation de l'appairage de réseaux virtuels

Le client doit ouvrir tous les ports spécifiés dans Réseau virtuel géré par le client avec des machines jointes à un domaine.

Lorsque l'appairage de réseaux virtuels est configuré, le client est responsable de la sécurité de son propre réseau virtuel et de sa connectivité à ses ressources locales. Le client est également responsable de la sécurité du trafic entrant provenant du réseau virtuel appairé géré par Citrix. Citrix ne prend aucune mesure pour bloquer le trafic entre le réseau virtuel géré par Citrix et les ressources locales du client.

Les clients disposent des options suivantes pour limiter le trafic entrant :

- Donnez au réseau virtuel géré par Citrix un bloc IP qui n'est pas utilisé ailleurs dans le réseau local du client ou dans le réseau virtuel connecté géré par le client. Ceci est nécessaire pour l'appairage de réseaux virtuels.
- Ajoutez des groupes de sécurité réseau Azure et des pare-feu au réseau virtuel du client et au réseau local pour bloquer ou restreindre le trafic provenant du bloc IP géré par Citrix.
- Déployez des mesures telles que des systèmes de prévention des intrusions, des pare-feu logiciels et des moteurs d'analyse comportementale dans le réseau virtuel du client et le réseau local, avec le bloc IP géré par Citrix comme cible.

Responsabilité du client lors de l'utilisation de la connectivité SD-WAN

Lorsque la connectivité SD-WAN est configurée, les clients disposent d'une flexibilité totale pour configurer les instances SD-WAN virtuelles utilisées avec Citrix DaaS en fonction de leurs besoins réseau, à l'exception de quelques éléments requis pour garantir le bon fonctionnement du SD-WAN dans le réseau virtuel géré par Citrix. Responsabilités du client :

- Conception et configuration de règles de routage et de pare-feu, y compris les règles relatives à la rupture du trafic DNS et Internet
- Maintenance de la configuration réseau SD-WAN
- Surveillance de l'état opérationnel du réseau
- Déploiement rapide des mises à jour logicielles Citrix SD-WAN ou des correctifs de sécurité Étant donné que toutes les instances de Citrix SD-WAN sur un réseau client doivent exécuter la même version du logiciel SD-WAN, les déploiements de versions logicielles mises à jour sur les instances SD-WAN de Citrix DaaS doivent être gérés par les clients en fonction des calendriers et des contraintes de maintenance du réseau.

Une configuration incorrecte des règles de routage et de pare-feu SD-WAN ou une mauvaise gestion des mots de passe de gestion SD-WAN peuvent entraîner des risques de sécurité pour les ressources virtuelles de Citrix DaaS et les ressources locales accessibles via les chemins virtuels Citrix SD-WAN.

Un autre risque de sécurité possible provient de la non-mise à jour du logiciel Citrix SD-WAN vers la dernière version du correctif disponible. Bien que SD-WAN Orchestrator et d'autres services Citrix Cloud fournissent les moyens de faire face à ces risques, il incombe aux clients de s'assurer que les instances SD-WAN virtuelles sont configurées de manière appropriée.

Proxy

Le client peut choisir d'utiliser un proxy pour le trafic sortant du VDA. Si un proxy est utilisé, le client a les responsabilités suivantes :

- Configuration des paramètres proxy sur l'image de machine VDA ou, si le VDA est joint à un domaine, utilisation de la stratégie de groupe Active Directory
- Maintenance et sécurité du proxy

Les proxy ne peuvent pas être utilisés avec Citrix Cloud Connector ou une autre infrastructure gérée par Citrix.

Résilience du catalogue

Citrix fournit trois types de catalogues avec différents niveaux de résilience :

- **Statique :** chaque utilisateur est affecté à un seul VDA. Ce type de catalogue n'offre pas de haute disponibilité. Si le VDA d'un utilisateur tombe en panne, il devra être placé sur un nouveau VDA. Azure fournit un contrat de niveau de service de 99,5 % pour les machines virtuelles à instance unique. Le client peut toujours sauvegarder le profil utilisateur, mais toutes les personnalisations effectuées sur le VDA (telles que l'installation de programmes ou la configuration de Windows) seront perdues.
- **Aléatoire :** chaque utilisateur est affecté aléatoirement à un VDA serveur au moment du lancement. Ce type de catalogue offre une haute disponibilité via la redondance. Si un VDA tombe en panne, aucune information n'est perdue car le profil de l'utilisateur se trouve ailleurs.
- **Multisession Windows 10 :** ce type de catalogue fonctionne de la même manière que le type aléatoire, mais utilise des VDA de station de travail Windows 10 au lieu de VDA de serveur.

Sauvegardes pour catalogues joints à un domaine

Si le client utilise des catalogues joints à un domaine avec un appairage de réseaux virtuels, il est responsable de la sauvegarde de ses profils utilisateur. Citrix recommande aux clients de configurer des partages de fichiers locaux et de définir des stratégies sur leur Active Directory ou leurs VDA pour extraire les profils utilisateur de ces partages de fichiers. Le client est responsable de la sauvegarde et de la disponibilité de ces partages de fichiers.

Récupération d'urgence

En cas de perte de données Azure, Citrix récupérera autant de ressources que possible dans l'abonnement Azure géré par Citrix. Citrix tentera de récupérer les Cloud Connector et les VDA. Si Citrix ne réussit pas à récupérer ces éléments, les clients sont responsables de la création d'un nouveau catalogue. Citrix suppose que les images machine sont sauvegardées et que les clients ont sauvegardé leurs profils utilisateur, ce qui permet de reconstruire le catalogue.

En cas de perte d'une région Azure entière, le client est responsable de la reconstruction de son réseau virtuel qu'il gère lui-même dans une nouvelle région et de la création d'un nouvel appairage de réseaux virtuels ou d'une nouvelle instance SD-WAN au sein de Citrix DaaS.

Responsabilités partagées des clients et de Citrix

Citrix Cloud Connector pour catalogues joints à un domaine

Citrix DaaS déploie au moins deux Cloud Connector dans chaque emplacement de ressources. Certains catalogues peuvent partager un emplacement de ressources s'ils se trouvent dans la même région, le même appairage de réseaux virtuels et le même domaine que d'autres catalogues pour le même client. Citrix configure les Cloud Connector du client joints à un domaine pour les paramètres de sécurité par défaut suivants sur l'image :

- mises à jour du système d'exploitation et correctifs de sécurité
- logiciel antivirus
- mises à jour logicielles des Cloud Connector

Les clients n'ont normalement pas accès aux Cloud Connector. Toutefois, ils peuvent obtenir un accès en utilisant les étapes de dépannage du catalogue et en se connectant à l'aide des informations d'identification du domaine. Le client est responsable des modifications qu'il apporte lors d'une connexion via le bastion.

Les clients ont également le contrôle sur les Cloud Connector joints à un domaine via la stratégie de groupe Active Directory. Il incombe au client de s'assurer que les stratégies de groupe qui s'appliquent au Cloud Connector sont sûres et raisonnables. Par exemple, si le client choisit de désactiver les mises à jour du système d'exploitation à l'aide de la stratégie de groupe, il doit effectuer les mises à jour du système d'exploitation sur les Cloud Connector. Le client peut également choisir d'utiliser la stratégie de groupe pour appliquer une sécurité plus stricte que les valeurs par défaut de Cloud Connector, par exemple en installant un autre logiciel antivirus. En général, Citrix recommande aux clients de placer les Cloud Connector dans leur propre unité organisationnelle Active Directory sans stratégie, car cela garantit que les valeurs par défaut utilisées par Citrix peuvent être appliquées sans problème.

Dépannage

Si le client rencontre des problèmes avec le catalogue dans Citrix DaaS, il existe deux options de dépannage : utiliser des bastions et activer l'accès RDP. Les deux options présentent un risque de sécurité pour le client. Le client doit comprendre et accepter ce risque avant d'utiliser ces options.

Il incombe à Citrix d'ouvrir et de fermer les ports nécessaires pour effectuer des opérations de dépannage, et de limiter les machines accessibles pendant ces opérations.

Avec des bastions ou un accès RDP, l'utilisateur actif effectuant l'opération est responsable de la sécurité des machines auxquelles il accède. Si le client accède au VDA ou au Cloud Connector via RDP et contracte accidentellement un virus, le client est responsable. Si le personnel du support Citrix accède à ces machines, il incombe à ce personnel d'effectuer les opérations en toute sécurité. La responsabilité des vulnérabilités exposées par toute personne accédant au bastion ou à d'autres machines du déploiement (par exemple, la responsabilité du client d'ajouter des plages IP pour autoriser la liste, la responsabilité Citrix de mettre en œuvre correctement les plages IP) est traitée ailleurs dans ce document.

Dans les deux scénarios, Citrix est responsable de la création correcte d'exceptions de pare-feu pour autoriser le trafic RDP. Citrix est également responsable de la révocation de ces exceptions après que le client a supprimé le bastion ou mis fin à l'accès RDP via Citrix DaaS.

Bastions Citrix peut créer des bastions dans le réseau virtuel du client géré par Citrix au sein de l'abonnement du client géré par Citrix pour diagnostiquer et réparer les problèmes, soit de manière proactive (sans notification du client), soit en réponse à un problème signalé par le client. Le bastion est une machine à laquelle le client peut accéder via RDP, puis utiliser pour accéder aux VDA et (pour les catalogues joints à un domaine) Cloud Connector via RDP pour collecter des journaux, redémarrer les services ou effectuer d'autres tâches administratives. Par défaut, la création d'un bastion ouvre une règle de pare-feu externe pour autoriser le trafic RDP depuis une plage d'adresses IP spécifiée par le client vers la machine bastion. Il ouvre également une règle de pare-feu interne pour autoriser l'accès aux Cloud Connector et aux VDA via RDP. L'ouverture de ces règles pose un risque important pour la sécurité.

Le client est responsable de fournir un mot de passe fort utilisé pour le compte Windows local. Le client est également responsable de fournir une plage d'adresses IP externe qui permet un accès RDP au bastion. Si le client choisit de ne pas fournir de plage IP (permettant à quiconque de tenter l'accès RDP), le client est responsable de toute tentative d'accès par des adresses IP malveillantes.

Le client est également responsable de la suppression du bastion une fois le dépannage terminé. L'hôte bastion exposant une surface d'attaque supplémentaire, Citrix arrête automatiquement la machine huit (8) heures après sa mise sous tension. Toutefois, Citrix ne supprime jamais automatiquement un bastion. Si le client choisit d'utiliser le bastion pendant une longue période, il est responsable de l'application des correctifs et des mises à jour. Citrix recommande qu'un bastion ne soit

utilisé que pendant plusieurs jours avant sa suppression. Si le client souhaite utiliser un bastion à jour, il peut supprimer son bastion actuel, puis créer un nouveau bastion, qui fournira à une nouvelle machine les derniers correctifs de sécurité.

Accès RDP Pour les catalogues appartenant à un domaine, si l'appairage de réseaux virtuels du client est fonctionnel, le client peut activer l'accès RDP depuis son réseau virtuel appairé vers son réseau virtuel géré par Citrix. Si le client utilise cette option, il est responsable de l'accès aux VDA et aux Cloud Connector via l'appairage de réseaux virtuels. Des plages d'adresses IP source peuvent être spécifiées afin que l'accès RDP puisse être encore plus restreint, même au sein du réseau interne du client. Le client devra utiliser les informations d'identification du domaine pour se connecter à ces machines. Si le client travaille avec le support Citrix pour résoudre un problème, il peut être nécessaire de partager ces informations d'identification avec le personnel de support. Une fois le problème résolu, le client est responsable de la désactivation de l'accès RDP. Garder l'accès RDP ouvert à partir du réseau appairé ou local du client présente un risque de sécurité.

Informations d'identification du domaine

Si le client choisit d'utiliser un catalogue joint à un domaine, il lui incombe de fournir à Citrix DaaS un compte de domaine (nom d'utilisateur et mot de passe) avec les autorisations nécessaires pour joindre des machines au domaine. Lorsqu'il fournit des informations d'identification de domaine, le client doit respecter les principes de sécurité suivants :

- **Audit :** le compte doit être créé spécifiquement pour l'utilisation de Citrix DaaS de sorte qu'il soit facile d'auditer à quoi sert le compte.
- **Étendue :** le compte nécessite uniquement des autorisations pour joindre des machines à un domaine. Il ne doit pas s'agir d'un administrateur de domaine complet.
- **Sécurité :** Un mot de passe fort doit être placé sur le compte.

Citrix est responsable du stockage sécurisé de ce compte de domaine dans un trousseau de clés Azure dans l'abonnement Azure du client géré par Citrix. Le compte est récupéré uniquement si une opération nécessite le mot de passe du compte de domaine.

Informations supplémentaires

Pour obtenir des informations connexes, voir :

- Guide de déploiement sécurisé pour la plate-forme Citrix Cloud : informations de sécurité pour la plateforme Citrix Cloud.
- Vue d'ensemble de la sécurité technique : informations de sécurité pour Citrix DaaS.
- Avis de tiers

Liste verte des canaux virtuels

May 17, 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`

Méthodes de mise à disposition

May 23, 2022

Une seule méthode de mise à disposition ne répondra probablement pas à tous vos besoins.

Vous pouvez envisager plusieurs méthodes de mise à disposition d'applications. 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, isolés du système d'exploitation et les uns des autres. Cette action permet de résoudre les problèmes de compatibilité. Pour plus d'informations, consultez 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, par exemple) 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. Consultez la section Citrix application 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 Citrix Virtual Apps 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.

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 modifier l'application, offrant une expérience utilisateur cohérente, sécurisée et fiable.
- Les utilisateurs doivent être en ligne pour accéder à leurs applications.

Expérience utilisateur :

- L'utilisateur demande une ou plusieurs applications depuis StoreFront, leur menu Démarrer ou une adresse URL que vous leur 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 cette machine, cette machine 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 sont hébergés, gérés et exécutés en toute sécurité sur les machines de votre datacenter, ce qui fournit une solution de mise à disposition d'applications 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 Personal vDisks 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 aux applications uniquement, un utilisateur peut utiliser plusieurs applications (et ne se limite pas à une seule application). Le système d'exploitation considère chaque application comme une nouvelle session.
- Dans un groupe de mise à disposition, les utilisateurs connectés 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 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 Citrix Virtual Apps, 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 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 unique.) Après la première utilisation, chaque fois qu'un utilisateur ouvre une session sur l'un de ces bureaux, 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 DaaS (anciennement Citrix Virtual Apps and Desktops Service) 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 DaaS 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 DaaS 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.

Pour commencer : Planifier et créer un déploiement

May 17, 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.

Si vous ne connaissez pas les composants, la terminologie et les objets utilisés avec ce service, consultez Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).

Pour un aperçu de l'expérience du client, accédez au Citrix Success Center. Le Success Center fournit des conseils sur les cinq étapes clés de votre expérience avec Citrix : planifier, créer, déployer, gérer et optimiser.

- Les informations du Citrix Success Center viennent compléter cette documentation produit.
- Les articles et guides du Citrix Success Center offrent une perspective globale basée sur les solutions. Ils contiennent également des liens vers des détails spécifiques au service dans cette documentation produit.

Si vous effectuez une migration à partir d'un déploiement Citrix Virtual Apps and Desktops, reportez-vous à Migrer vers le cloud.

> **Important :**
>
> Pour être sûr d'obtenir les informations importantes sur Citrix Cloud et les services Citrix auxquels vous êtes abonné, vérifiez que vous pouvez recevoir toutes les notifications par e-mail.

> Dans le coin supérieur droit de la console Citrix Cloud, développez le menu situé à droite des champs Nom du client et OrgID. Sélectionnez **Paramètres du compte**. Dans l'onglet **Mon profil**, sélectionnez toutes les entrées de la section **Notifications par e-mail**.

Comment utiliser cet article

Pour configurer le déploiement du service Citrix DaaS, effectuez les tâches indiquées ci-dessous. Des liens sont fournis vers les détails de chaque tâche.

Passez en revue l'ensemble du processus avant de commencer le déploiement afin de savoir à quoi vous attendre. Cet article présente également des liens vers d'autres sources d'information utiles.

> **Remarque :**
>
> Si vous prévoyez d'utiliser l'interface de déploiement rapide pour provisionner des machines Microsoft Azure, suivez les instructions d'installation dans Commencer avec Déploiement rapide.

Planifier et préparer

Utilisez les instructions de la section Plan du Success Center pour vous aider à établir des objectifs, à définir des cas d'utilisation, à identifier les risques potentiels et à créer un plan de projet.

Dans la documentation Citrix Tech Zone, consultez un guide de validation de concept étape par étape pour ce service.

S'inscrire

Ouvrez un compte Citrix et demandez une démo du service Citrix DaaS.

Configurer un emplacement de ressources

Un emplacement de ressources contient les ressources requises pour mettre des applications et bureaux à la disposition des utilisateurs. La création d'emplacements de ressources permet au DaaS d'utiliser ces ressources. Pour en savoir plus sur les emplacements de ressources, consultez Se connecter à Citrix Cloud.

Avant de créer des machines, vous devez connecter un emplacement de ressources au DaaS :

- Les machines jointes à un domaine nécessitent l'installation de Cloud Connector dans l'emplacement des ressources. Dans ce cas, vous pouvez :
  - Créer des catalogues joints à Active Directory local

  - Créer des catalogues joints à Azure Active Directory
  - Créer des catalogues joints à Azure Active Directory hybride

  Nous recommandons d'installer deux composants Cloud Connector dans chaque emplacement de ressources pour garantir une haute disponibilité. Voir Installation de Cloud Connector.

  Informations complémentaires :

  - Que sont les emplacements des ressources et les Cloud Connector ?
  - Vidéo sur l'installation de Cloud Connector :

- Les machines qui ne sont pas jointes à un domaine ne nécessitent pas de Cloud Connector, mais vous devez activer Rendezvous V2. Le protocole Rendezvous permet aux VDA de contourner les Cloud Connector pour se connecter directement et en toute sécurité au DaaS. Voir Rendezvous V2. Dans ce cas, vous pouvez :

  - Créer des catalogues non joints à un domaine

Si vous utilisez l'interface Déploiement rapide pour provisionner des machines virtuelles Azure, Citrix crée l'emplacement des ressources et les Cloud Connector pour vous.

Créer une connexion à l'emplacement de ressources

Après avoir ajouté un emplacement de ressources et des Cloud Connector, créez une connexion à l'emplacement de ressources à l'aide de l'interface Configuration complète de Citrix DaaS.

Cette étape n'est pas nécessaire dans l'un ou l'autre des cas suivants :

- Vous créez un déploiement simple de validation de concept.
- Vous utilisez l'interface Déploiement rapide pour provisionner des machines virtuelles Azure.

Informations complémentaires :

- Que sont les hôtes ?
- Que sont les connexions hôtes ?

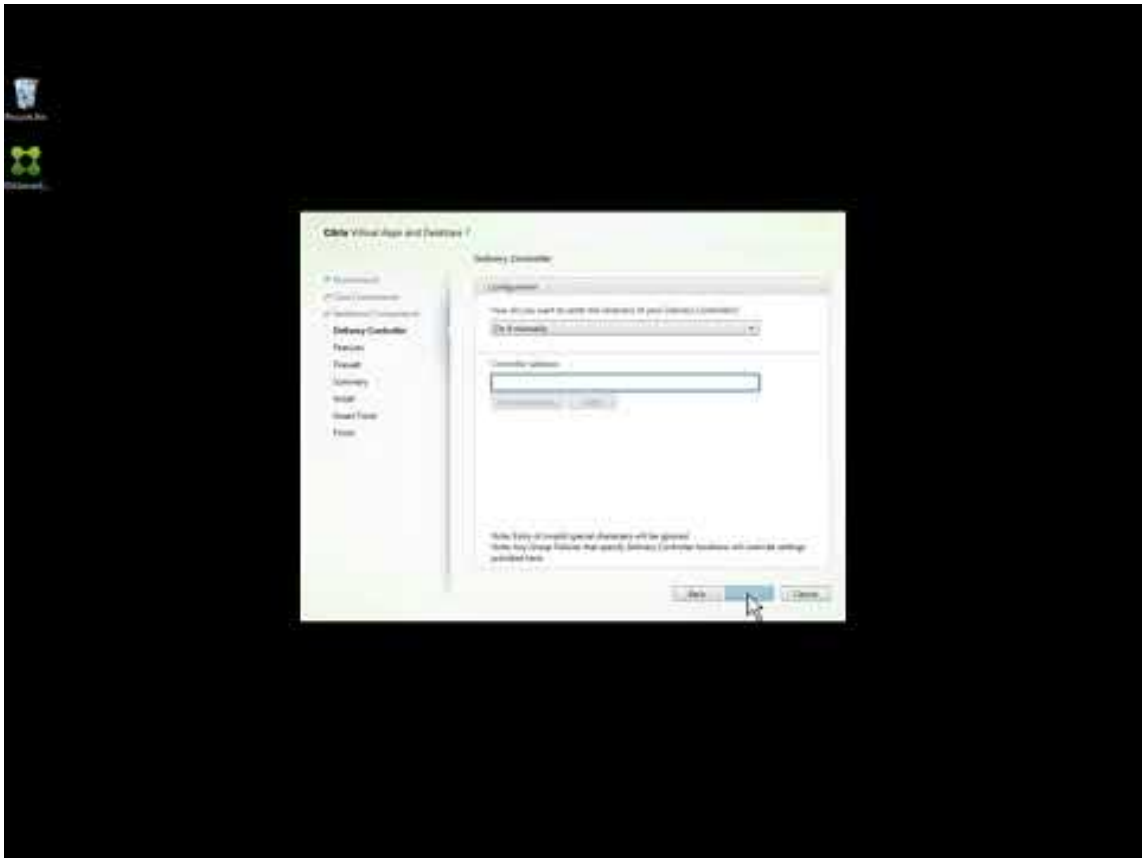
Installer des VDA

Chaque machine qui fournit des applications et des bureaux aux utilisateurs doit être équipée d'un Virtual Delivery Agent (VDA) Citrix.

- Si vous déployez une preuve de concept simple, téléchargez et installez un VDA sur une machine.
- Si vous utilisez une image pour provisionner des machines virtuelles, installez un VDA sur l'image.
- Pour un déploiement Remote PC Access, installez la version principale du VDA pour OS monosession sur chaque PC de bureau physique.

Procédures et informations supplémentaires :

- Que sont les VDA ?
- Préparation de l'installation et instructions
- Installation d'un VDA par ligne de commande
- Vidéo sur le téléchargement et l'installation d'un VDA :

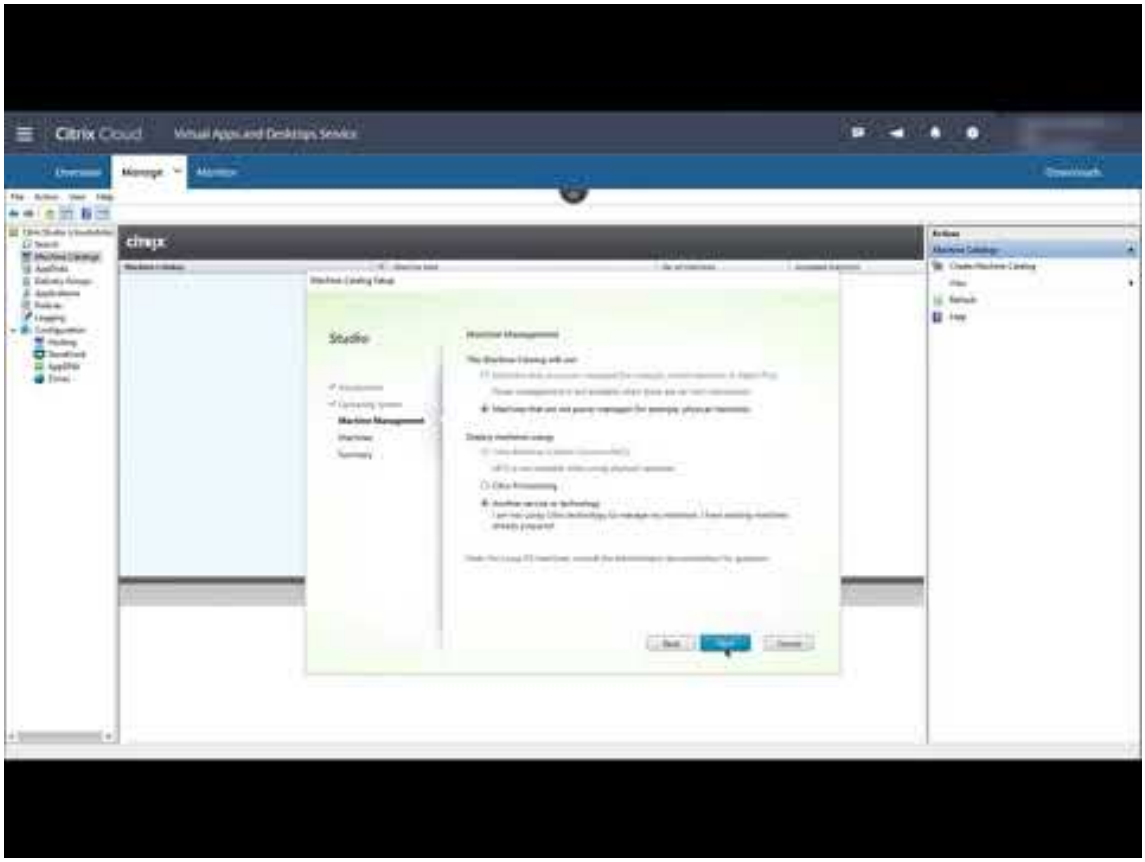


Créer un catalogue

Après avoir créé une connexion à votre emplacement de ressources (si nécessaire), vous créez un catalogue. Si vous utilisez l'interface Configuration complète, le workflow vous guide automatiquement à cette étape.

Procédures et informations supplémentaires :

- Que sont les catalogues ?
- Créer un catalogue
- Utilisez l'interface Déploiement rapide pour déployer un catalogue contenant des machines virtuelles Azure.
- Vidéo sur la création d'un catalogue à l'aide de l'interface de gestion Configuration complète :



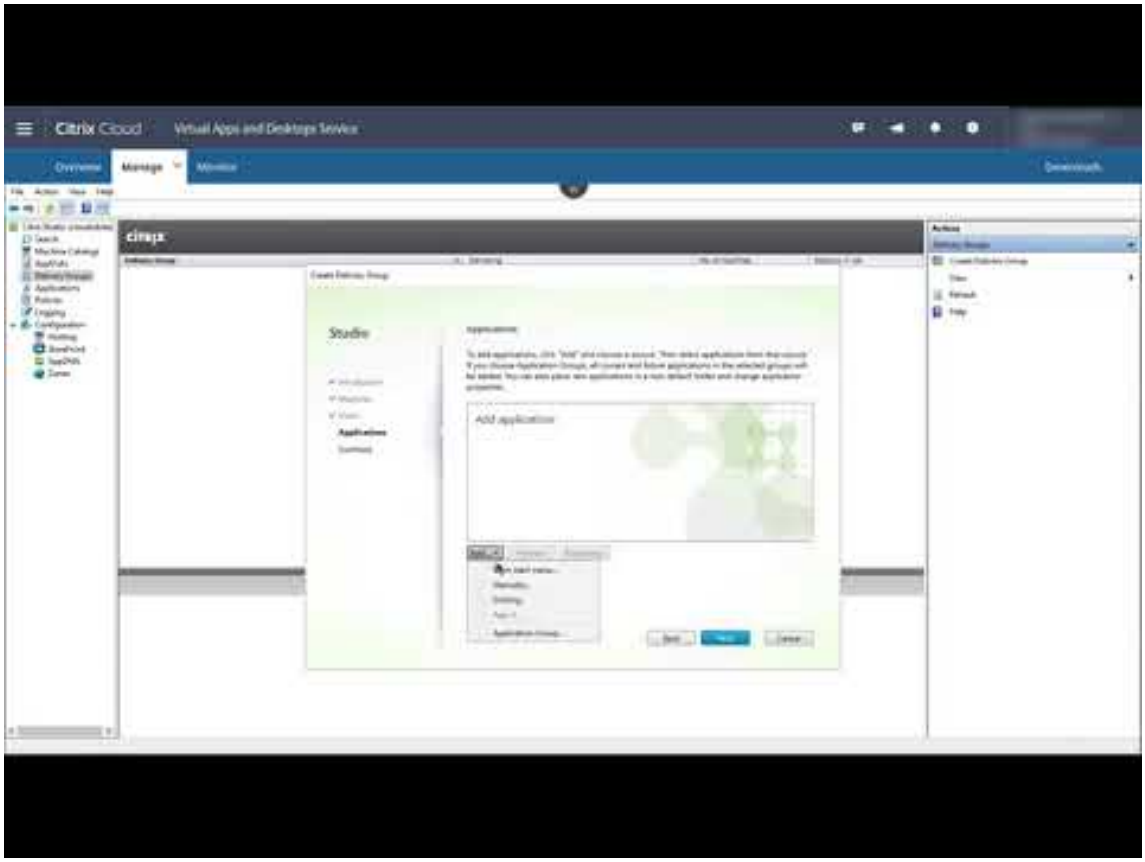
Créer un groupe de mise à disposition

Après la création du premier catalogue, le workflow de **gestion** vous guide dans le processus de création d'un groupe de mise à disposition.

Cette étape n'est pas nécessaire si vous utilisez l'interface Déploiement rapide pour provisionner des machines virtuelles Azure.

Procédures et informations supplémentaires :

- Que sont les groupes de mise à disposition ?
- Créer un groupe de mise à disposition
- Vidéo sur la façon de créer un groupe de mise à disposition :



Déployer d'autres composants et technologies

Après avoir terminé les tâches ci-dessus pour configurer le déploiement Citrix DaaS, suivez les instructions dans la zone Build du Citrix Success Center. Vous trouverez des informations sur le provisionnement et la configuration d'autres composants et technologies dans la solution Citrix, tels que :

- stratégies Citrix
- StoreFront
- App Layering
- Workspace Environment Management (WEM) Service
- Citrix Gateway Service
- Zones
- Service d'authentification fédérée (FAS)

Effectuez les autres tâches qui s'appliquent à votre configuration. Par exemple, si vous prévoyez de fournir des charges de travail Windows Server, configurez un serveur de licences Microsoft RDS.

Lancer des applications et des bureaux

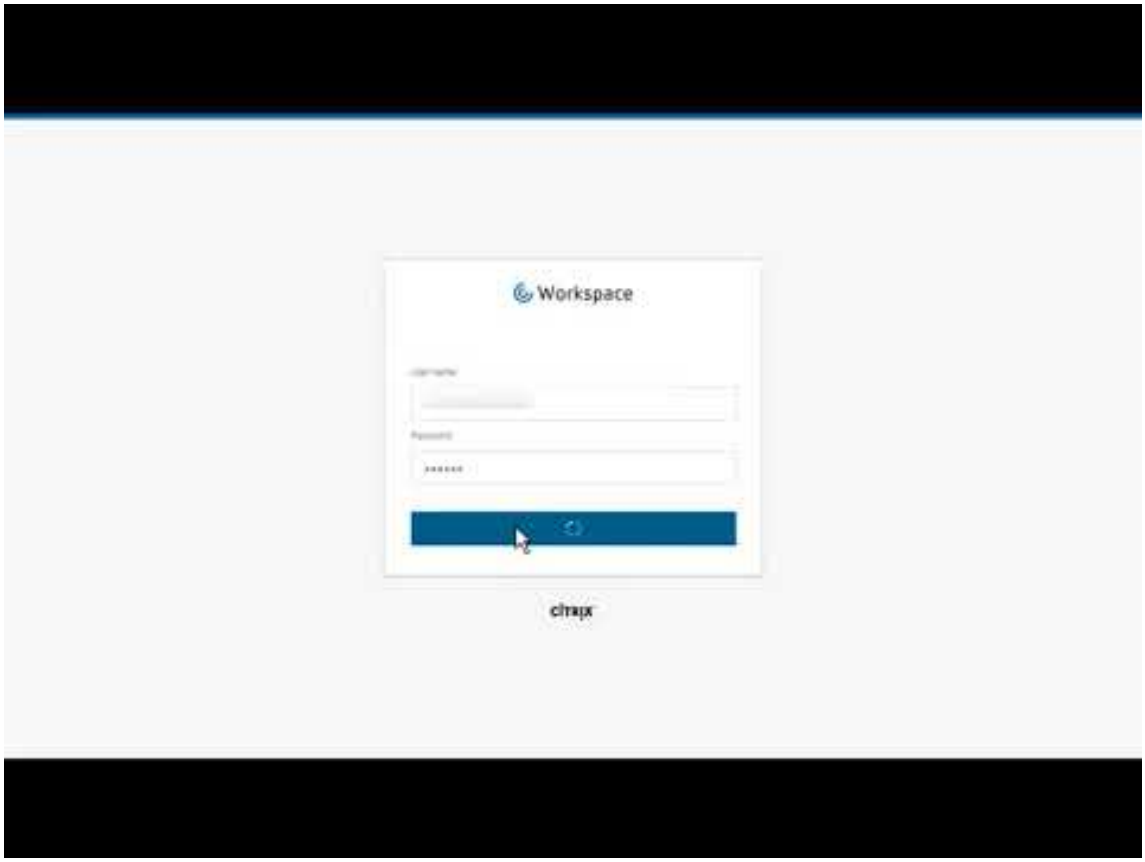
Une fois que vous avez configuré votre déploiement, la publication s'effectue automatiquement. Les applications et bureaux que vous avez configurés sont disponibles pour les utilisateurs dans leur Citrix Workspace. Un utilisateur accède simplement à son URL Workspace et sélectionne une application ou un bureau, qui se lance immédiatement.

Envoyez l'URL Workspace à vos utilisateurs. Vous pouvez trouver l'URL Workspace à deux emplacements :

- Dans la console Citrix Cloud, sélectionnez **Configuration de l'espace de travail** et cliquez sur le menu dans l'angle supérieur gauche. L'onglet **Accès** contient l'URL de l'espace de travail.
- Sur la page **Aperçu** de Citrix DaaS, l'URL de l'espace de travail apparaît au bas de la page.

Informations complémentaires :

- Vidéo sur des utilisateurs qui lancent des applications et des bureaux depuis leur Workspace :



Informations supplémentaires

Citrix Cloud Learning Series propose des cours éducatifs organisés selon votre parcours :

- Si vous débutez avec Citrix DaaS, consultez New to Citrix DaaS Learning Path.
- Si vous effectuez une migration à partir d'un déploiement Citrix Virtual Apps and Desktops, consultez Migrating Citrix DaaS to Citrix Cloud Learning Path.

S'inscrire à Citrix DaaS

July 11, 2023

Introduction

Vous pouvez vous abonner à Citrix DaaS via Citrix ou via Azure Marketplace.

Si vous prévoyez d'utiliser Azure géré par Citrix, vous pouvez également commander Citrix Azure Consumption Fund via Citrix ou sur Azure Marketplace.

- Lorsque vous commandez via Citrix, vous pouvez commander simultanément Citrix DaaS et Citrix Azure Consumption Fund.
- Lorsque vous commandez via Azure Marketplace, vous commandez d'abord Citrix DaaS. Vous pouvez ensuite passer une autre commande pour Citrix Azure Consumption Fund.

Si vous commandez uniquement Citrix DaaS maintenant, vous pouvez commander Citrix Azure Consumption Fund ultérieurement, soit via Azure Marketplace ou votre représentant de compte Citrix.

Démos et essais

Vous pouvez évaluer Citrix DaaS sur demande via Citrix. Vous pouvez convertir un essai en abonnement au service payant.

Lors d'un essai, vous pouvez éventuellement utiliser un abonnement Azure géré par Citrix pour les catalogues, les images et les connexions réseau. Si vous possédez des ressources gérées par Citrix au moment de la conversion en abonnement payant, vous devez soit acheter des unités de consommation, soit supprimer ces ressources gérées par Citrix. Si vous n'achetez pas d'unités de consommation, ces ressources sont automatiquement supprimées, ce qui peut affecter les utilisateurs.

Si vous êtes actuellement abonné à un service Citrix DaaS

En général, un compte Citrix Cloud vous permet de vous abonner à un seul des services Citrix DaaS (ou une édition) à la fois par Citrix OrgID. Par exemple, vous pouvez vous abonner à Citrix DaaS Premium Edition OU Citrix DaaS pour Azure, mais pas aux deux.

Si vous êtes actuellement abonné à un service Citrix DaaS et que vous souhaitez vous abonner à ce service, deux options s'offrent à vous :

- Vous abonner à ce service à l'aide d'un autre compte Citrix Cloud (OrgID).
- Désactiver le service Citrix DaaS que vous avez déjà, puis commander ce service. Vous trouverez des instructions pour la désactivation dans CTX239027.

Commander via Citrix

Vous pouvez commander ce service (et Citrix Azure Consumption Fund) via Citrix Cloud ou par l'intermédiaire de votre représentant de compte Citrix.

Via Citrix Cloud :

- Suivez les instructions de la section Inscription à Citrix Cloud pour obtenir un compte Citrix Cloud et un ID d'organisation.
- Vous pouvez demander une démonstration Citrix DaaS. Dans la vignette Citrix DaaS, cliquez sur **Demander une démo**. Entrez les informations demandées.

  Un représentant Citrix vous contactera pour discuter de vos besoins, de votre environnement et de vos plans. Selon l'évaluation de notre représentant, vous serez autorisé à participer à une démonstration d'administrateur ou à un essai de preuve de concept. Pour de plus amples informations, consultez la section Évaluations de services Citrix Cloud.

Lorsque vous êtes autorisé à effectuer une évaluation, le texte de la vignette Citrix DaaS dans la console Citrix Cloud est remplacé par **Gérer**.

Commander via Azure Marketplace

Vous pouvez commander les offres Citrix suivantes via Azure Marketplace :

- Citrix DaaS pour Azure
- Citrix DaaS Advanced Edition
- Citrix DaaS Premium Edition
- Workspace Premium Plus

Si vous envisagez d'héberger vos charges de travail Citrix Virtual Apps and Desktops sur Microsoft Azure et que vous souhaitez utiliser un abonnement Azure géré par Citrix, commandez Citrix Azure Consumption Fund après avoir commandé Citrix DaaS ou Workspace Premium Plus.

Avec Citrix Azure Consumption Fund, vous êtes facturé chaque mois pour votre consommation, qui peut varier en fonction des ressources d'hébergement que vous choisissez et des heures d'utilisation. Vous pouvez vérifier votre consommation via Citrix Cloud.

Sur Azure Marketplace :

- Vous ne pouvez pas combiner Citrix DaaS et fonds de consommation en une seule commande.
- Le processus de commande pour Citrix Azure Consumption Fund est essentiellement le même que celui de la commande de DaaS, mais vous devez avoir déjà commandé Citrix DaaS.

Conditions requises pour la commande via Azure Marketplace

- L'OrgID de votre compte Citrix Cloud.
  - Si vous possédez un compte Citrix Cloud, mais que vous ne connaissez pas l'OrgID, regardez dans le coin supérieur droit de la console Citrix Cloud. Vous pouvez également consulter l'e-mail que vous avez reçu lorsque vous avez créé le compte.
  - Si vous n'avez pas de compte Citrix Cloud, suivez les instructions de la section S'inscrire à Citrix Cloud.
- Un compte Azure et au moins un abonnement Azure dans ce compte.

Procédure de commande via Azure Marketplace

Suivez cette procédure pour commander un service Citrix DaaS ou Workspace Premium Plus via Azure Marketplace. (Si vous souhaitez utiliser Azure géré par Citrix, passez une autre commande pour Citrix Azure Consumption Fund, après avoir commandé Citrix DaaS.)

1. Connectez-vous à Azure Marketplace à l'aide des informations d'identification de votre compte Azure.
2. Recherchez puis accédez à l'offre Citrix que vous souhaitez commander.
3. Sélectionnez **Obtenir maintenant**.
4. Dans le message **Vous avez presque terminé**, renseignez les informations requises, activez la case du consentement, puis sélectionnez **Continuer**.
5. Consultez les onglets contenant des informations sur le produit, les plans, les prix et l'utilisation. Lorsque vous êtes prêt, sélectionnez un plan (si plusieurs sont disponibles), puis sélectionnez **Configurer + s'abonner**.
6. Dans l'onglet **Fonctions de base** :
   - **Abonnement :** indique le plan que vous avez sélectionné.
   - **Groupe de ressources :** sélectionnez ou créez un groupe de ressources.
   - **Nom :** entrez un nom pour votre commande d'abonnement afin que vous puissiez facilement l'identifier ultérieurement.

- Les informations du **plan** indiquent le prix du plan sélectionné, en fonction de la durée de facturation. Pour modifier la durée du plan, sélectionnez **Modifier le plan**. Sélectionnez la durée souhaitée et sélectionnez **Modifier le plan**.

7. Dans l'onglet **Vérifier + s'abonner**, consultez les informations de contact et mettez-les à jour, si nécessaire. Consultez les informations de base sur l'abonnement. Sélectionnez **S'abonner**.
8. Sur la page **Abonnement en cours**, sélectionnez **Configurer le compte maintenant**. (Si le bouton est désactivé, attendez un instant.) Vous accédez à une page d'activation Citrix.
9. Sur la page d'activation :

   - Utilisez le lien **Connexion** pour vous connecter à Citrix Cloud. Une connexion réussie remplit automatiquement le champ **ID d'organisation**.
   - **Quantité :** entrez le nombre d'utilisateurs. (Une commande initiale doit être d'au moins 25.) Un prix estimé est affiché.
   - Acceptez les conditions générales, puis sélectionnez **Activer la commande**.

Après avoir commandé via Azure Marketplace

Citrix vous envoie un e-mail lorsque votre service est provisionné. Le provisionnement peut prendre un certain temps. Si vous ne recevez pas l'e-mail le jour suivant, contactez l'assistance Citrix. Lorsque vous recevez l'e-mail de Citrix, vous pouvez commencer à utiliser Citrix DaaS.

Le traitement d'une commande Citrix Azure Consumption Fund ne prend pas beaucoup de temps. Lorsque Citrix est averti de la commande, une bannière apparaît dans la console Citrix DaaS, indiquant qu'un abonnement Azure géré par Citrix va être préparé pour vous.

Ne supprimez pas la ressource Citrix DaaS dans Azure. La suppression de cette ressource annule votre abonnement.

Commande via Google Cloud Marketplace

Vous pouvez commander les offres Citrix suivantes via Google Cloud Marketplace :

- Citrix DaaS Standard pour Google Cloud
- Citrix DaaS Premium pour Google Cloud

Pour commander des offres via Google Cloud Marketplace, vous devez disposer des éléments suivants :

- L'OrgID de votre compte Citrix Cloud.

  - Si vous possédez un compte Citrix Cloud, mais que vous ne connaissez pas l'OrgID, regardez dans le coin supérieur droit de la console Citrix Cloud. Vous pouvez également consulter l'e-mail que vous avez reçu lorsque vous avez créé le compte.
  - Si vous n'avez pas de compte Citrix Cloud, suivez les instructions de la section S'inscrire à Citrix Cloud.

- Un compte Google Cloud et au moins un abonnement Google Cloud associé à ce compte.

Pour passer la commande :

1. Connectez-vous à Google Cloud Marketplace.
2. Suivez les instructions de la page Citrix DaaS pour Google Cloud pour effectuer votre achat.

Citrix vous envoie un e-mail lorsque votre service est provisionné. Le provisionnement peut prendre un certain temps. Si vous ne recevez pas l'e-mail le jour suivant, contactez l'assistance Citrix. Lorsque vous recevez l'e-mail de Citrix, vous pouvez commencer à utiliser Citrix DaaS.

Ne supprimez pas la ressource Citrix DaaS dans Google Cloud. La suppression de cette ressource annule votre abonnement.

Prochaine étape

Une fois votre commande traitée, passez aux étapes suivantes de la section Planifier et créer un déploiement.

Par exemple :

- Si vous n'avez pas encore configuré votre hyperviseur ou votre service de cloud, ou Active Directory, consultez la section Configurer un emplacement de ressources.
- Si votre environnement hôte et Active Directory sont déjà configurés, consultez la section Créer une connexion.

Citrix HDX Plus pour Windows 365

April 18, 2024

Citrix HDX Plus pour Windows 365 vous permet d'intégrer Citrix Cloud à Windows 365 afin d'utiliser les technologies Citrix HDX pour une expérience Windows 365 Cloud PC améliorée et plus sécurisée, en plus des autres services Citrix Cloud pour une gestion améliorée.

Pour plus d'informations, consultez Citrix HDX Plus pour Windows 365

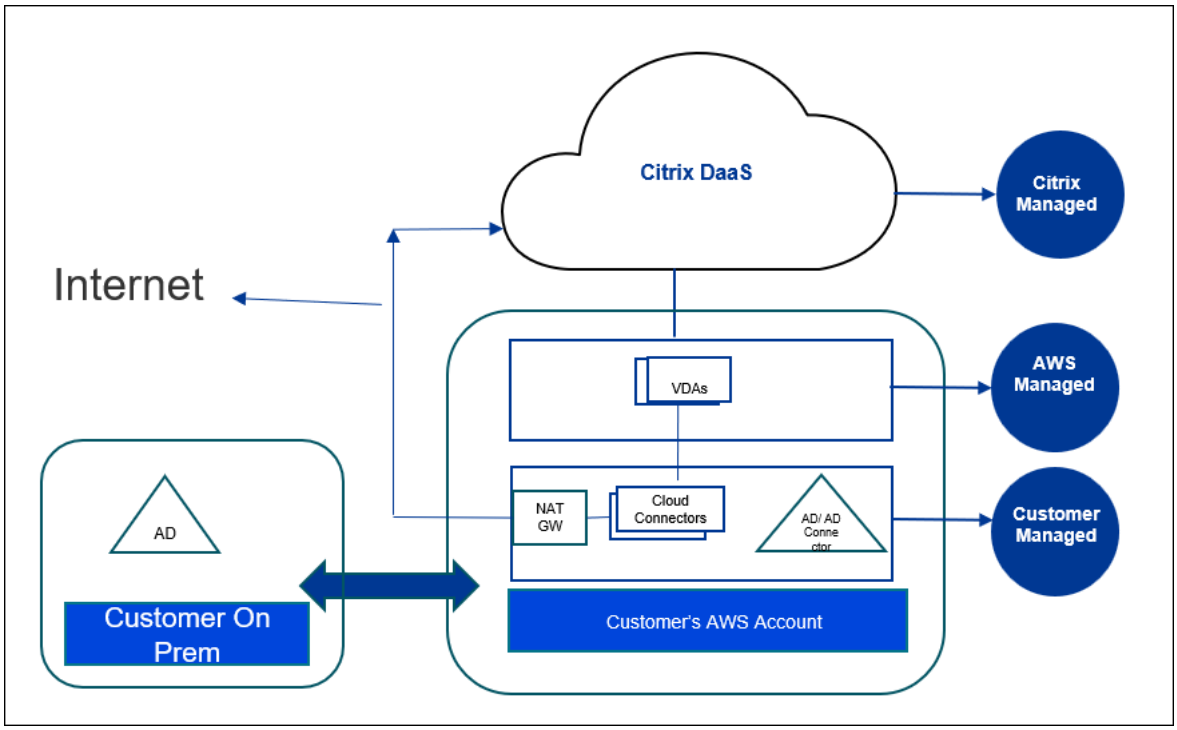
Citrix DaaS pour Amazon WorkSpaces Core (Technical Preview)

May 17, 2024

Introduction

Cet article explique comment préparer et créer un déploiement avec Citrix pour Amazon WorkSpaces Core. Amazon WorkSpaces Core est hébergé par Amazon Web Services (AWS).

Voici la représentation de la mise en œuvre d'AWS et de sa gestion avec Citrix DaaS :



À propos de la version Technical Preview

- Pour obtenir de l'aide pendant l'utilisation de cette version Technical Preview, contactez le support AWS ou Citrix.
- Pour gérer l'environnement Citrix au cours de cette évaluation, utilisez uniquement la console de **gestion** de Citrix DaaS. Aucune API Citrix ou AWS n'est prise en charge dans cette version Technical Preview. (Citrix apprécie vos commentaires sur les API que vous souhaitez utiliser à l'avenir.)

Préparer et créer un déploiement

La liste de contrôle de déploiement de l'interface **Déploiement rapide** contient des liens vers les procédures 1 à 5.

1. Avant de commencer, vérifiez que les pré-requis sont remplis dans Citrix Cloud et AWS.
2. Créez un emplacement de ressources dans Citrix Cloud. (Cette procédure est également incluse comme pré-requis.)
3. Connectez votre compte AWS. Cette procédure active les autorisations afin que Citrix DaaS puisse se connecter à AWS.
4. Créez une connexion à un annuaire. Cette procédure configure une connexion qui permet d'accéder à l'annuaire Active Directory de votre organisation.
5. Importez une image. Cette procédure vous permet de créer une expérience de bureau pour vos utilisateurs.
6. Créer un déploiement. Cette procédure spécifie les machines à déployer et les utilisateurs qui peuvent y accéder via Citrix Workspace.

Avant de commencer

Assurez-vous d'avoir effectué les tâches suivantes avant de commencer à préparer et à créer votre déploiement.

Il existe une exception : la création d'un emplacement de ressources dans Citrix Cloud est répertoriée comme un pré-requis. Il s'agit également de la première procédure de la liste de contrôle du déploiement. Ainsi, si vous créez l'emplacement de ressources dans le cadre des pré-requis, ignorez cette procédure dans la séquence de la liste de contrôle. De même, effectuez cette procédure dans la liste de contrôle si vous ne l'avez pas déjà fait.

Pré-requis à remplir dans Citrix Cloud

- Créez un compte Citrix Cloud et abonnez-vous à Citrix DaaS. Votre représentant Citrix peut vous aider à ce sujet. Il active également la version Technical Preview pour vous.
- Créez un emplacement de ressources Citrix Cloud. (Cette procédure est également liée à l'interface Déploiement rapide.)

Pré-requis à remplir dans AWS

- Créez un compte utilisateur AWS. Le compte doit disposer des éléments suivants :
  - Autorisations de rôle pour le client d'API Citrix.

  - Autorisations pour l'accès par programmation. Pour plus d'informations, consultez la section Autorisations d'accès par programmation aux comptes AWS.
  - Créez le rôle workspaces_DefaultRole. Pour plus d'informations, consultez la page Création du rôle workspaces_DefaultRole.

- Dans votre annuaire Active Directory :

  - Utilisez l'option de connecteur AD pour stocker et gérer les informations. Pour plus de détails, consultez la page sur le connecteur AD.
  - Créez une unité d'organisation dans laquelle les machines virtuelles sont créées. Cette unité d'organisation doit disposer d'une stratégie Citrix pour communiquer avec les instances de Cloud Connector et Citrix Cloud. Pour plus d'informations, consultez la section Référence.
  - Configurez une stratégie de groupe pour la configuration de Citrix Cloud Connector :
    1. Téléchargez la dernière console de gestion des stratégies de groupe fournie par Citrix (CitrixGroupPolicyManagement_64.msi) depuis le site de téléchargement de Citrix.
    2. Installez le MSI (l'environnement d'exécution Visual Studio 2015 doit être installé sur cette machine). Créez ensuite une stratégie Citrix contenant le paramètre de stratégie Controller. Ce paramètre spécifie les adresses de Cloud Connector.

- Créez ou utilisez une passerelle NAT existante. Pour plus d'informations, consultez la section Passerelle NAT.

- Créez ou utilisez un ou plusieurs groupes de sécurité existants qui permettent aux instances de Citrix Cloud Connector de communiquer avec les machines virtuelles déployées. Pour plus d'informations, reportez-vous à la page Contrôler le trafic vers vos ressources AWS à l'aide de groupes de sécurité

- Ouvrez un ticket auprès du support AWS pour activer la fonctionnalité BYOL sur votre compte. Pour commencer, contactez votre gestionnaire de compte ou votre représentant commercial AWS, ou contactez le centre de support AWS. Votre contact vérifiera et activera la fonctionnalité BYOL. Pour plus d'informations, consultez la page Activez BYOL pour votre compte BYOL à l'aide de la console Amazon WorkSpaces.

  > **Remarque :**
  >
  > Les versions Windows 10 N et Windows 11 N ne sont pas prises en charge pour la fonctionnalité BYOL actuellement.

  - L'utilisation de la fonctionnalité Citrix DaaS pour Amazon WorkSpaces Core activera automatiquement la fonctionnalité BYOP (Bring Your Own Protocol) dans AWS WorkSpaces Core.
  - Vérifiez que vous disposez d'un nombre de licences Windows 10 suffisant pour les bureaux qui seront créés. Pour plus d'informations, consultez la section Apportez votre propre licence (BYOL) de bureau Windows.

Préparation générale

Examinez chaque procédure avant de commencer. Avantage : cela facilitera la réalisation des processus.

Créer un emplacement de ressources

Vous créez un emplacement de ressources dans Citrix Cloud.

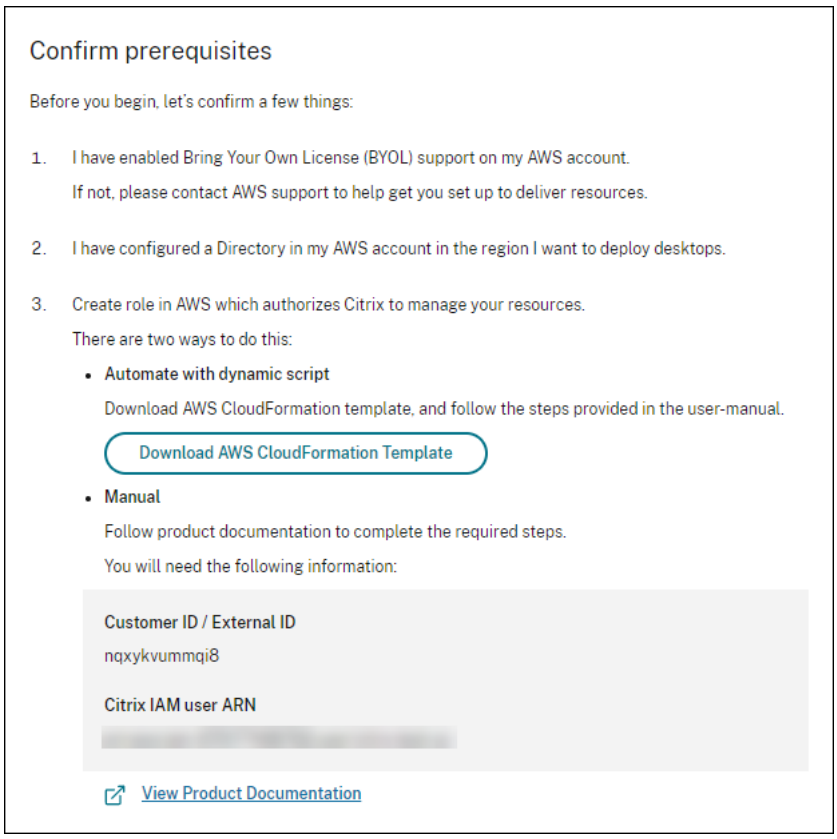
- Un emplacement de ressources contient au moins deux Cloud Connector qui communiquent avec Citrix Cloud. Les serveurs sur lesquels vous installez les Cloud Connector doivent se trouver dans un VPC EC2, être rattachés à un domaine et disposer d'une connectivité Internet. Les Cloud Connector doivent se trouver dans le même VPC que l'annuaire que vous prévoyez d'utiliser.
- Pour plus d'informations sur les Cloud Connector, consultez Citrix Cloud Connector et découvrez comment les provisionner.
- L'emplacement des ressources peut également contenir vos serveurs Active Directory. Pour plus d'informations, consultez la section Connecter Active Directory à Citrix Cloud.

Connecter le compte AWS

Cette procédure autorise Citrix DaaS à se connecter à AWS.

Pour créer AssumeRole pour AWS WorkSpaces Core, procédez comme suit :

1. Dans Citrix DaaS, sous **Gérer > Déploiement rapide > Comptes**, cliquez sur **Connecter le compte**.
2. Sur la page **Connecter un compte AWS**, sous **Confirmer les pré-requis**, cliquez sur **Télécharger le modèle AWS CloudFormation**. Une fois le modèle téléchargé, cliquez sur **Suivant**.



1. Pour charger le modèle, consultez la section Créer un AssumeRole pour l'intégration d'AWS Workspaces Core.
2. Sur la page **Authentifier le compte**, ajoutez le **nom de ressource Amazon** (ARN) généré dans le champ **ID de rôle**, saisissez un nom dans le champ **Nom**, puis cliquez sur **Suivant**. La page **Choisir une région** s'ouvre.

   L'**ID de rôle** correspond à l'ARN du rôle qui autorise Citrix à gérer les ressources. L'ID de rôle se trouve dans la console AWS Management Console en accédant à **IAM > Rôles**.

   Si vous utilisez le script `CloudFormation`, accédez à CloudFormation, puis cliquez sur la pile correspondante utilisée pour créer le rôle. Accédez à l'onglet **Ressources**, puis cliquez sur la ressource avec LogicalID `CitrixAssumeRole`.

   > **Remarque :**
   >
   > Vous ne pouvez pas connecter deux comptes dans la même région pour le même compte AWS.

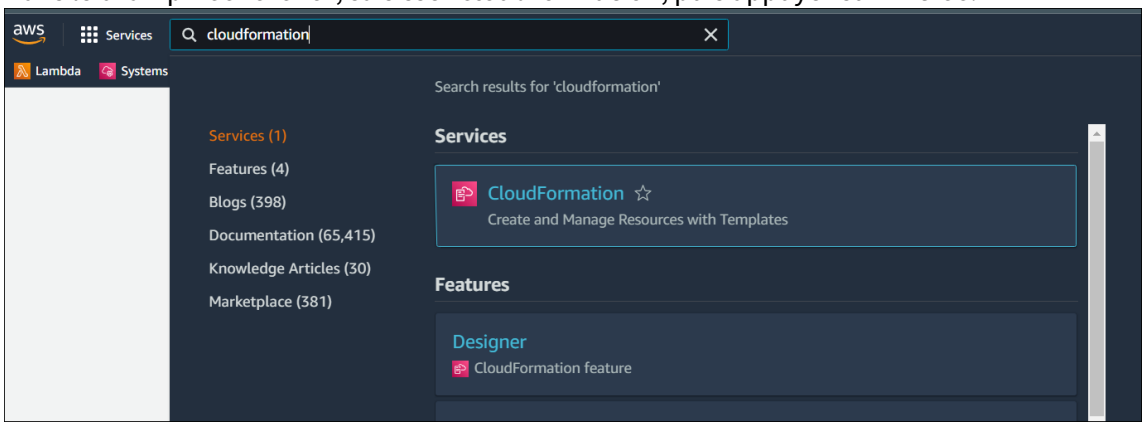
3. Sur la page **Choisir une région**, sélectionnez la région dans laquelle vous souhaitez déployer vos bureaux, puis cliquez sur **Suivant**.
4. Sur la page **Configurer prise en charge de BYOL**, pour configurer la prise en charge de BYOL, une interface réseau de gestion connectée à un réseau Amazon sécurisé est requise. Sélec-

tionnez une plage d'adresses IP dans laquelle rechercher une interface à utiliser. Sélectionnez ensuite Afficher les blocs CIDR disponibles. Si des blocs CIDR sont disponibles dans la plage de recherche sélectionnée, sélectionnez un bloc CIDR disponible. Un message vous confirme lorsque vous avez sélectionné une plage d'adresses de recherche et un bloc CIDR disponible. Cliquez sur **Suivant**.

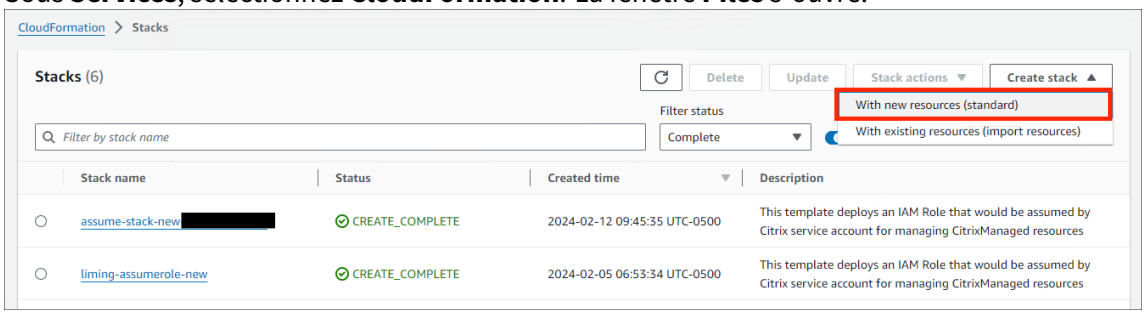
5. Dans la page **Résumé**, vérifiez les informations que vous avez spécifiées. Vous pouvez revenir aux pages précédentes. Lorsque vous avez terminé, cliquez sur **Terminer**.
   Le processus de connexion peut prendre plusieurs heures.

Créer un AssumeRole pour l'intégration d'AWS Workspaces Core

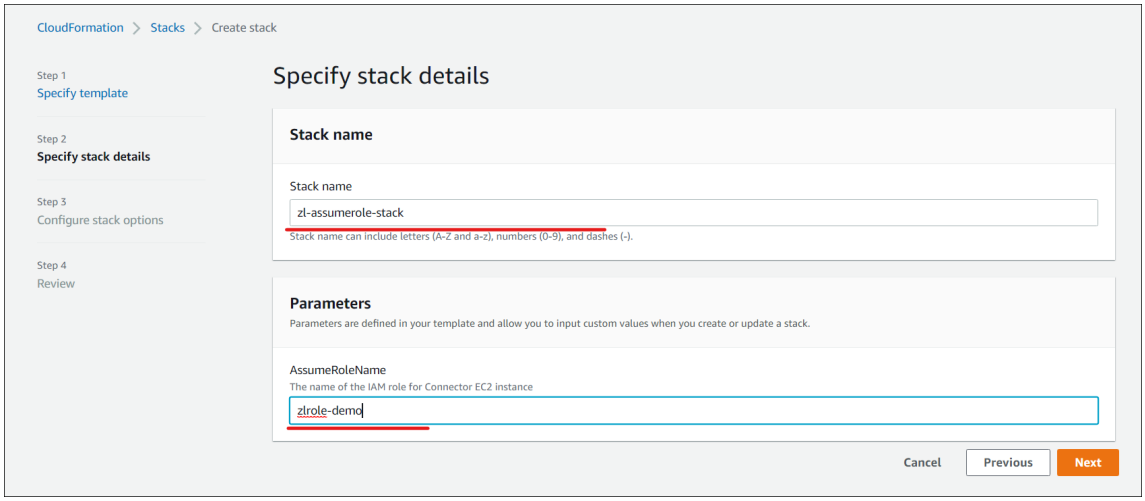
1. Dans la fenêtre de votre navigateur, ouvrez le site Web **Amazon Web Services** et connectez-vous.
2. Dans le champ **Rechercher**, saisissez **cloudformation**, puis appuyez sur **Entrée**.



3. Sous **Services**, sélectionnez **CloudFormation**. La fenêtre **Piles** s'ouvre.

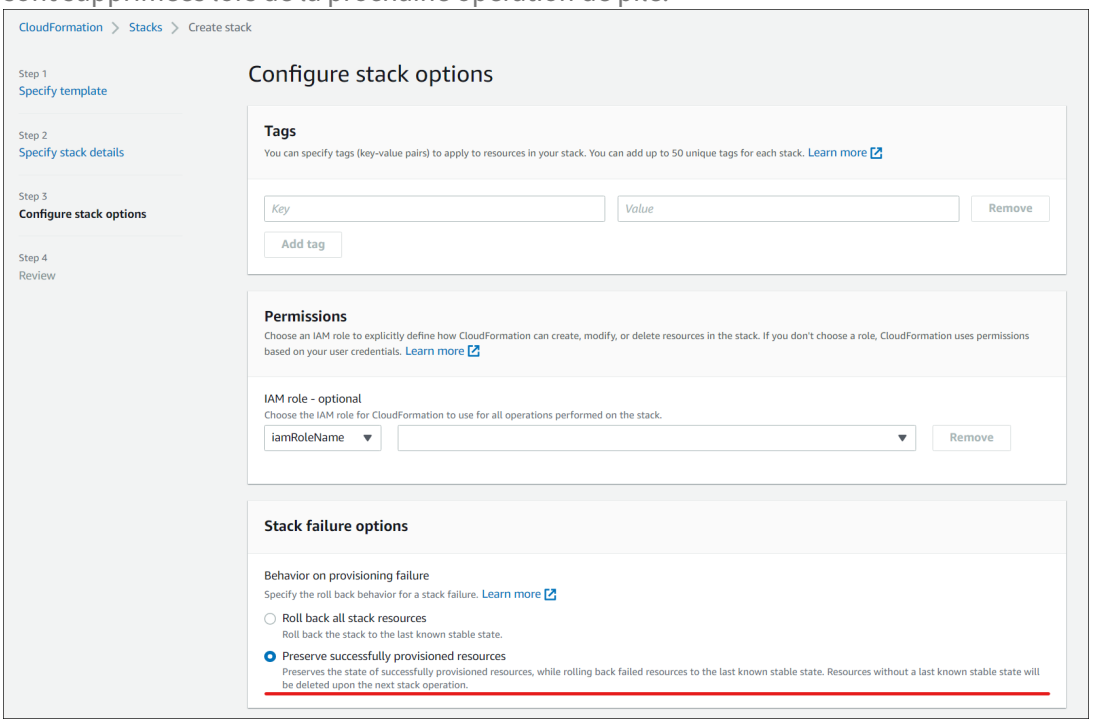


4. Cliquez sur **Créer une pile > Avec de nouvelles ressources (standard)** dans le coin supérieur droit. La fenêtre **Créer une pile** s'ouvre.
   a) Sous **Pré-requis —Préparer le modèle**, sélectionnez **Le modèle est prêt**.
   b) Sous **Spécifier le modèle**, cliquez sur **Charger un fichier modèle > Choisir un fichier**, puis cliquez sur **Suivant**. Le panneau **Spécifier les détails de la pile** s'ouvre.
5. Dans le panneau **Spécifier les détails de la pile**, indiquez un **nom de pile** et un **AssumeRole-Name**, puis cliquez sur **Suivant**. Le panneau **Configurer les options de pile** s'ouvre.

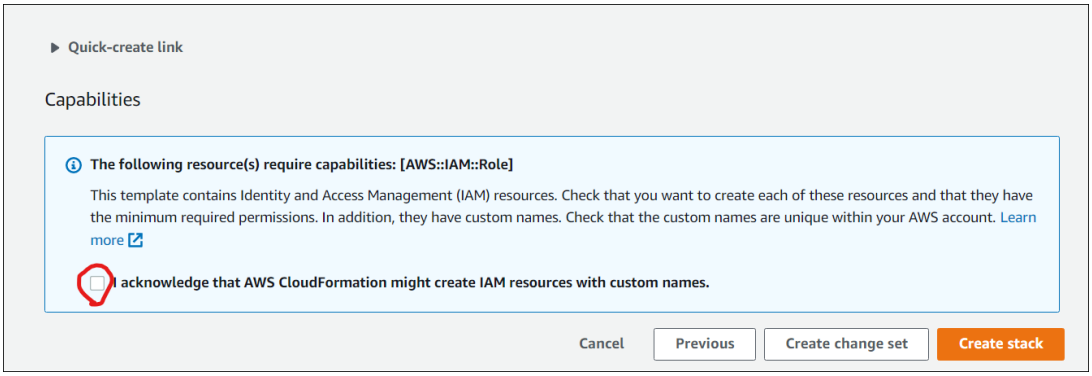


Remarque :

- Dans le panneau **Configurer les options de pile**, sélectionnez l'option **Conserver les ressources correctement provisionnées**. Cette option conserve l'état des ressources correctement provisionnées. Les ressources dont le dernier état stable n'est pas connu sont supprimées lors de la prochaine opération de pile.

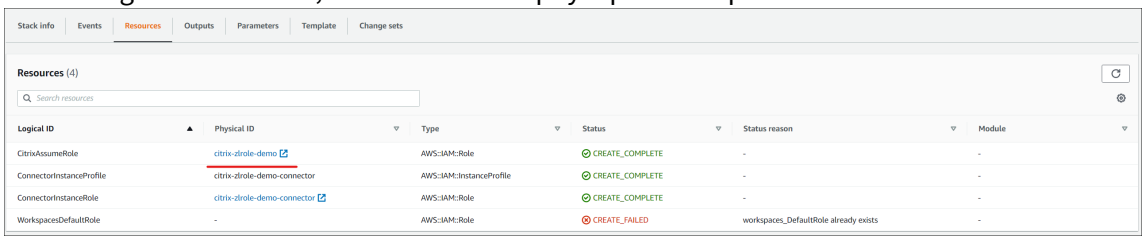


- Dans la fenêtre contextuelle **Fonctionnalités**, cochez la case **Je reconnais qu'AWS CloudFormation peut créer des ressources IAM avec des noms personnalisés**, puis cliquez sur **Créer une pile**.

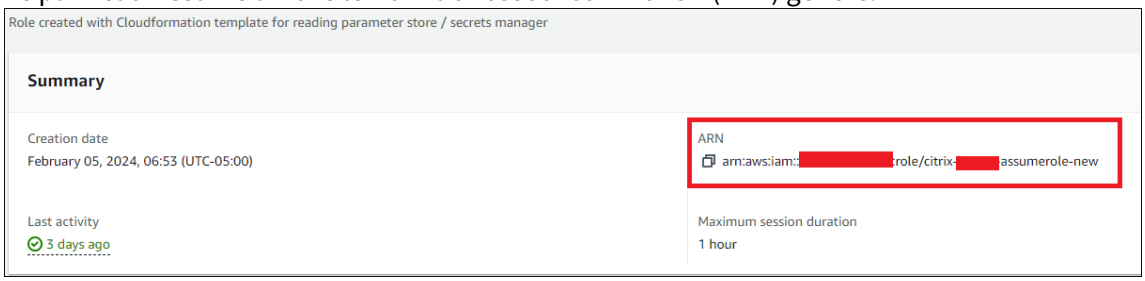


La création de la pile peut échouer à la fin, car **Workspace_DefaultRole** a déjà été créé. Cela n'affecte pas la création d'**AssumeRole**.

1. L'onglet **Événements** indique l'état de la pile créée.
2. Dans l'onglet **Ressources**, sélectionnez l'ID physique correspondant à l'**AssumeRole** créé.



3. Le panneau Résumé affiche le **nom de ressource Amazon** (ARN) généré.



4. Reprenez la procédure à partir de l'étape 4 dans Connecter un compte AWS

Créer une connexion à un annuaire

> **Remarque :**
>
> Désenregistrez votre répertoire AWS au début de cette étape. Une fois que vous avez créé une connexion à un répertoire avec Citrix DaaS, le répertoire sélectionné est enregistré pour créer des espaces de travail Amazon avec Citrix DaaS.

Cette procédure crée une connexion qui permet d'accéder au répertoire Active Directory de votre organisation.

Logiciels requis :

- Un emplacement de ressources contenant deux Cloud Connector.

- Un groupe de sécurité.
- Une unité d'organisation dans votre annuaire Active Directory.

Pour plus de détails sur les pré-requis, consultez la section Avant de commencer.

Vous pouvez démarrer cette procédure à partir de l'un des deux emplacements suivants :

- Un lien sur la liste de contrôle de démarrage.
- Dans la console DaaS **Gérer**, sélectionnez **Déploiement rapide** dans le panneau gauche, puis **Connexions d'annuaire** dans la section **Amazon WorkSpaces Core**. Sélectionnez ensuite **Créer connexion d'annuaire**.

Suivez la séquence **Créer connexion d'annuaire** :

1. **Confirmer les pré-requis :** si les conditions liées aux pré-requis sont remplies, cliquez sur **Suivant**.
2. **Connecter annuaire :** sélectionnez l'emplacement des ressources, le compte et l'annuaire. (Le compte sélectionné doit avoir au moins un annuaire.)
    - Sélectionnez deux sous-réseaux dans lesquels les ordinateurs de bureau seront déployés. Les sous-réseaux doivent se trouver dans des zones de disponibilité appropriées.
    - Spécifiez un nom convivial pour cette connexion.
    - Lorsque vous avez terminé, cliquez sur **Suivant**.
3. **Paramètres de la machine virtuelle :** les paramètres que vous sélectionnez s'appliquent à toutes les machines virtuelles qui utilisent cette connexion à un annuaire.
    - L'unité d'organisation sélectionnée doit correspondre à l'unité d'organisation ciblée par la stratégie de groupe Citrix.
    - Sélectionnez un groupe de sécurité.
    - Indiquez si vous souhaitez accorder des privilèges d'administrateur à chaque utilisateur affecté aux machines virtuelles.

Importer une image

Cette procédure vous permet de créer une expérience de bureau pour vos utilisateurs.

Pré-requis pour importer l'image :

- Il doit s'agir d'une image EC2.
- Un Citrix Virtual Delivery Agent (VDA) doit être installé.
- Elle doit être préparée pour BYOL. Un script BYOL est disponible à l'adresse suivante : BYOLChecker.zip.

Pour importer l'image, procédez comme suit :

1. **Confirmer les pré-requis :** après les étapes relatives aux pré-requis, cliquez sur **Suivant**. (Si vous n'avez pas préparé l'image pour BYOL, vous pouvez télécharger le script à partir de cette page.) Pour plus d'informations, consultez la section Exigences.
2. **Choisissez une image** et donnez-lui un nom convivial. Sélectionnez le compte et l'AMI, puis ajoutez une description. Cliquez sur **Suivant**. La page **Résumé** s'ouvre.
3. Sur la page **Résumé**, vérifiez les informations que vous avez fournies. Après vérification, sélectionnez **Importer une image**.

   > **Remarque :**
   >
   > L'importation d'une image peut prendre plusieurs heures.

Intégrer une image Microsoft Office 2019 lors de l'importation d'une image

Pour intégrer une image Microsoft Office 2019 lors de l'importation d'une image :

1. Dans **Web Studio > Déploiement rapide**, cliquez sur **Images**.
2. Dans **Mes images**, cliquez sur **Importer une image**.
3. Dans **Importer une image > Pré-requis**, cliquez sur **Suivant : Choisissez une image**.
4. Dans **Importer une image > Choisir une image :**
   - Sélectionnez un compte dans la liste déroulante **Compte**.
   - Sélectionnez une AMI dans la liste déroulante **AMI**.
   - Entrez le nom de l'image dans le champ **Nom**.
   - Sélectionnez l'option **Inclure Microsoft Office 2019 Professionnel Plus** dans l'image.
   - Entrez une description dans le champ **Description**.
5. Dans **Importer une image > Choisir une image**, cliquez sur **Suivant : résumé**.
6. Dans **Choisir une image > Résumé**, assurez-vous que **Sélectionné** s'affiche pour **Microsoft Office 2019**.
7. Dans **Mes images**, cliquez sur **Importer une image**.
   L'état de l'image récemment déployée affiche **Importation** jusqu'à la fin de l'opération d'importation.
8. Dans **Mes images**, sélectionnez l'image récemment déployée, puis cliquez sur **Afficher les détails**.
9. Dans le panneau **Détails**, le champ **Microsoft Office 2019** affiche la mention **Inclus**.

> **Remarque :**
>
> Seules les versions suivantes du système d'exploitation sont compatibles :
>
> - Windows 10 version 21H2 (mise à jour de décembre 2021)
> - Windows 10 version 22H2 (mise à jour de novembre 2022)

> - Windows 10 Entreprise LTSC 2019 (1809) (1809)
> - Windows 10 Entreprise LTSC 2021 (21H2) (21H2)
> - Windows 11 version 22H2 (version d'octobre 2022)

Créer un déploiement

Un déploiement est un groupe de bureaux auxquels les utilisateurs peuvent accéder depuis leur Citrix Workspace. Cette procédure spécifie les caractéristiques des machines virtuelles à déployer en tant que bureaux et les utilisateurs AD qui peuvent les utiliser.

Logiciels requis

Effectuez toutes les étapes répertoriées dans la section Préparer et créer un déploiement.

1. Dans **Web Studio > Déploiement rapide**, cliquez sur **Déploiements** dans la colonne **Amazon Web Services**. Cliquez sur **Créer un déploiement**.
2. **Nom et connexion :** entrez un nom convivial pour ce groupe de machines. Ce nom doit être unique. Sélectionnez une connexion à un annuaire, puis cliquez sur **Suivant : Image et performances**.
3. **Image et performances :** sélectionnez le système d'exploitation et les performances pour les machines. Spécifiez la taille par défaut pour le volume racine et le volume utilisateur.
   Vous ne pouvez pas modifier la taille du volume après avoir lancé un bureau de ce groupe. Spécifiez donc la taille maximale dont vous pensez avoir besoin. Vous pouvez également spécifier ces tailles par utilisateur sur la page suivante. Cliquez sur **Suivant** : Utilisateurs.
4. **Utilisateurs :** recherchez et sélectionnez les utilisateurs qui seront autorisés à accéder aux bureaux.
   Si vous souhaitez personnaliser les tailles de volume pour un utilisateur, sélectionnez **Modifier les tailles des volumes racine et utilisateur**, puis spécifiez les tailles. Cliquez sur **Suivant : résumé**.
5. **Résumé :** vérifiez les informations fournies, puis cliquez sur **Créer déploiement**.

Intégrer les applications Microsoft 365 Windows

Pour intégrer les applications Microsoft 365, consultez les pages Microsoft 365 Apps for Enterprise désormais disponibles sur les services Amazon WorkSpaces et Microsoft 365 Bring Your Own License (BYOL).

Gérer des machines dans un déploiement

Outre les fonctionnalités de gestion des machines décrites dans la section Gérer des catalogues de machines, pour certaines actions, vous pouvez sélectionner les machines à gérer à partir d'un dé-

ploiement.

Pour gérer les machines dans un déploiement :

1. Dans **Web Studio > Déploiement rapide**, sélectionnez **Déploiements**.
2. Dans le panneau **Déploiements**, sélectionnez le déploiement contenant les machines que vous souhaitez gérer.
3. Cliquez sur **Afficher les détails**.
4. Dans le panneau **Détails du déploiement**, sélectionnez la machine que vous souhaitez gérer.
5. Dans les actions affichées, sélectionnez l'action que vous souhaitez effectuer sur la machine :

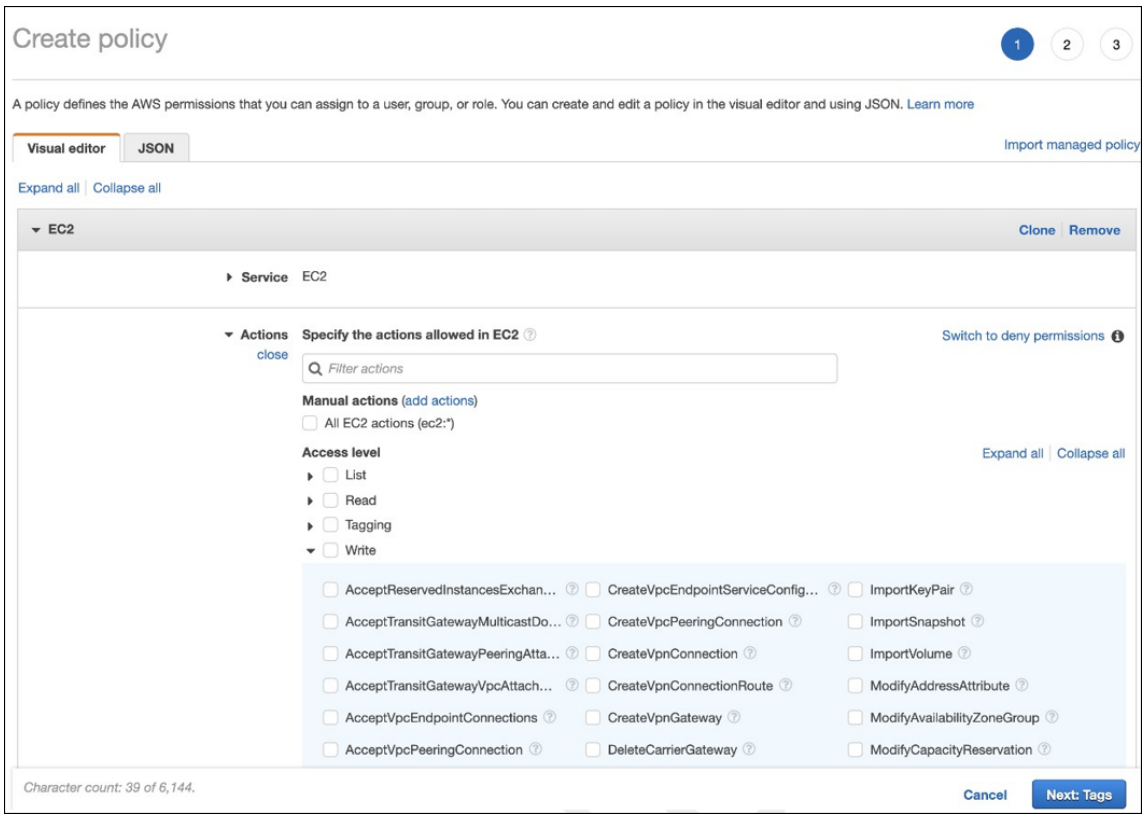
- Cliquez sur **Modifier la taille du volume** pour modifier la taille du volume de la machine.
- Cliquez sur **Supprimer** pour supprimer la machine du déploiement et d'AWS. Si une machine fait partie d'un groupe de mise à disposition, elle ne peut être supprimée que si elle est en mode de maintenance.
- Cliquez sur **Activer/désactiver le mode de maintenance** pour activer le mode de maintenance (s'il est désactivé) ou le désactiver (s'il est activé) pour la machine.

Référence

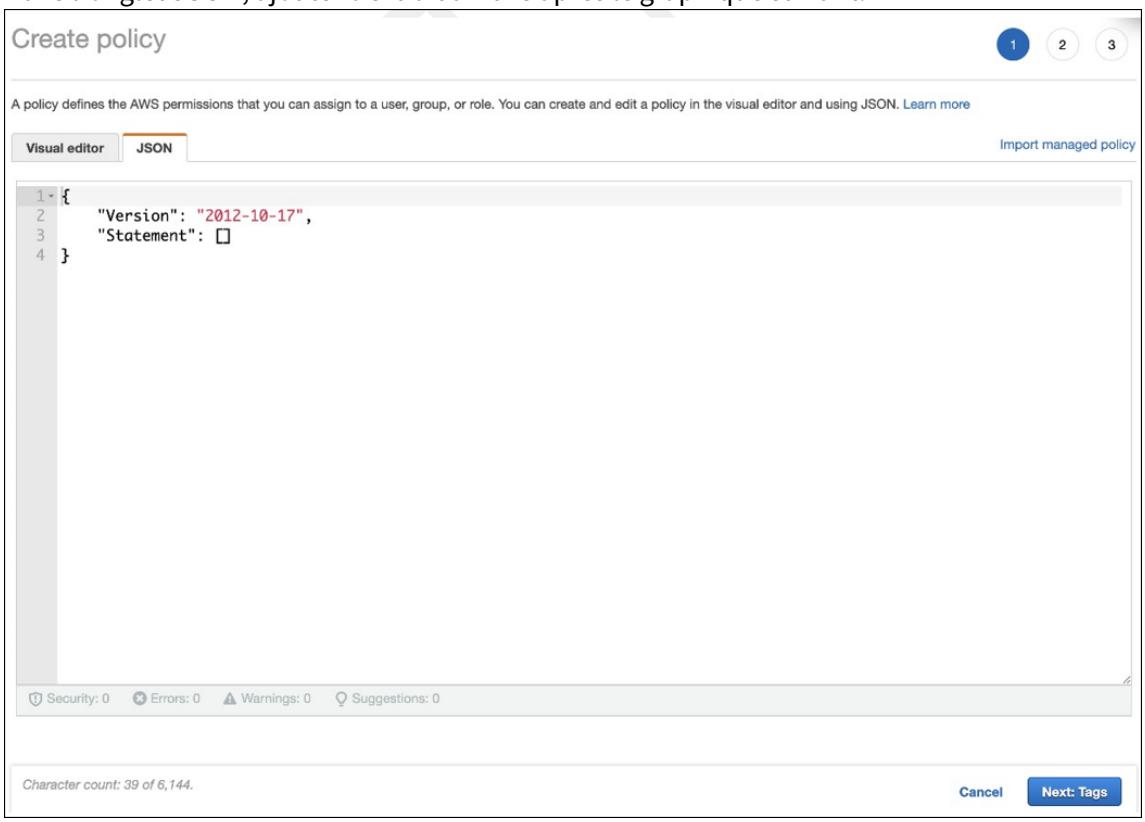
Autorisations d'accès par programmation aux comptes AWS

Le compte utilisateur AWS doit disposer de certaines autorisations d'accès par programmation pour effectuer des appels d'API vers la couche de ressources AWS. L'accès par programmation crée un ID de clé d'accès et une clé d'accès secrète.
Vous pouvez créer une stratégie contenant ces autorisations dans la console IAM. Comme le montrent les graphiques suivants, vous pouvez utiliser l'éditeur visuel (en ajoutant les autorisations une par une) ou le fichier JSON (en ajoutant l'extrait ci-dessous).
Pour plus d'informations, consultez la page Création d'un utilisateur IAM dans votre compte AWS.

- Dans l'onglet **Éditeur visuel**, ajoutez les autorisations une par une.



- Dans l'onglet **JSON**, ajoutez l'extrait affiché après le graphique suivant.



Autorisations requises

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                    "workdocs:DeregisterDirectory",
                    "workdocs:RegisterDirectory",
                    "workdocs:AddUserToGroup",
                    "ec2:ImportInstance",
                    "ec2:DescribeImages",
                    "ec2:DescribeImageAttribute"
                    "ec2:CreateKeyPair",
                    "ec2:DescribeKeyPairs",
                    "ec2:ModifyImageAttribute",
                    "ec2:DescribeVpcs",
                    "ec2:DescribeSubnets",
                    "ec2:RunInstances",
                    "ec2:DescribeSecurityGroups",
                    "ec2:CreateTags",
                    "ec2:DescribeRouteTables",
                    "ec2:DescribeInternetGateways",
                    "ec2:CreateSecurityGroup",
                    "ec2:DescribeInstanceTypes",
                    "servicequotas:ListServices",
                    "servicequotas:GetRequestedServiceQuotaChange",
                    "servicequotas:ListTagsForResource",
                    "servicequotas:GetServiceQuota",
                    "servicequotas:
                       GetAssociationForServiceQuotaTemplate",
                    "servicequotas:ListAWSDefaultServiceQuotas",
                    "servicequotas:ListServiceQuotas",
                    "servicequotas:GetAWSDefaultServiceQuota",
                    "servicequotas:
                       GetServiceQuotaIncreaseRequestFromTemplate",
                    "servicequotas:
                       ListServiceQuotaIncreaseRequestsInTemplate",
                    "servicequotas:
                       ListRequestedServiceQuotaChangeHistory",
                    "servicequotas:
                       ListRequestedServiceQuotaChangeHistoryByQuota",
                    "sts:DecodeAuthorizationMessage",
                    "ds:*",
                    "workspaces:*",
                    "iam:GetRole",
                    "iam:GetContextKeysForPrincipalPolicy",
                    "iam:SimulatePrincipalPolicy"

                ],
```



```
                "Resource": "*"
            }

        ]
 }

<!--NeedCopy-->
```

Citrix DaaS pour Google Cloud

November 17, 2022

Citrix DaaS pour Google Cloud vous permet de déployer des bureaux et des applications Google Cloud à l'aide de l'interface de gestion Configuration complète du service. Citrix DaaS pour Google Cloud est disponible dans les éditions Standard et Premium.

Pour plus d'informations sur les fonctionnalités prises en charge, consultez le tableau des fonctionnalités Citrix Virtual Apps and Desktops.

Vous pouvez commander Citrix DaaS pour Google Cloud sur Google Cloud Marketplace.

Après avoir commandé Citrix DaaS, connectez-vous à Citrix Cloud. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.

Suivez les instructions de configuration dans la documentation de ce produit. Dans l'interface Configuration complète, vous pouvez créer des connexions, des catalogues et des groupes de mise à disposition, comme vous le feriez lorsque vous utilisez cette interface avec d'autres éditions de produits. (Ces éditions ne disposent actuellement pas d'interface de gestion Déploiement rapide)

Certains écrans de l'interface Configuration complète peuvent différer de ceux de la documentation. Par exemple, lors de la création d'une connexion dans une édition Citrix Virtual Apps and Desktops pour Google Cloud, les types de connexion disponibles incluent les hyperviseurs pris en charge et Google Cloud. Les autres services cloud ne sont pas disponibles.

De même, utilisez les informations de la documentation du produit qui s'appliquent aux hyperviseurs pris en charge et à Google Cloud.

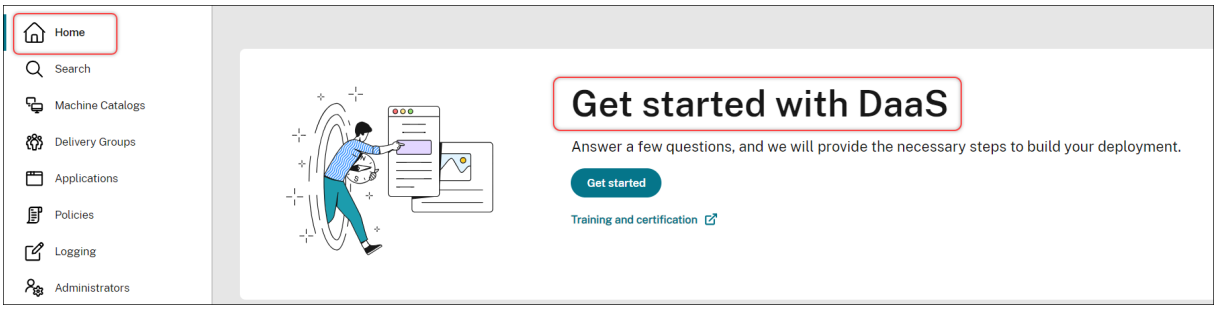
Pour obtenir des instructions détaillées sur le déploiement et la configuration de Citrix DaaS sur Google Cloud, consultez cet article Citrix Tech Zone : Virtualisation Citrix sur Google Cloud. Cet article explique comment définir l'architecture de déploiement, préparer le projet Google Cloud, configurer les services réseau et déployer Active Directory.

Utilisation du guide de démarrage DaaS (Technical Preview)

May 17, 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.

Le guide de démarrage DaaS rationalise et simplifie le processus de déploiement de DaaS pour les administrateurs débutants et expérimentés. À l'aide de ce guide, vous pouvez configurer rapidement vos déploiements DaaS en répondant à une série de questions.



Cet article décrit les processus de configuration de cinq scénarios de déploiement DaaS typiques.

Avantages

L'utilisation de ce guide présente les avantages suivants :

- **Démarrage facile**. Ce guide relie les étapes essentielles du déploiement par le biais d'un flux de travail étape par étape basé sur un questionnaire. Si vous êtes un nouvel administrateur, vous pouvez configurer rapidement votre déploiement tout en apprenant les concepts et la terminologie grâce à une aide contextuelle.
- **Simplification des configurations complexes**. Ce guide fournit des paramètres préconfigurés si nécessaire et donne accès à l'interface utilisateur Configuration complète pour les configurations avancées. Si vous êtes un administrateur expérimenté, vous pouvez utiliser le guide comme point de départ pour les configurations complexes.

Scénarios de déploiement pris en charge

Ce guide propose des déploiements rapides pour les scénarios suivants :

Éléments à mettre à disposition	Les machines existent déjà ?	Type de machine	Remarque
Applications et bureaux virtuels	Non	Machines virtuelles (provisionnées par DaaS)	Gestion de l'alimentation
Applications et bureaux virtuels	Oui	Machines virtuelles ou PC lames	Gestion de l'alimentation
Applications et bureaux virtuels	Oui	Machines physiques ou virtuelles	Pas de gestion de l'alimentation
PC de bureau	Oui	Machines physiques	Gestion de l'alimentation
PC de bureau	Oui	Machines physiques	Pas de gestion de l'alimentation

Consultez les sections suivantes pour obtenir des instructions détaillées :

- Mettre à disposition des applications et des ordinateurs de bureau à partir de zéro (gestion de l'alimentation)
- Mettre à disposition des applications et des bureaux à l'aide de machines existantes (gestion de l'alimentation)
- Mettre à disposition des applications et des bureaux à l'aide de machines existantes (sans gestion de l'alimentation)
- Fournissez des ordinateurs de bureau (alimentation gérée)
- Mettre à disposition des ordinateurs de bureau (sans gestion de l'alimentation)

Terminologie

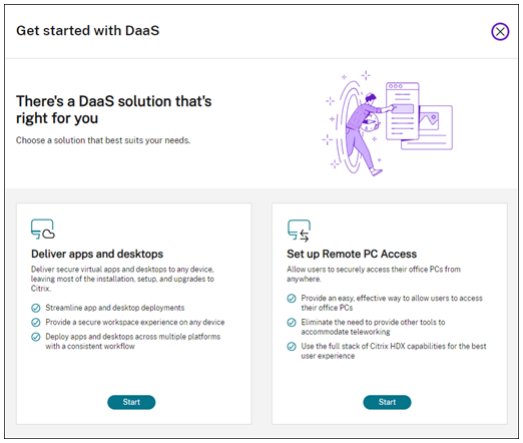
Les termes suivants sont spécifiques à DaaS :

- **Emplacement de ressources.** Contient les ressources nécessaires pour mettre des applications et des bureaux à disposition des utilisateurs.
- **Connexion hôte.** Connecte DaaS à un hôte (hyperviseur ou service cloud) dans un emplacement de ressources. La création de connexions hôtes est requise lorsque vous souhaitez créer et gérer des machines sur des hôtes ou gérer l'alimentation de machines existantes.
- **Image principale.** Sert de modèle pour répliquer des machines virtuelles sur votre hôte. Elle inclut le système d'exploitation, les applications, le Virtual Delivery Agent (VDA) et d'autres logiciels.

- **Catalogue de machines.** Collection de machines identiques. Elles peuvent être virtuelles ou physiques selon vos besoins. Vous pouvez créer un catalogue de machines pour créer des machines configurées de manière identique sur un hôte ou importer des machines dans DaaS à des fins de gestion.
- **Groupe de mise à disposition.** Contient des machines issues de catalogues de machines. Il spécifie quels utilisateurs peuvent utiliser ces machines, ainsi que les applications et bureaux disponibles pour ces utilisateurs.
- **Profil de machine.** Spécifie les propriétés des machines virtuelles. Les machines virtuelles d'un catalogue peuvent hériter des propriétés d'un profil de machine.

Accéder au guide

1. Accédez à la page **DaaS > Accueil**.
2. Repérez **Découvrez DaaS**.
3. Cliquez sur **Mise en route** pour lancer votre processus de déploiement.



> **Remarque :**
>
> Vous pouvez quitter le processus à tout moment en cliquant sur **Fermer** et le guide enregistre automatiquement vos paramètres. Pour poursuivre votre configuration, cliquez sur **Continuer**. Pour repartir à zéro, cliquez sur **Recommencer**.

Mettre à disposition des applications et des ordinateurs de bureau à partir de zéro (gestion de l'alimentation)

Cette section vous guide tout au long du processus de déploiement qui consiste à créer des machines virtuelles et à les utiliser pour mettre à disposition des applications et des bureaux.

Logiciels requis

Avant de commencer, vous avez besoin des éléments suivants :

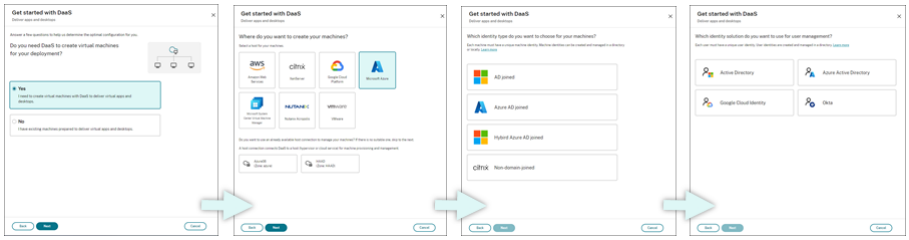
- Connectivité entre Citrix Cloud et le fournisseur d'identité cible

  Pour plus d'informations, consultez la section correspondante dans Fournisseurs d'identité.
- Rôle : Administrateur complet ou Administrateur Cloud
- Autorisations requises sur l'hyperviseur ou le service cloud cible.

  Pour plus d'informations, consultez les sections correspondantes dans Créer et gérer des connexions.
- Informations d'identification d'administrateur pour la création de comptes de machine virtuelle

Préparation

Répondez aux questions qui s'affichent à l'écran pour définir les paramètres suivants au niveau de l'infrastructure. Consultez le tableau suivant pour plus de détails.

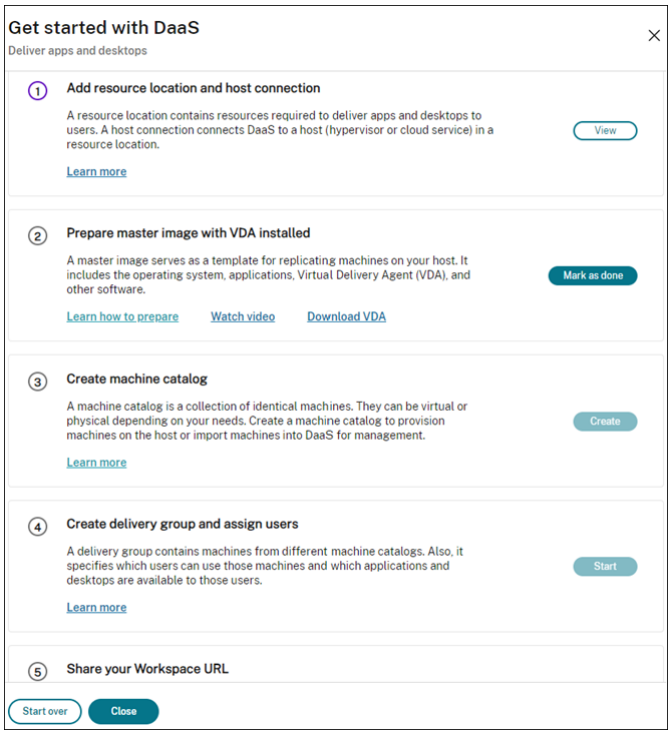


N°	Paramètre	Description
1	Spécifier si la création d'une machine virtuelle est nécessaire	Sélectionnez **Oui**.
2	Sélectionner le type d'hôte	Sélectionnez un type d'hôte pour votre déploiement. Options : AWS, XenServer (anciennement Citrix Hypervisor), Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis et VMware

N°	Paramètre	Description
3	Sélectionner le type d'identité machine	Sélectionnez un type d'identité pour la gestion des machines. Options : Joint à AD, Joint à Azure AD, Joint à Azure AD Hybride et Non joint au domaine
4	Sélectionner le type d'identité utilisateur	Sélectionnez un type d'identité pour la gestion des utilisateurs. Options : Active Directory, Azure Active Directory, Google Cloud Identity et Okta

Étapes de déploiement

Une fois que vous avez défini les paramètres au niveau de l'infrastructure, les étapes spécifiques à ce scénario de déploiement apparaissent comme suit.



Suivez les instructions qui s'affichent à l'écran pour effectuer les réglages.

Étape 1 : Ajouter un emplacement de ressources et des connexions hôtes Configurez l'emplacement de vos ressources en installant des Cloud Connector et configurez les connexions aux hyperviseurs ou aux services cloud de l'emplacement.

1. Nommez l'emplacement des ressources.
2. Téléchargez et installez des Cloud Connector sur au moins deux machines Windows Server.
3. Détectez les Cloud Connector installés.
4. Ajoutez et configurez des connexions hôtes pour l'emplacement des ressources. Les paramètres détaillés d'une connexion incluent :

    - Détails de la connexion, tels que l'adresse connexion, le nom d'utilisateur et le mot de passe de la connexion.
    - Ressources de stockage
    - Ressources réseau

    > **Remarque :**
    >
    > DaaS crée et gère des machines virtuelles sur des hôtes via ces connexions. Vous devez spécifier les connexions lorsque vous créez des catalogues de machines.

Étape 2 : Préparer les images principales pour vos machines Préparez les images principales sur les machines virtuelles de votre emplacement de ressources. Pour plus d'informations, voir Préparer une image principale sur l'hyperviseur ou le service de cloud.

Étape 3 : Créer des catalogues de machines Créez un catalogue de machines pour créer un groupe de machines configurées de manière identique sur un hôte. Les étapes détaillées sont les suivantes :

1. Donnez un nom au catalogue.
2. Sélectionnez le type de machine.

    Options : Multi-session, Statique mono-session (bureaux personnels) et Aléatoire mono-session (bureaux groupés).
3. Sélectionnez une connexion hôte.

    Les options proviennent de toutes les connexions hôtes que vous avez configurées pour vos emplacements de ressources à l'étape 1.
4. Sélectionnez une image principale.
5. Sélectionnez un profil de machine.

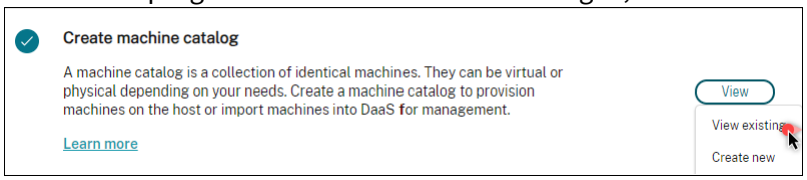
> **Remarque :**
>
> La prise en charge des profils de machine est actuellement disponible pour les services cloud Azure, GCP et AWS, et l'utilisation des profils de machine est facultative pour GCP.

6. Définissez le nombre de machines que vous souhaitez créer.
7. Définissez les identités des machines.

   Par défaut, le type d'identité de machine que vous avez sélectionné lors de la phase de préparation est affiché. Fournissez les paramètres d'identité requis pour les machines virtuelles, tels que le domaine, l'unité d'organisation et le schéma de dénomination.
8. Entrez les informations d'identification de l'administrateur requises pour la création de machine.
9. Cliquez sur **Créer**.

   > **Conseil :**
   >
   > Le bouton **Créer** n'est disponible qu'une fois que vous avez défini tous les paramètres requis.

   Pour voir la progression de la création du catalogue, sélectionnez **Afficher > Afficher existant**.



Étape 4 : Créer des groupes de mise à disposition et attribuer des utilisateurs

> **Conseil :**
>
> Avant de créer des groupes de mise à disposition, consultez les catalogues existants pour vous assurer qu'au moins un catalogue a été créé avec succès. Dans le cas contraire, vous ne pourrez pas créer de groupes de mise à disposition.

La création d'un groupe de mise à disposition inclut les sous-tâches suivantes :

- Ajouter des machines virtuelles au groupe
- Attribuer des utilisateurs au groupe
- Spécifier les applications et les bureaux que vous souhaitez mettre à la disposition des utilisateurs attribués

1. Donnez un nom au groupe.
2. Ajoutez des machines au groupe en sélectionnant un catalogue de machines et en spécifiant le nombre de machines virtuelles disponibles pour le groupe.

3. Spécifiez les applications et les bureaux disponibles pour ce groupe :
    - Pour ajouter des applications à partir d'une machine en cours d'exécution dans le catalogue sélectionné, cliquez sur **Ajouter > Depuis le menu Démarrer**.
    - Pour ajouter des applications déployées sur des partages réseau, cliquez sur **Ajouter > Manuellement**, puis indiquez les paramètres requis, tels que le chemin, le répertoire de travail, etc.
    - (Visible uniquement sur les machines avec OS multi-session) Pour la mise à disposition de bureaux, maintenez la sélection de l'option **Activer mise à disposition de bureaux**.
4. Ajoutez les utilisateurs qui peuvent accéder aux applications et aux bureaux de ce groupe.

Étape 5 : Partager l'URL de l'espace de travail avec vos utilisateurs Accédez à **Configuration de l'espace de travail > Accès**, puis partagez l'URL de l'espace de travail avec vos utilisateurs.

Mettre à disposition des applications et des bureaux à l'aide de machines existantes (gestion de l'alimentation)

Cette section vous guide tout au long du processus de déploiement qui consiste à mettre à disposition des applications et des bureaux à l'aide de machines existantes (gestion de l'alimentation).

Logiciels requis

Avant de commencer, vous avez besoin des éléments suivants :

- Connectivité entre Citrix Cloud et le fournisseur d'identité cible

  Pour plus d'informations, consultez la section correspondante dans Fournisseurs d'identité.
- Rôle : Administrateur complet ou Administrateur Cloud

Préparation

Répondez aux questions qui s'affichent à l'écran pour définir les paramètres suivants au niveau de l'infrastructure.

N°	Paramètre	Description
1	Spécifier si la création d'une machine virtuelle est nécessaire	Sélectionnez **Non**.

N°	Paramètre	Description
2	Indiquer si la gestion de l'alimentation est requise	Sélectionnez **Machines dont l'alimentation est gérée (par exemple, machines virtuelles ou PC lames)**.
3	Sélectionner la plateforme hôte	Sélectionnez la plate-forme hôte sur laquelle résident vos machines existantes. Options : AWS, Citrix, Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis et VMware
4	Sélectionner le type d'identité utilisateur	Sélectionnez un type d'identité pour la gestion des utilisateurs. Options : Active Directory, Azure Active Directory, Google Cloud Identity et Okta

Étapes de déploiement

Une fois que vous avez défini les paramètres au niveau de l'infrastructure, les étapes spécifiques à ce scénario de déploiement apparaissent. Suivez les instructions qui s'affichent à l'écran pour effectuer les réglages.

Étape 1 : Ajouter un emplacement de ressources et des connexions hôtes Configurez l'emplacement de vos ressources en installant des Cloud Connector et configurez les connexions aux hyperviseurs ou aux services cloud de votre emplacement.

1. Nommez l'emplacement des ressources.
2. Téléchargez et installez des Cloud Connector sur au moins deux machines Windows Server.
3. Détectez les Cloud Connector installés.
4. Ajoutez et configurez des connexions hôtes pour l'emplacement des ressources. Les paramètres de connexion sont par exemple l'adresse de connexion, le nom d'utilisateur et le mot de passe.

> **Remarque :**
>
> DaaS gère l'alimentation des machines situées sur des sites de ressources par le biais de connexions. Vous devez spécifier une connexion lors de l'importation de vos machines dans un catalogue.

Étape 2 : Créer des catalogues de machines Créez un catalogue de machines et importez-y vos machines.

1. Nommez le catalogue.
2. Sélectionnez le type de machine.

   Options : Multi-session, Statique mono-session (bureaux personnels) et Aléatoire mono-session (bureaux groupés).
3. Sélectionnez un emplacement de ressources.
4. Importez des machines dans le catalogue.
   Les machines sont organisées par connexion hôte. Choisissez une connexion hôte pour importer les machines associées.
5. Cliquez sur **Créer**.

Étape 3 : Créer des groupes de mise à disposition et attribuer des utilisateurs Pour créer un groupe de mise à disposition, vous devez :

- Ajouter des machines virtuelles au groupe
- Attribuer des utilisateurs au groupe
- Spécifier les applications et les bureaux que vous souhaitez mettre à la disposition des utilisateurs attribués

1. Donnez un nom au groupe.
2. Sélectionnez un catalogue de machines selon vos besoins, puis spécifiez le nombre de machines disponibles pour le groupe de mise à disposition.
3. Spécifiez les applications et les bureaux disponibles pour ce groupe :
   - Pour ajouter des applications à partir d'une machine en cours d'exécution dans le catalogue sélectionné, cliquez sur **Ajouter > Depuis le menu Démarrer**.
   - Pour ajouter des applications déployées sur des partages réseau, cliquez sur **Ajouter > Manuellement**, puis indiquez les paramètres requis, tels que le chemin, le répertoire de travail, etc.
   - (Visible uniquement sur les machines avec OS multi-session) Pour la mise à disposition de bureaux, maintenez la sélection de l'option **Activer mise à disposition de bureaux**.
4. Ajoutez des utilisateurs au groupe.

Étape 4 : Partager l'URL de l'espace de travail avec vos utilisateurs Accédez à **Configuration de l'espace de travail > Accès**, puis partagez l'URL de l'espace de travail avec vos utilisateurs.

Mettre à disposition des applications et des bureaux à l'aide de machines existantes (sans gestion de l'alimentation)

Cette section vous guide tout au long du processus de déploiement qui consiste à mettre à disposition des applications et des bureaux à l'aide de machines existantes (sans gestion de l'alimentation).

Logiciels requis

Avant de commencer, vous avez besoin des éléments suivants :

- Connectivité entre Citrix Cloud et le fournisseur d'identité cible

  Pour plus d'informations, consultez la section correspondante dans Fournisseurs d'identité
- Rôle : Administrateur complet ou Administrateur Cloud

Préparation

Répondez aux questions qui s'affichent à l'écran pour définir les paramètres suivants au niveau de l'infrastructure.

N°	Paramètre	Description
1	Spécifier si la création d'une machine virtuelle est nécessaire	Sélectionnez **Non**.
2	Indiquer si la gestion de l'alimentation est requise	Sélectionnez **des machines dont l'alimentation n'est pas gérée (par exemple, machines physiques)**.
3	Sélectionner le type d'identité utilisateur	Sélectionnez un type d'identité pour la gestion des utilisateurs. Options : Active Directory, Azure Active Directory, Google Cloud Identity et Okta

Étapes de déploiement

Une fois que vous avez défini les paramètres au niveau de l'infrastructure, les étapes spécifiques à ce scénario de déploiement apparaissent. Suivez les instructions qui s'affichent à l'écran pour effectuer les réglages.

Étape 1 : Ajouter un emplacement de ressources Configurez l'emplacement de vos ressources en installant des Cloud Connector.

1. Nommez l'emplacement des ressources.
2. Téléchargez et installez des Cloud Connector sur au moins deux machines Windows Server.
3. Détectez les Cloud Connector installés.

> **Remarque :**
>
> La création de connexions hôtes n'est requise que lorsque vous souhaitez gérer l'alimentation des machines.

Étape 2 : créer un catalogue de machines Créez un catalogue de machines et importez-y vos machines.

1. Nommez le catalogue.
2. Sélectionnez le type de machine.

   Options : Multi-session, Statique mono-session (bureaux personnels) et Aléatoire mono-session (bureaux groupés).
3. Sélectionnez un emplacement de ressources.
4. Importez des machines dans le catalogue.

   Pour faciliter la recherche de machines, utilisez des noms d'ordinateurs partiels et sélectionnez des répertoires.
5. Cliquez sur **Créer**.

Étape 3 : Créer des groupes de mise à disposition et attribuer des utilisateurs Pour créer un groupe de mise à disposition, vous devez :

- Ajouter des machines virtuelles au groupe
- Attribuer des utilisateurs au groupe
- Spécifier les applications et les bureaux que vous souhaitez mettre à la disposition des utilisateurs attribués

1. Donnez un nom au groupe.

2. Sélectionnez un catalogue de machines selon vos besoins, puis spécifiez le nombre de machines disponibles pour le groupe de mise à disposition.
3. Spécifiez les applications et les bureaux disponibles pour ce groupe :
    - Pour ajouter des applications à partir d'une machine en cours d'exécution dans le catalogue sélectionné, cliquez sur **Ajouter > Depuis le menu Démarrer**.
    - Pour ajouter des applications déployées sur des partages réseau, cliquez sur **Ajouter > Manuellement**, puis indiquez les paramètres requis, tels que le chemin, le répertoire de travail, etc.
    - (Visible uniquement sur les machines avec OS multi-session) Pour la mise à disposition de bureaux, maintenez la sélection de l'option **Activer mise à disposition de bureaux**.
4. Ajoutez des utilisateurs au groupe.

Étape 4 : Partager l'URL de l'espace de travail avec vos utilisateurs Accédez à **Configuration de l'espace de travail > Accès**, puis partagez l'URL de l'espace de travail avec vos utilisateurs.

Fournissez des ordinateurs de bureau (alimentation gérée)

Cette section vous guide tout au long du processus de déploiement qui consiste à mettre à disposition des ordinateurs de bureau (gestion de l'alimentation).

Logiciels requis

Avant de commencer, vous aurez besoin de :

- Noms de machine des ordinateurs.
- Citrix Virtual Delivery Agent (VDA) installé sur chaque PC. (Cette étape peut être effectuée après la création du catalogue.)

  Pour plus d'informations, consultez Télécharger le VDA.

Préparation

Répondez aux questions qui s'affichent à l'écran pour définir les paramètres suivants au niveau de l'infrastructure.

N°	Étape	Description
1	Sélectionnez le type d'attribution des machines.	Sélectionnez la manière dont les machines sont attribuées. Options : Attribution automatique statique, Préattribution statique et Pool aléatoire sans attribution
2	Déterminer s'il convient d'autoriser les utilisateurs à allumer les machines	Sélectionnez **Je souhaite que les utilisateurs distants allument eux-mêmes les machines**.
3	Sélectionner le type d'identité utilisateur	Sélectionnez un type d'identité pour la gestion des utilisateurs. Options : Active Directory, Azure Active Directory, Google Cloud Identity et Okta

Étapes de déploiement

Une fois que vous avez défini les paramètres au niveau de l'infrastructure, les étapes spécifiques à ce scénario de déploiement apparaissent. Suivez les instructions qui s'affichent à l'écran pour effectuer les réglages.

Étape 1 : Ajouter un emplacement de ressources et des connexions hôtes Configurez l'emplacement de vos ressources en installant des Cloud Connector et ajoutez une connexion de type **Wake on LAN de Remote PC**.

1. Nommez l'emplacement des ressources.
2. Téléchargez et installez des Cloud Connector sur au moins deux machines Windows Server.
3. Détectez les Cloud Connector installés.
4. Cliquez sur **Ajouter** pour ajouter une connexion :
    a) Sélectionnez un emplacement de ressources (zone).
    b) Sélectionnez **Remote PC Wake on LAN** pour **Type de connexion**.
    c) Entrez un nom pour la connexion.

> **Remarque :**
>
> DaaS gère l'alimentation des machines via les connexions configurées. Vous devez configurer

> des connexions de type **Wake on LAN de Remote PC** lors de la création de catalogues Remote PC Access pour les machines dont l'alimentation est gérée.

Étape 2 : Créer un catalogue Remote PC Access Créez un catalogue de machines et importez-y vos ordinateurs de bureau.

1. Nommez le catalogue.
2. Sélectionnez un emplacement de ressources.
3. Sélectionnez un type d'attribution des machines. Par défaut, le type que vous avez sélectionné lors de la phase de préparation est affiché.
4. Sélectionnez **Connexion Wake on LAN**. Les options sont les connexions du type **Wake on LAN de Remote PC** que vous avez configurées pour l'emplacement sélectionné.
5. Importez vos machines.
6. Cliquez sur **Créer**.

Étape 3 : Créer des groupes de mise à disposition et attribuer des utilisateurs Créez un groupe de mise à disposition pour regrouper les machines que vous souhaitez mettre à disposition et spécifiez qui peut y accéder.

1. Donnez un nom au groupe.
2. Sélectionnez un catalogue de machines selon vos besoins. Seuls les catalogues **Remote PC Access** apparaissent.
3. Attribuez des utilisateurs au groupe.

Étape 4 : Partager l'URL de l'espace de travail avec vos utilisateurs Accédez à **Configuration de l'espace de travail > Accès**, puis partagez l'URL de l'espace de travail avec vos utilisateurs.

Mettre à disposition des ordinateurs de bureau (sans gestion de l'alimentation)

Cette section vous guide tout au long du processus de déploiement qui consiste à mettre à disposition des ordinateurs de bureau (sans gestion de l'alimentation).

Logiciels requis

Avant de commencer, vous aurez besoin de :

- Noms de machine des ordinateurs.

- Citrix Virtual Delivery Agent (VDA) installé sur chaque PC. (Cette étape peut être effectuée après la création du catalogue.)

  Pour plus d'informations, consultez Télécharger le VDA.

Préparation

Répondez aux questions qui s'affichent à l'écran pour définir les paramètres suivants au niveau de l'infrastructure.

N°	Paramètre	Description
1	Sélectionnez le type d'attribution des machines.	Sélectionnez la manière dont les machines sont attribuées. Options : Attribution automatique statique, Préattribution statique et Pool aléatoire sans attribution
2	Déterminer s'il convient d'autoriser les utilisateurs à allumer les machines	Laissez l'option **Je souhaite que les utilisateurs distants allument eux-mêmes les machines** sélectionnée.
3	Sélectionner le type d'identité utilisateur	Sélectionnez un type d'identité pour la gestion des utilisateurs. Options : Active Directory, Azure Active Directory, Google Cloud Identity et Okta

Étapes de déploiement

Une fois que vous avez défini les paramètres au niveau de l'infrastructure, les étapes spécifiques à ce scénario de déploiement apparaissent. Suivez les instructions qui s'affichent à l'écran pour effectuer les réglages.

Étape 1 : Ajouter un emplacement de ressources Configurez l'emplacement de vos ressources en installant des Cloud Connector.

1. Nommez l'emplacement des ressources.
2. Téléchargez et installez des Cloud Connector sur au moins deux machines Windows Server.
3. Détectez les Cloud Connector installés.

> **Remarque :**
>
> La création de connexions hôtes n'est requise que lorsque vous souhaitez gérer l'alimentation des machines.

Étape 2 : Créer un catalogue Remote PC Access Créez un catalogue et importez-y vos ordinateurs de bureau.

1. Nommez le catalogue.
2. Sélectionnez un emplacement de ressources.
3. Sélectionnez un type d'attribution. Par défaut, le type que vous avez sélectionné lors de la phase de préparation est affiché.
4. Importez vos machines.
5. Cliquez sur **Créer**.

Étape 3 : Créer des groupes de mise à disposition et attribuer des utilisateurs Créez un groupe de mise à disposition pour les machines que vous souhaitez mettre à disposition et spécifiez qui peut y accéder.

1. Donnez un nom au groupe.
2. Sélectionnez un catalogue de machines selon vos besoins. Seuls les catalogues **Remote PC Access** apparaissent.
3. Attribuez des utilisateurs au groupe.

Étape 4 : Partager l'URL de l'espace de travail avec vos utilisateurs Accédez à **Configuration de l'espace de travail > Accès**, puis partagez l'URL de l'espace de travail avec vos utilisateurs.

Identités des machines

November 2, 2023

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	Les identités sont créées et gérées dans Azure AD. Les machines provisionnées sont jointes à Azure AD à l'aide des identités de machine attribuées. L'importation de machines virtuelles dans Citrix DaaS n'est pas prise en charge.
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 et Azure AD. 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 DaaS.
Non joint au domaine	Les identités sont créées et gérées localement sur les machines. L'importation de machines virtuelles dans Citrix DaaS n'est pas prise en charge.

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 DaaS	Citrix Workspace	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
Joint à AD	Oui	Oui	Oui	Oui	Oui
Joint à Azure AD	Oui	Oui	Non	Oui	Non
Joint à Azure AD Hybride	Oui	Oui	Oui	Oui	Oui
Non joint au domaine	Oui	Oui	Oui	Oui	Oui

> **Remarque**
>
> Ni le cache d'hôte local ni la continuité de service ne sont disponibles pour les hôtes de session non joints à un domaine lors de l'utilisation de Storefront.

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 adapta-tive
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

July 5, 2023

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. Pour plus d'informations sur les niveaux fonctionnels pris en charge pour la forêt et le domaine, voir Niveaux fonctionnels d'Active Directory.

Pour plus d'informations sur la création de catalogues joints à Active Directory (AD) à l'aide de Citrix DaaS, voir Créer des catalogues de machines.

Joint à Azure Active Directory

May 17, 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 (AAD) à l'aide de Citrix DaaS, en plus des exigences décrites dans la section Configuration système requise pour Citrix DaaS.

Exigences

- Plan de contrôle : voir Configurations prises en charge
- Type de VDA : mono-session (bureaux uniquement) ou multisession (applications et bureaux)
- Version de VDA : 2203 ou ultérieure
- Type de provisioning : Machine Creation Services (MCS) persistant et non persistant utilisant le workflow de profil de machine
- Type d'affectation : dédié et regroupé
- Plateforme d'hébergement : Azure uniquement
- Rendezvous V2 doit être activé

Limitations

- La continuité du service n'est pas prise en charge.
- L'authentification unique aux bureaux virtuels n'est pas prise en charge. Les utilisateurs doivent saisir manuellement leurs informations d'identification lorsqu'ils se connectent à leur bureau.

- La connexion avec Windows Hello sur le bureau virtuel n'est pas prise en charge. Seuls le nom d'utilisateur et le mot de passe sont actuellement pris en charge. Si les utilisateurs essaient de se connecter avec une méthode Windows Hello, ils reçoivent un message d'erreur indiquant qu'ils ne sont pas l'utilisateur négocié et la session est déconnectée. Les méthodes associées incluent le code PIN, la clé FIDO2, l'authentification multifacteur, etc.
- Environnements de cloud Microsoft Azure Resource Manager uniquement.
- La première fois qu'une session de bureau virtuel est lancée, l'écran de connexion Windows peut afficher l'invite d'ouverture de session pour le dernier utilisateur connecté sans possibilité de passer à un autre utilisateur. L'utilisateur doit attendre que l'ouverture de session expire et que l'écran de verrouillage du bureau apparaisse, puis cliquer sur l'écran de verrouillage pour afficher à nouveau l'écran d'ouverture de session. À ce stade, l'utilisateur peut sélectionner **Autre utilisateur** et entrer ses informations d'identification. C'est le comportement à chaque nouvelle session lorsque les machines ne sont pas persistantes.

Considérations

Configuration de l'image

- Vous pouvez optimiser votre image Windows à l'aide de l'outil Citrix Optimizer.

Joint à Azure AD

- Envisagez de désactiver Windows Hello afin que les utilisateurs ne soient pas invités à le configurer lorsqu'ils se connectent à leur bureau virtuel. Si vous utilisez VDA 2209 ou version ultérieure, cela se fait automatiquement. Pour les versions antérieures, vous pouvez procéder de l'une des deux manières suivantes :
  - Stratégie de groupe ou stratégie locale
    - Accédez à **Configuration ordinateur > Modèles d'administration > Composants Windows > Windows Hello Entreprise**.
    - Configurez l'option **Utiliser Windows Hello Entreprise** sur :
      - **Désactivé**, ou
      - **Activé** et sélectionnez **Ne pas démarrer le provisioning Windows Hello après la connexion**.
  - Microsoft Intune
    - Créez un profil d'appareil qui désactive Windows Hello pour les entreprises. Reportez-vous à la documentation de Microsoft pour plus de détails.

    * Actuellement, Microsoft prend en charge l'inscription Intune des machines persistantes uniquement, ce qui signifie que vous ne pouvez pas gérer les machines non persistantes avec Intune.

- Les utilisateurs doivent disposer d'un accès explicite dans Azure pour se connecter aux machines à l'aide de leurs informations d'identification AAD. Cela peut être facilité en ajoutant l'attribution de rôle au niveau du groupe de ressources :

    1. Connectez-vous au portail Azure.
    2. Sélectionnez **Resource Groups**.
    3. Cliquez sur le groupe de ressources dans lequel résident les charges de travail de bureau virtuel.
    4. Sélectionnez **Access control (IAM)**.
    5. Cliquez sur **Add role assignment**.
    6. Recherchez **Virtual Machine User Login**, sélectionnez-la dans la liste, puis cliquez sur **Next**.
    7. Sélectionnez **User, group, or service principal**.
    8. Cliquez sur **Select members** et sélectionnez les utilisateurs et les groupes auxquels vous souhaitez accorder l'accès aux bureaux virtuels.
    9. Cliquez sur **Sélectionner**.
    10. Cliquez sur **Review + assign**.
    11. Cliquez à nouveau sur **Review + assign** .

> **Remarque :**
>
> Si vous choisissez de laisser MCS créer le groupe de ressources pour les bureaux virtuels, vous ajoutez cette attribution de rôle après la création du catalogue de machines.

- Les VM principales peuvent être jointes à Azure AD ou ne pas être jointes à un domaine. Cette fonctionnalité nécessite la version 2212 ou ultérieure du VDA.

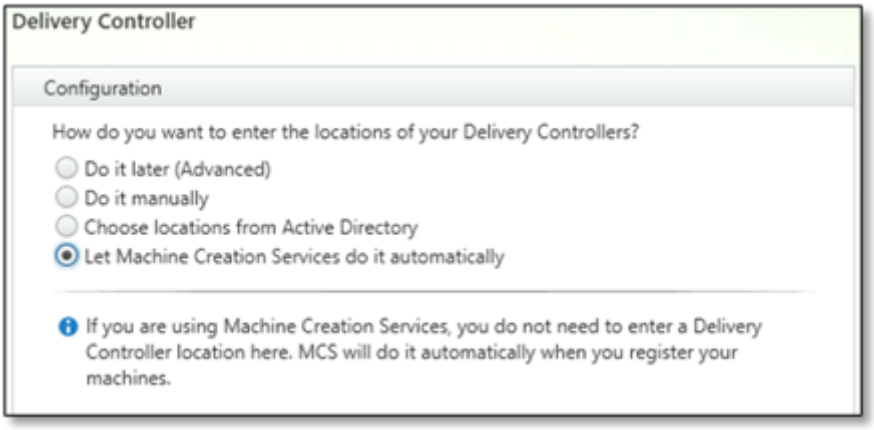
Installation et configuration du VDA

Suivez les étapes d'installation du VDA :

1. Assurez-vous de sélectionner les options suivantes dans l'assistant d'installation :

    - Sur la page Environnement, sélectionnez **Créer une image MCS principale**.

- Sur la page Delivery Controller, sélectionnez **Laisser Machine Creation Services effectuer ceci automatiquement**.



2. Une fois le VDA installé, ajoutez 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

3. 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.

```
1 reg ADD HKLM\Software\AzureAD\VirtualDesktop /v Provider /t REG_SZ
      /d Citrix /f
2 <!--NeedCopy-->
```


4. Si vous joignez la machine virtuelle principale à Azure AD, puis que vous utilisez l'utilitaire `dsregcmd` pour la retirer d'Azure, assurez-vous que la valeur de `AADLoginForWindowsExtensionJoi` sous HKLM\Software\Microsoft\Windows Azure\CurrentVersion\AADLoginForWindowsExtension est égale à zéro.

Autres ressources

Une fois que l'emplacement des ressources et la connexion d'hébergement sont disponibles, créez le catalogue de machines. Pour plus d'informations sur la création de catalogues de machines joints à Azure Active Directory, voir Créer des catalogues joints à Azure Active Directory.

Microsoft Intune

March 7, 2024

Cet article décrit les conditions requises pour créer des catalogues compatibles Microsoft Intune à l'aide de Citrix DaaS, en plus des exigences décrites dans la section Configuration système requise pour Citrix DaaS.

Microsoft Intune est un service basé sur le cloud pour la gestion des appareils mobiles (MDM) et la gestion des applications mobiles (MAM). Vous contrôlez la façon dont les appareils de votre entreprise sont utilisés, y compris les téléphones mobiles, les tablettes et les ordinateurs portables. Pour plus d'informations, consultez Microsoft Intune. Les appareils doivent répondre à la configuration minimale requise. Pour plus d'informations, consultez la documentation Microsoft Systèmes d'exploitation et navigateurs pris en charge dans Intune.

Microsoft Intune fonctionne en utilisant les fonctionnalités d'Azure AD.

> **Important :**
>
> Avant d'activer cette fonctionnalité, vérifiez que votre environnement Azure répond aux exigences de licence pour utiliser Microsoft Intune. Pour de plus amples informations, consultez la documentation de Microsoft : `https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses`. N'activez pas cette fonctionnalité si vous ne possédez pas la licence Intune appropriée.

Exigences

- Plan de contrôle : Citrix DaaS
- Type de VDA : VDA avec OS mono-session

- Version de VDA : 2203 ou ultérieure
- Type de provisioning : Machine Creation Services (MCS) persistant utilisant le workflow de profil de machine uniquement
- Type d'affectation : dédié

Limitations

- Ne prend en charge que les machines virtuelles persistantes mono-session jointes à Azure AD.
- Ne prend en charge que les machines virtuelles persistantes jointes à Azure AD hybride mono-session à l'aide d'informations d'identification d'utilisateur ou d'appareil avec fonction de co-gestion. Pour plus d'informations, voir Inscrire automatiquement un appareil Windows à l'aide de stratégie de groupe.
- N'ignorez pas la préparation des images lors de la création ou de la mise à jour des catalogues de machines.

Considérations

- Créez un profil d'appareil qui désactive Windows Hello pour les entreprises.
- Utilisez VDA version 2212 ou ultérieure si Microsoft Intune doit gérer une machine virtuelle principale.

Autres ressources

Pour plus d'informations sur la création de catalogues compatibles avec Microsoft Intune, voir Créer des catalogues compatibles avec Microsoft Intune.

Joint à Azure Active Directory Hybride

May 17, 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

- Plan de contrôle : voir Configurations prises en charge
- 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')
    {

        break;
     }


    if ($provider -eq 1)
    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
           Provider" -Value "Citrix" -Force
        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
           autoWorkplaceJoin" -Value 1 -Force
        Start-Sleep 5
        dsregcmd /join
        break
     }
```



```
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.

Non joint au domaine

November 24, 2023

Cet article décrit les conditions requises pour créer des catalogues non joints à un domaine à l'aide de Citrix DaaS, en plus des exigences décrites dans la section Configuration système requise pour Citrix DaaS.

Exigences

- Plan de contrôle : voir Configurations prises en charge
- Type de VDA : mono-session (bureaux uniquement) ou multisession (applications et bureaux)
- Version de VDA : 2203 ou ultérieure
- Type de provisioning : Machine Creation Services (MCS) persistant et non persistant
- Type d'affectation : dédié et regroupé
- Plateforme d'hébergement : Toutes les plateformes prises en charge par MCS
- Rendezvous V2 doit être activé
- Cloud Connector : uniquement nécessaires si vous envisagez de provisionner des machines sur des hyperviseurs locaux ou si vous souhaitez utiliser Active Directory comme fournisseur d'identité dans Workspace.

Limitations

- La continuité du service n'est pas prise en charge.

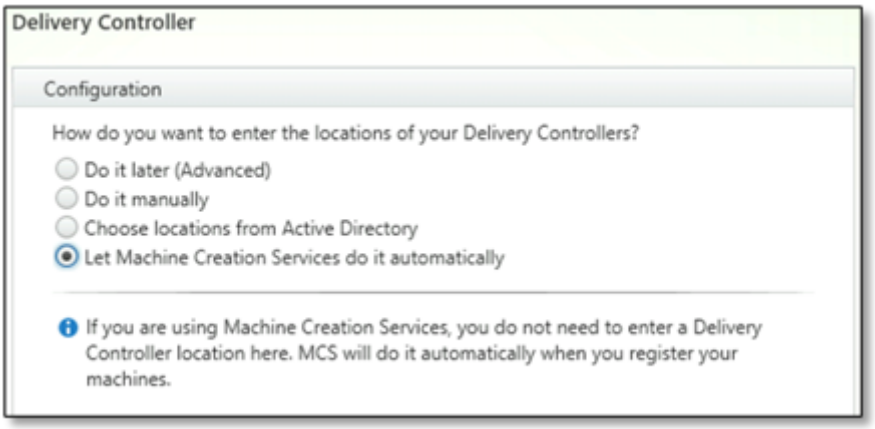
- Chaque fois que nous utilisons un VDA multisession non joint à un domaine, les données de profil de l'utilisateur local ne sont pas conservées et sont supprimées lors de la fermeture de session.

Installation et configuration du VDA

Suivez les étapes d'installation du VDA :

1. Assurez-vous de sélectionner les options suivantes dans l'assistant d'installation :
    - Sur la page Environnement, sélectionnez **Créer une image MCS principale**.

    - Sur la page Delivery Controller, sélectionnez **Laisser Machine Creation Services effectuer ceci automatiquement**.



2. Une fois le VDA installé, ajoutez 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

Autres ressources

Une fois que l'emplacement des ressources et la connexion d'hébergement sont disponibles, créez le catalogue de machines. Pour plus d'informations sur la création de catalogues de machines non joints à un domaine, voir Créer des catalogues non joints à un domaine.

Configurer des emplacements de ressources

June 12, 2024

Les emplacements de ressources contiennent les ressources requises pour mettre des applications et bureaux à la disposition des utilisateurs. Vous pouvez gérer les ressources à partir de Citrix Cloud. En général, les ressources comprennent :

- Des hyperviseurs ou services cloud, appelés *hôtes*, qui incluent les composants suivants :
  - Contrôleurs de domaine Active Directory.
  - Virtual Delivery Agents (VDA) : les VDA sont installés sur une machine qui fournit les applications et les bureaux aux utilisateurs.
  - Citrix Gateway (facultatif) : pour activer l'accès externe sécurisé aux applications et bureaux proposés aux utilisateurs, ajoutez une appliance Citrix Gateway VPX à l'emplacement de ressources. Configurez ensuite Citrix Gateway.
  - Serveurs Citrix StoreFront.
  - Pour communiquer avec Citrix Cloud, chaque emplacement de ressources doit contenir un Citrix Cloud Connector. Afin d'assurer une disponibilité permanente, au moins deux connecteurs cloud par emplacement de ressources sont recommandés.

Une zone équivaut à un emplacement de ressources. Lorsque vous créez un emplacement de ressources et installez un Cloud Connector, une zone est automatiquement créée pour vous. Pour plus d'informations, consultez la section Zones.

Pour en savoir plus sur les types de ressources, consultez Se connecter à Citrix Cloud.

Configuration requise de l'hôte

L'hyperviseur ou le service cloud, sur lequel vous provisionnez des machines virtuelles, nécessite des autorisations ou une configuration uniques.

- Si l'hyperviseur ou le service de cloud requiert des réseaux virtuels, suivez les instructions dans la documentation qui l'accompagne.
- Créez le cloud privé virtuel (VPC) (pour AWS ou GCP) ou le réseau virtuel (VNET) (pour Azure) approprié aux machines que vous ajouterez à l'emplacement de ressources.
- Créez des règles appropriées pour sécuriser le trafic entrant et sortant entre les machines dans le réseau virtuel. Par exemple, si vous utilisez AWS, vérifiez que des règles appropriées sont configurées sur le groupe de sécurité du VPC pour que les machines dans le VPC soient accessibles uniquement aux adresses IP que vous spécifiez.

Les types d'hôtes suivants sont pris en charge :

- Environnements de virtualisation Amazon Web Services (AWS)
- Environnements de virtualisation XenServer
- Environnements de virtualisation Google Cloud Platform
- Environnements de virtualisation HPE Moonshot
- Environnements de virtualisation Microsoft Azure Resource 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

Active Directory

Provisionnez un serveur Windows, installez Active Directory Domain Services (AD DS) et promouvez-le en contrôleur de domaine. Pour obtenir des conseils, consultez la documentation Microsoft Présentation d'Active Directory Domain Services.

Remarques importantes :

- Vous devez disposer d'au moins un contrôleur de domaine exécutant Active Directory Domain Services.
- N'installez aucun composant Citrix sur un contrôleur de domaine.

Pour plus d'informations, consultez :

- Niveaux fonctionnels Active Directory
- Gestion des identités et des accès dans Citrix Cloud.
- Connecter Active Directory à Citrix Cloud
- Scénarios de déploiement pour l'utilisation de Connector Appliance avec Active Directory

Cloud Connector

Le composant Cloud Connector est un groupe de services de Citrix Cloud qui permet aux VDA, à StoreFront et au Delivery Controller basés sur le cloud de communiquer entre eux. Vous pouvez installer des Cloud Connector de manière interactive ou à partir de la ligne de commande.

Pour plus d'informations sur les services Cloud Connector, consultez les pages suivantes :

- Citrix Cloud Connector
- Détails techniques
- Configuration du proxy et du pare-feu
- Installation
- Mises à jour de Connector

Considérations sur le dimensionnement et la scalabilité

- Lorsque vous évaluez le dimensionnement et la scalabilité de Citrix DaaS, tenez compte de tous les composants.
- Effectuez des recherches et des tests sur la configuration des services Cloud Connector et de StoreFront de manière à déterminer celle qui répond le mieux à vos besoins spécifiques.
- Le sous-dimensionnement des machines peut avoir un impact négatif sur les performances du système.

L'article Considérations relatives à la taille et à la montée en charge des Cloud Connectors couvrent les sujets suivants :

- Informations sur les tests de taille et de montée en charge
- Capacités maximales testées
- Meilleures pratiques recommandées pour la configuration des machines Cloud Connector

Ajouter un type de ressource

1. Connectez-vous à Citrix Cloud.
2. Dans le menu en haut à gauche, sélectionnez **Emplacements des ressources**.
3. Sélectionnez **+ Emplacements de ressources** pour ajouter un emplacement de ressources.
4. Entrez un nom pour l'emplacement de ressources, puis cliquez sur **Enregistrer**. Pour plus d'informations sur les considérations relatives à la dénomination, consultez Restrictions de nom.
5. Sous le nouvel emplacement des ressources, sélectionnez **Cloud Connector**.
6. Téléchargez et installez le logiciel Cloud Connector sur au moins deux serveurs du domaine où résident les ressources Citrix DaaS.

- Lors de l'installation, sélectionnez l'emplacement des ressources créé aux étapes précédentes.
- Après l'installation, Citrix Cloud ajoute les serveurs à l'emplacement des ressources et enregistre les domaines dans lesquels vous avez installé les Cloud Connector.

7. Vérifiez que les domaines enregistrés sont actifs :

   - Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**.
   - Sélectionnez **Domaines**. La liste des domaines dans lesquels les Cloud Connector ont été déployés s'affiche.
   - Localisez les domaines que vous utilisez avec Citrix DaaS. Les domaines actifs s'affichent avec une barre verte sur le côté gauche de l'entrée du domaine.

   Si votre domaine ne possède pas l'indicateur visuel, cela signifie que le domaine est à l'état **inutilisé**. Si vous spécifiez un domaine inutilisé lors de la configuration du catalogue de machines, la création du catalogue échoue. Pour vous assurer que la configuration du catalogue de machines se déroule sans erreur, suivez les étapes de la section Activer un domaine inutilisé.

   Pour plus d'informations, consultez l'article CTX473009: DaaS Catalog Creation Wizard: "Internal Server Error"when creating adding new machine accounts.

Activer un domaine inutilisé

1. Dans l'onglet **Domaine**, sous **Gestion des identités et des accès**, sélectionnez **Afficher les domaines inutilisés**. Une fois cette option sélectionnée, l'intitulé passe à **Masquer les domaines inutilisés**.
2. Recherchez le domaine inutilisé dans la liste. Les domaines inutilisés s'affichent sous la forme d'une barre grise sur le côté gauche de l'entrée du domaine et d'un menu de points de suspension à option unique sur le côté droit.
3. Sélectionnez le menu des points de suspension, puis **Utiliser le domaine**. La barre grise devient verte et le menu des points de suspension passe à **Désactiver**.

Autres ressources

- Pour un simple déploiement de validation de principe, installez un VDA sur une machine destinée à fournir des applications ou un bureau à vos utilisateurs.
- Pour configurer l'emplacement des ressources pour des types d'hôtes spécifiques :
  - Environnements de virtualisation AWS
  - Environnements de virtualisation Google Cloud
  - Environnements de virtualisation HPE Moonshot

  - Environnements de virtualisation Microsoft Azure Resource 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 virtualisation XenServer

- Pour un déploiement complet, créez et gérez des connexions et des ressources pour un emplacement de ressources.
- Passez en revue toutes les étapes du processus d'installation et de configuration

Environnements de virtualisation AWS

March 30, 2024

Cet article explique comment configurer votre compte AWS en tant qu'emplacement des ressources compatible avec Citrix DaaS.

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.

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.
- Deux instances appartenant au domaine sur lesquelles le Citrix Cloud Connector est installé, situées dans le sous-réseau privé du VPC.
- Une instance qui agit en tant qu'hôte Bastion, située 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.

Après avoir terminé ces tâches, vous pouvez installer des VDA, provisionner des machines, créer des catalogues et des groupes de mise à disposition.

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 des passerelles NAT avec une adresse IP élastique dans le sous-réseau public. Cela 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. Un VPC Amazon, des services DHCP et DNS sont fournis par défaut, ce qui affecte la façon de configurer le 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.

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

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.

> **Remarque :**
>
> La modification du nom d'un VPC (cloud privé virtuel) AWS dans la console AWS démonte l'unité

> d'hébergement existante dans Citrix Cloud. Lorsque l'unité d'hébergement est démontée, vous ne pouvez pas créer de catalogues ou ajouter des machines à des catalogues existants. Problème connu : PMCS-7701

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 **Yes, Create**.

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

3. Lorsque vous avez terminé, sélectionnez **Save**.

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 **Save**.

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 encore configuré le trafic provenant du groupe de sécurité public, vous devez définir les ports TCP. 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	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.
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 **Save**.
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 **Save**.

Tâche 3 : Lancer des instances

Les étapes suivantes créent quatre instances EC2 et décryptent 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 and Connectors : sélectionner le sous-réseau privé
6. Dans **Auto-assign Public IP address**, effectuez les sélections suivantes pour chaque instance :
   - Bastion host : sélectionner **Enable**
   - Domain controller and Connectors : sélectionner **Use default setting** ou **Disable**
7. Dans **Network Interfaces**, entrez une adresse IP principale au sein de la plage d'adresses IP de votre sous-réseau privé pour le contrôleur de domaine et les instances de Cloud Connector.
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.
- Domain controller and Cloud Connectors : 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 nouvelle 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**. Cliquez sur **View Instances** pour afficher une liste d'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 toute 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
    - Trois instances du sous-réseau privé à utiliser en tant que :
      - Un, en tant que contrôleur de domaine
      - Deux, en tant que Cloud Connector

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 **Yes, Create.**

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.

5. Configurez le premier Cloud Connector comme suit :

    a) Joignez l'instance au domaine et redémarrez lorsque vous y êtes invité. À partir de l'instance de hôte Bastion, reconnectez-vous à l'instance à l'aide de RDP.
    b) Connectez-vous à Citrix Cloud. Sélectionnez **Emplacements des ressources** à partir du menu en haut à gauche.

c) Téléchargez le Cloud Connector.
d) Lorsque vous y êtes invité, exécutez le fichier `cwcconnector.exe` et entrez vos informations d'identification Citrix Cloud. Suivez les instructions de l'assistant.
e) Une fois terminé, sélectionnez **Actualiser** pour afficher la page **Emplacements des ressources**. Une fois le Cloud Connector enregistré, l'instance s'affiche sur la page.

6. Répétez la procédure de configuration du Cloud Connector afin de configurer le second composant Cloud Connector.
7. Associez une stratégie IAM aux Cloud Connectors pour prendre en charge les connexions d'hébergement AWS avec une autorisation basée sur les rôles. La même stratégie IAM doit être associée à tous les Cloud Connector d'un emplacement de ressources. Pour plus d'informations sur les autorisations AWS requises, consultez Autorisations AWS requises.

Autres ressources

- Pour un simple déploiement de validation de principe, installez un VDA sur une machine destinée à fournir des applications ou un bureau à vos utilisateurs.
- Pour créer et gérer une connexion, consultez Connexion à AWS.
- Passez en revue toutes les étapes du processus d'installation et de configuration

Informations supplémentaires

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

Environnements de virtualisation Google Cloud

May 17, 2024

Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) vous permet de provisionner et de gérer des machines sur Google Cloud.

Logiciels requis

Avant de commencer à provisionner les machines virtuelles sur Google Cloud Platform (GCP), vous devez vous assurer d'avoir installé les logiciels requis suivants.

1. L'abonnement Citrix doit inclure la prise en charge des charges de travail multicloud hybrides. Pour plus d'informations, consultez Comparer les fonctionnalités des abonnements Citrix.
2. Le compte administrateur doit disposer d'autorisations suffisantes pour créer des connexions hôtes, des catalogues de machines et des groupes de mise à disposition. Pour plus d'informations, consultez Configurer l'administration déléguée.
3. Identifiez un projet Google Cloud dans lequel toutes les ressources de calcul associées au catalogue de machines sont stockées. Il peut s'agir d'un projet existant ou d'un nouveau. Pour plus d'informations, consultez Projets Google Cloud.
4. Activez les API Google Cloud requises pour l'intégration à Citrix DaaS. Pour plus d'informations, consultez Activer les API Google Cloud.
5. Créez les comptes de service dans Google Cloud et accordez les autorisations appropriées. Pour plus d'informations, consultez Configurer et mettre à jour des comptes de service.
6. Téléchargez le fichier de clé du compte de service Citrix Cloud. Pour plus d'informations, consultez Clé de compte du service Citrix Cloud.
7. Les machines virtuelles doivent pouvoir accéder aux API Google sans adresse IP publique. Pour plus d'informations, consultez Activer l'accès privé à Google.

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, à savoir des autorisations d'utilisation du VPC uniquement.

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`

Activer les API Google Cloud

Pour utiliser la fonctionnalité Google Cloud via l'interface Configuration complète de Citrix DaaS, activez ces API dans votre projet Google Cloud :

- API Compute Engine
- API Cloud Resource Manager
- API IAM (Identity and Access Management)
- API Cloud Build

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

1. Dans le menu supérieur gauche, sélectionnez **API et services > API et services activés**.
2. Sur l'écran **API et services activés**, vérifiez 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. De même, activez les API **Identity and Access Management (IAM)**, **Cloud Build** et **Cloud Key Management Service (KMS)**.

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
    - gcloud services enable cloudkms.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 DaaS améliore le processus de signalement d'échecs Cloud Build pour le service Google Cloud. Ce service exécute des builds sur Google Cloud. Citrix DaaS 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 DaaS 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. Identifiez les sous-réseaux utilisés pour l'environnement Citrix dans l'onglet **Subnets in current project**.
3. Cliquez sur le nom des sous-réseaux et activez l'**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

- Pour un simple déploiement de validation de principe, installez un VDA sur une machine destinée à fournir des applications ou un bureau à vos utilisateurs.
- Pour créer et gérer des connexions, consultez Connexion aux environnements Google Cloud.
- Passez en revue toutes les étapes du processus d'installation et de configuration.

Informations supplémentaires

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

Environnements de virtualisation HPE Moonshot

June 12, 2024

Citrix DaaS gère vos charges de travail HPE Moonshot via un plug-in HPE Moonshot géré par Citrix et présent dans le plan de contrôle de DaaS. 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.

Étapes clés

1. Configurez vos environnements HPE.
2. Créez une connexion avec le châssis HPE Moonshot.

   > **Remarque :**
   >
   > Une fois que vous avez activé cette fonctionnalité, le plug-in HPE Moonshot géré par Citrix est automatiquement installé. Vous pouvez donc continuer à utiliser le catalogue de machines existant à l'aide du plug-in Moonshot géré par Citrix au lieu du plug-in HPE Moonshot géré par HPE.

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 châs-

> sis 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

- Pour un simple déploiement de validation de principe, installez un VDA sur une machine qui fournira des applications ou un bureau à vos utilisateurs.
- Pour créer et gérer des connexions, consultez Connexion à HPE Moonshot.
- Passez en revue toutes les étapes du processus d'installation et de configuration.

Informations supplémentaires

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

Environnements de virtualisation Microsoft Azure Resource Manager

May 17, 2024

Lorsque vous provisionnez des machines virtuelles dans votre déploiement Citrix DaaS à l'aide de Microsoft Azure Resource Manager, consultez les pages suivantes :

- Qu'est-ce que Microsoft Entra ID ?
- Guide de démarrage sur l'intégration de Microsoft Entra ID aux applications
- Objets d'application et du principal de service dans Microsoft Entra ID

Pour configurer votre Microsoft Azure Resource Manager, consultez Configurer l'emplacement des ressources.

Autres ressources

- Pour un simple déploiement de validation de principe, installez un VDA sur une machine destinée à fournir des applications ou un bureau à vos utilisateurs.
- Pour créer et gérer une connexion, consultez Connexion à Microsoft Azure.
- Passez en revue toutes les étapes du processus d'installation et de configuration.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Créer des catalogues de machines
- CTX219211 : Configurer un compte Microsoft Entra ID
- CTX219243 : Grant XenApp and XenDesktop access to your Azure subscription
- CTX219271 : Deploy hybrid cloud using site-to-site VPN

Environnements de virtualisation Microsoft System Center Virtual Machine Manager

January 25, 2024

Suivez ce guide si vous utilisez Hyper-V avec Microsoft System Center Virtual Machine Manager (VMM) pour fournir des machines virtuelles.

La section Configuration système requise répertorie les versions de VMM prises en charge.

Vous pouvez utiliser Machine Creation Services ou Citrix Provisioning (anciennement Provisioning Services) pour provisionner :

- Machines virtuelles avec OS de serveur ou de bureau génération 1
- Machines virtuelles Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 10 et Windows 11 génération 2 (avec ou sans démarrage sécurisé)

Installer et configurer un hyperviseur

Installez le rôle Microsoft Hyper-V et VMM sur vos serveurs.

Vérifiez les informations de compte suivantes :

Dans **Gérer > Configuration complète**, le compte que vous spécifiez lors de la création d'une connexion doit être 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 l'interface **Configuration complète** lors du processus de création de la connexion.

Votre compte d'utilisateur doit également être membre du groupe de sécurité Administrateurs local sur chaque serveur Hyper-V pour prendre en charge la gestion du cycle de vie des VM (telle que la création, la mise à jour et la suppression de VM).

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.

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.

Installer la console VMM

Installez une console System Center Virtual Machine Manager sur chaque serveur contenant un Citrix Cloud Connector.

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.

Provisionnement 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 et l'enregisrer auprès d'Azure, 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 administrateur SCVMM 2019 UR3 ou version ultérieure dans les machines virtuelles Cloud Connector.

   b) Sur la page **Paramètres** de la console VMM, créez un compte Exécuter en tant que.

   c) Exécutez les commandes PowerShell suivantes avec des autorisations 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 l'interface **Configuration complète**.

Autres ressources

- Pour un simple déploiement de validation de principe, installez un VDA sur une machine destinée à fournir des applications ou un bureau à vos utilisateurs.
- Pour créer et gérer des connexions, consultez Connexion à Microsoft System Center Virtual Machine Manager.
- Passez en revue toutes les étapes du processus d'installation et de configuration.

Informations supplémentaires

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

Environnements de virtualisation Nutanix

February 13, 2024

Suivez ces instructions pour fournir des machines virtuelles dans votre déploiement Citrix DaaS à l'aide de Nutanix Acropolis. Le processus de configuration inclut l'installation et l'enregistrement du plug-in Nutanix dans votre environnement Citrix DaaS.

Pour de plus amples informations, consultez le Guide d'installation du plug-in Nutanix Acropolis MCS, disponible sur le portail d'assistance Nutanix.

> **Important :**
>
> Installez le plug-in Nutanix sur tous les Cloud Connector où Citrix DaaS doit créer une connexion hôte à l'emplacement de ressources doté d'un hyperviseur Nutanix.

Installer et enregistrer le plug-in Nutanix

Réalisez la procédure suivante pour installer et enregistrer le plug-in Nutanix sur tous vos Cloud Connector. Utilisez les fonctions **Gérer > Configuration complète** de Citrix Cloud pour créer une connexion à Nutanix.

Pour de plus amples informations sur l'installation du plug-in Nutanix, consultez le site de documentation de Nutanix.

Pour plus d'informations sur la configuration de vos environnements de virtualisation Nutanix, consultez Ajouter un type de ressource ou activer un domaine inutilisé dans Citrix Cloud.

Autres ressources

- Pour un simple déploiement de validation de principe, installez un VDA sur une machine destinée à fournir des applications ou un bureau à vos utilisateurs.
- Pour créer et gérer des connexions, consultez Connexion à Nutanix.
- Passez en revue toutes les étapes du processus d'installation et de configuration.

Informations supplémentaires

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

Solutions partenaires et cloud Nutanix

January 25, 2024

Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) prend en charge la solution partenaire et cloud Nutanix suivante :

- Nutanix Cloud Clusters sur AWS

Nutanix Cloud Clusters sur AWS

Citrix DaaS 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 Nutanix Clusters 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-xxxxxxxxxxxx: disable network interface source/dest check error.`
- Cluster Nutanix hôte - Nœud `XXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxx network interface info.`

Si la création du cluster échoue, procédez comme suit :

- 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, survolez le lien **Launch Prism Element** et copiez l'URL.

Autres ressources

- Pour un simple déploiement de validation de principe, installez un VDA sur une machine destinée à fournir des applications ou un bureau à vos utilisateurs.
- Pour créer et gérer des connexion, consultez la section Connexion aux solutions partenaires et cloud Nutanix.
- Passez en revue toutes les étapes du processus d'installation et de configuration.

Informations supplémentaires

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

Environnements de virtualisation VMware

January 25, 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.)

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

Si vous envisagez d'utiliser Machine Creation Services (MCS), ne désactivez pas la fonctionnalité de navigateur de magasin de données dans vCenter Server comme décrit dans Désactivation du navigateur de magasin de données vCenter Server. Si vous désactivez cette fonctionnalité, MCS ne fonctionne pas correctement.

Pour configurer vos environnements de virtualisation VMware, consultez la section Ajouter un type de ressource ou activer un domaine inutilisé dans Citrix Cloud.

Autres ressources

- Pour un simple déploiement de validation de principe, installez un VDA sur une machine destinée à fournir des applications ou un bureau à vos utilisateurs.
- Pour créer et gérer des connexions, consultez Connexion à VMware.
- Passez en revue toutes les étapes du processus d'installation et de configuration.

Informations supplémentaires

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

Solutions partenaires et cloud VMware

January 25, 2024

Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) 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)

Utilisez Citrix DaaS pour migrer les charges de travail Citrix locales basées sur VMware vers les solutions partenaires VMware respectives.

Intégration de la solution Azure VMware (AVS)

Citrix DaaS prend en charge AVS. AVS fournit une infrastructure cloud contenant des clusters vSphere créés par l'infrastructure Azure. Utilisez DaaS pour provisionner les charges de travail du VDA à l'aide d'AVS de la même manière que vous utiliseriez vSphere dans des environnements locaux.

Configurer le cluster AVS

Pour permettre à Citrix DaaS d'utiliser AVS, procédez comme suit dans Azure :

- Demander un quota d'hôtes
- Enregistrer le fournisseur de ressources `Microsoft.AVS`
- Vérifier la liste de contrôle de planification du réseau
- Liste de contrôle du réseau
- Créer un cloud privé AVS
- Accéder au cloud privé AVS
- Configurer la mise en réseau de votre cloud privé VMware dans Azure
- Configurer DHCP pour AVS
- Ajouter un segment de réseau dans AVS
- Vérifier l'environnement Azure AVS

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 : sélectionner un abonnement
- Service :**Tous les services > Solution Azure VMware**
- Ressource : question générale
- Résumé : capacité requise
- 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.

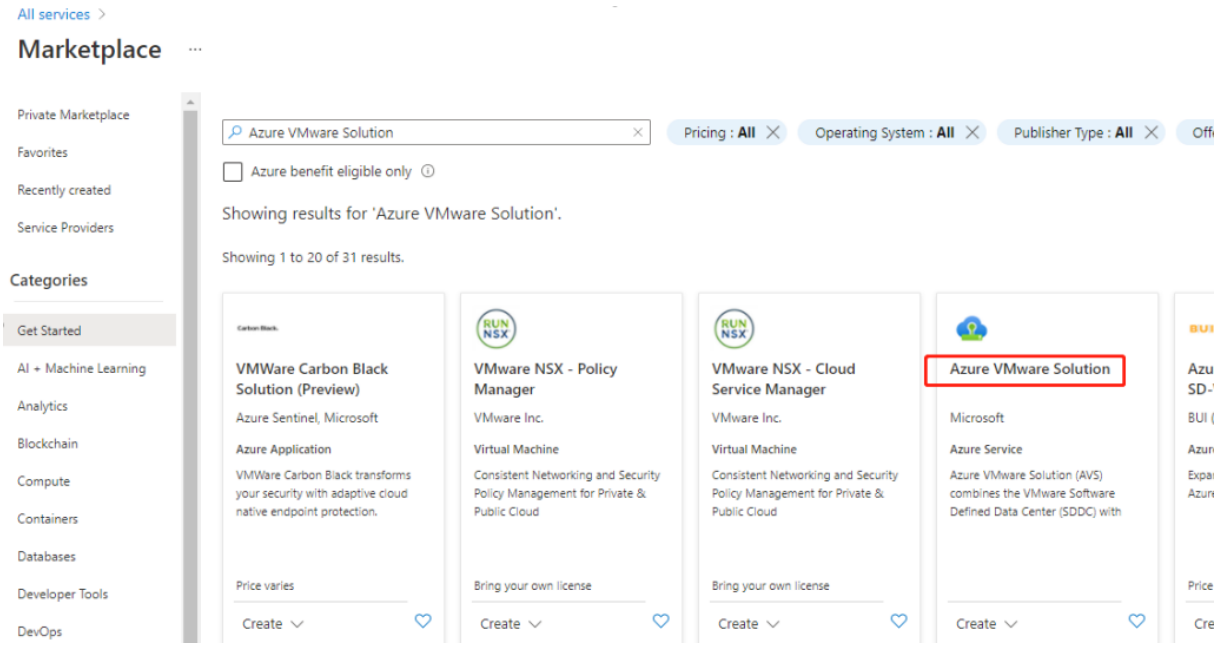
Enregistrer le fournisseur de ressources Microsoft.AVS Après avoir demandé le quota d'hôte, enregistrez le fournisseur de ressources :

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 AVS 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.



Dans la fenêtre **Solution Azure VMware** :

1. Sélectionnez **Créer**.
2. Accédez à l'onglet **Notions 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.
Taille de l'hôte	Sélectionnez la taille selon vos besoins.

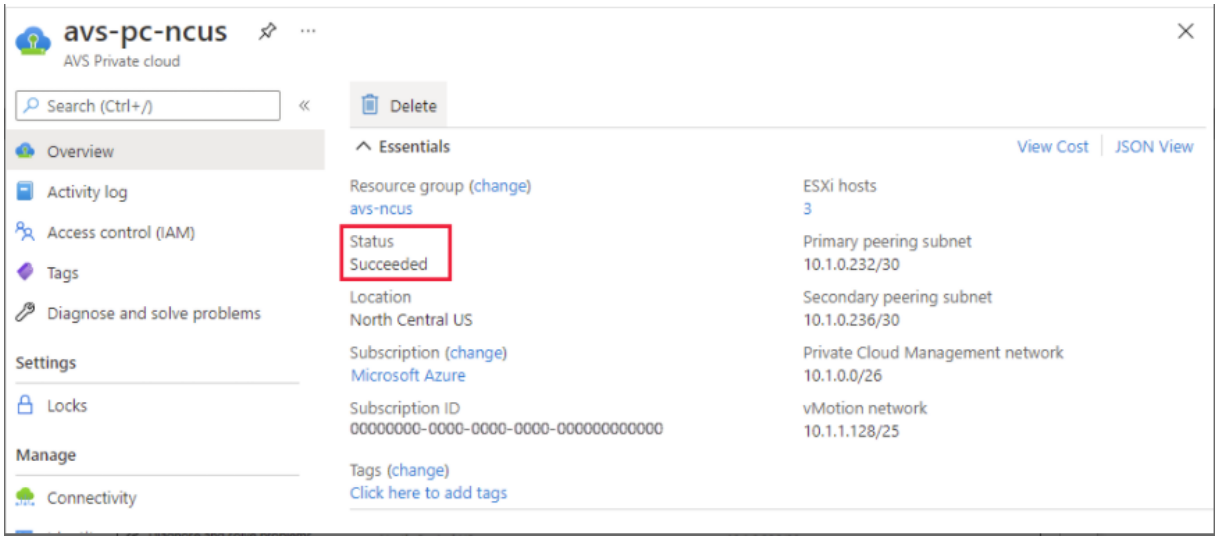
Champ	Valeur
Nombre d'hôtes	Affiche le nombre d'hôtes alloués au cluster de cloud privé. La valeur par défaut est 3, qui peut être augmentée ou réduite après le déploiement.
Bloc d'adresses pour le cloud privé	Fournissez un bloc d'adresses IP pour le cloud privé. Le CIDR représente le réseau de gestion 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.

Dans l'écran **Créer un cloud privé** :

1. Dans le champ **Emplacement**, sélectionnez la région qui possède l'AVS. La région du groupe de ressources est identique à la région AVS.
2. Dans le champ **Taille de l'hôte**, sélectionnez une taille selon vos besoins.
3. Spécifiez une adresse IP dans le champ **Bloc d'adresses pour le cloud privé**. 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 le cloud privé. Lorsque l'**état** indique **Réussi**, le déploiement est terminé.



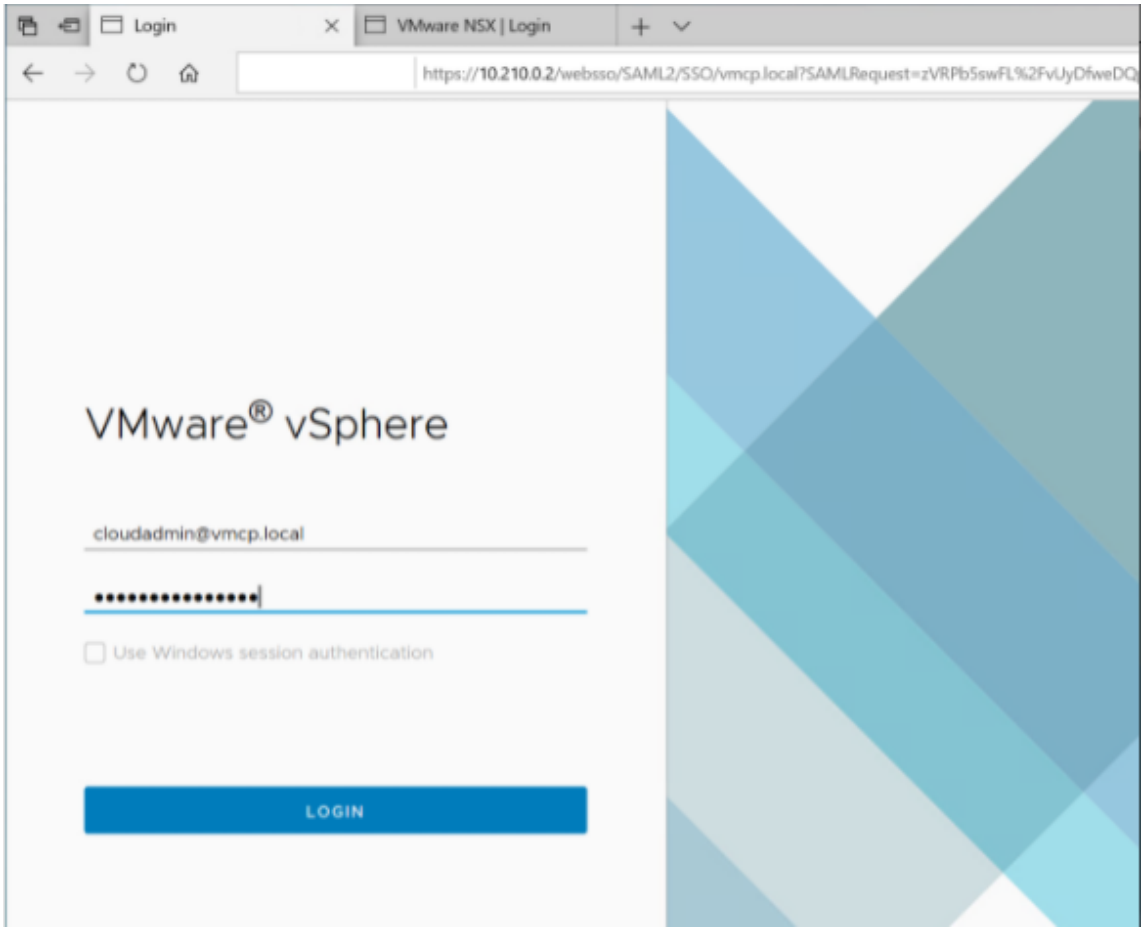
Accéder au cloud privé AVS Une fois que vous avez créé un cloud privé, créez une machine virtuelle Windows et connectez-vous au vCenter local de votre cloud privé.

Créer une machine virtuelle Windows

1. Dans le groupe de ressources, sélectionnez **+ Ajouter**, puis recherchez et sélectionnez **Microsoft Windows 10/11 ou Windows Server 2016/2019**.
2. Saisissez les informations requises, puis sélectionnez **Réviser+Créer**.
3. Une fois la validation terminée, sélectionnez **Créer** pour lancer le processus de création de machine virtuelle.

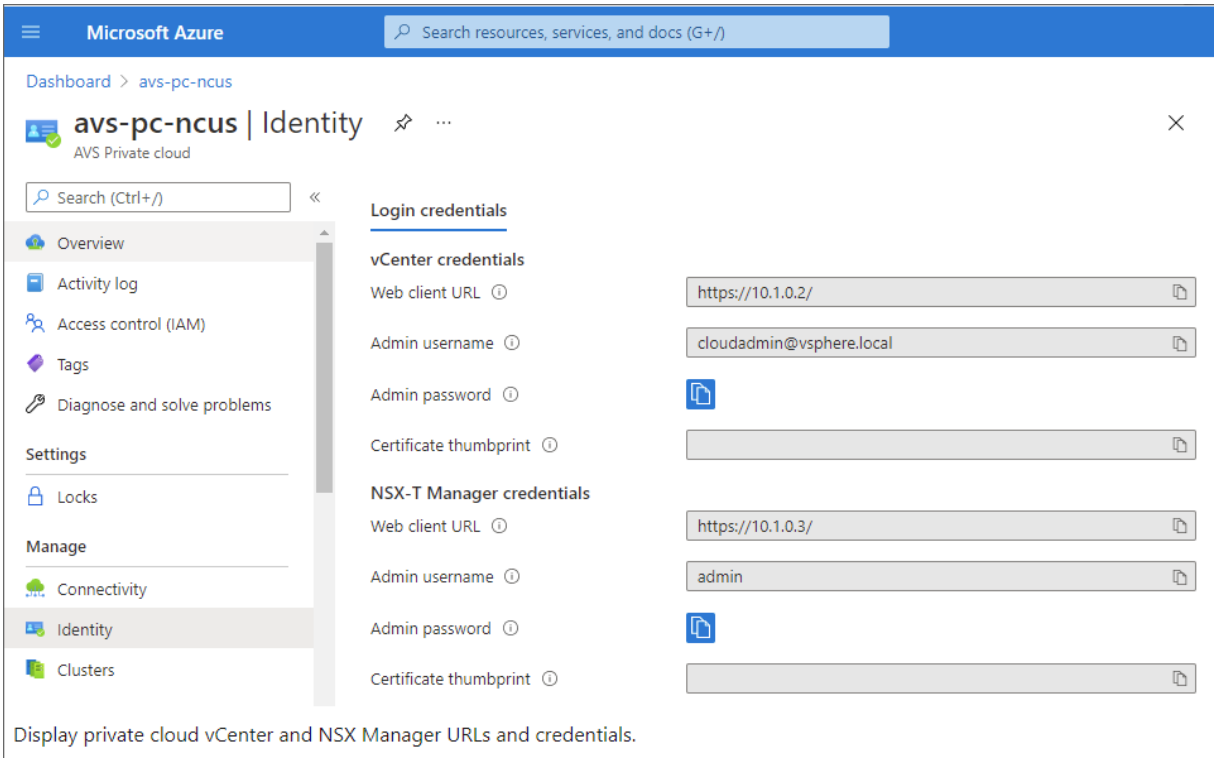
Se connecter au vCenter local de votre cloud privé

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 et connectez-vous à la machine virtuelle créée à l'étape précédente.
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.

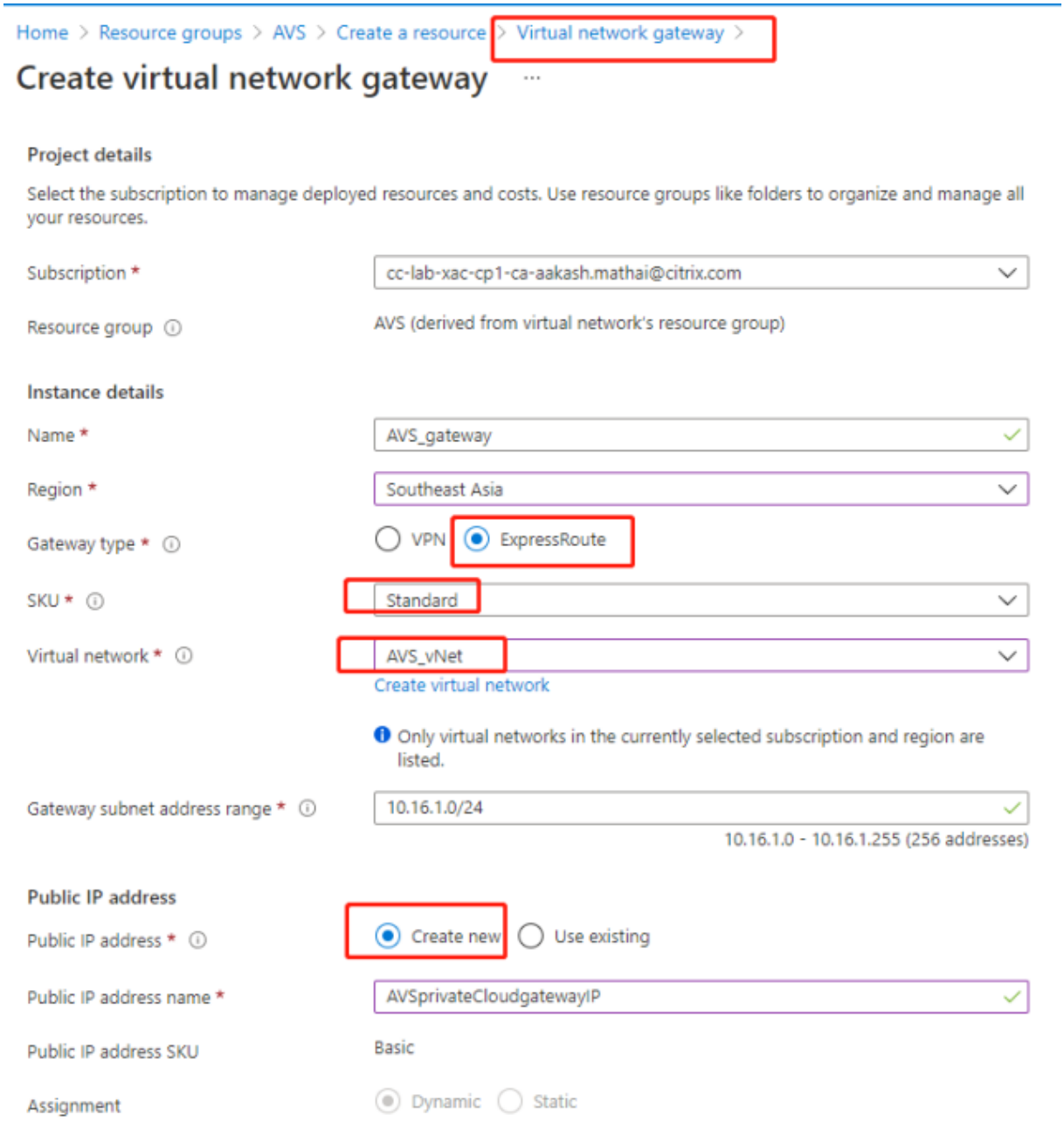
> **Important :**
>
> Utilisez une adresse qui ne chevauche pas l'espace d'adressage que vous avez utilisé lors de la création de votre cloud privé.

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**.

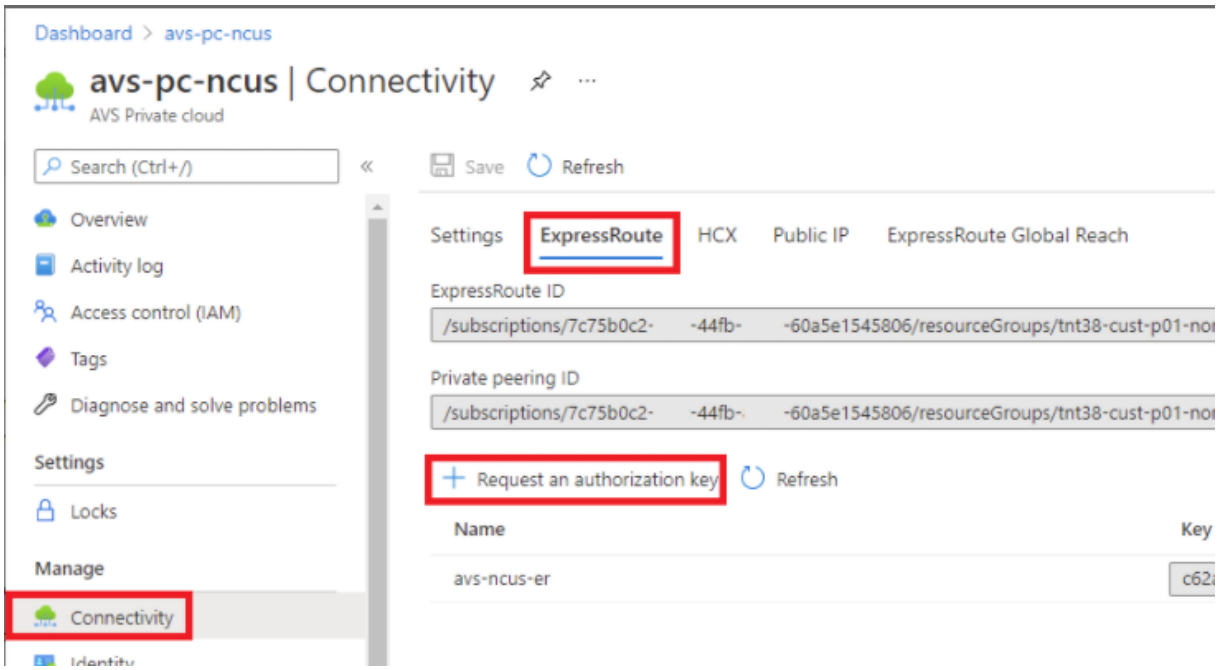


Après avoir examiné la configuration de la passerelle du réseau virtuel, cliquez sur **Créer** pour déployer votre passerelle de réseau virtuel.
Une fois le déploiement terminé, connectez votre connexion **ExpressRoute** à la passerelle de réseau virtuel contenant votre cloud privé Azure AVS.

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 :

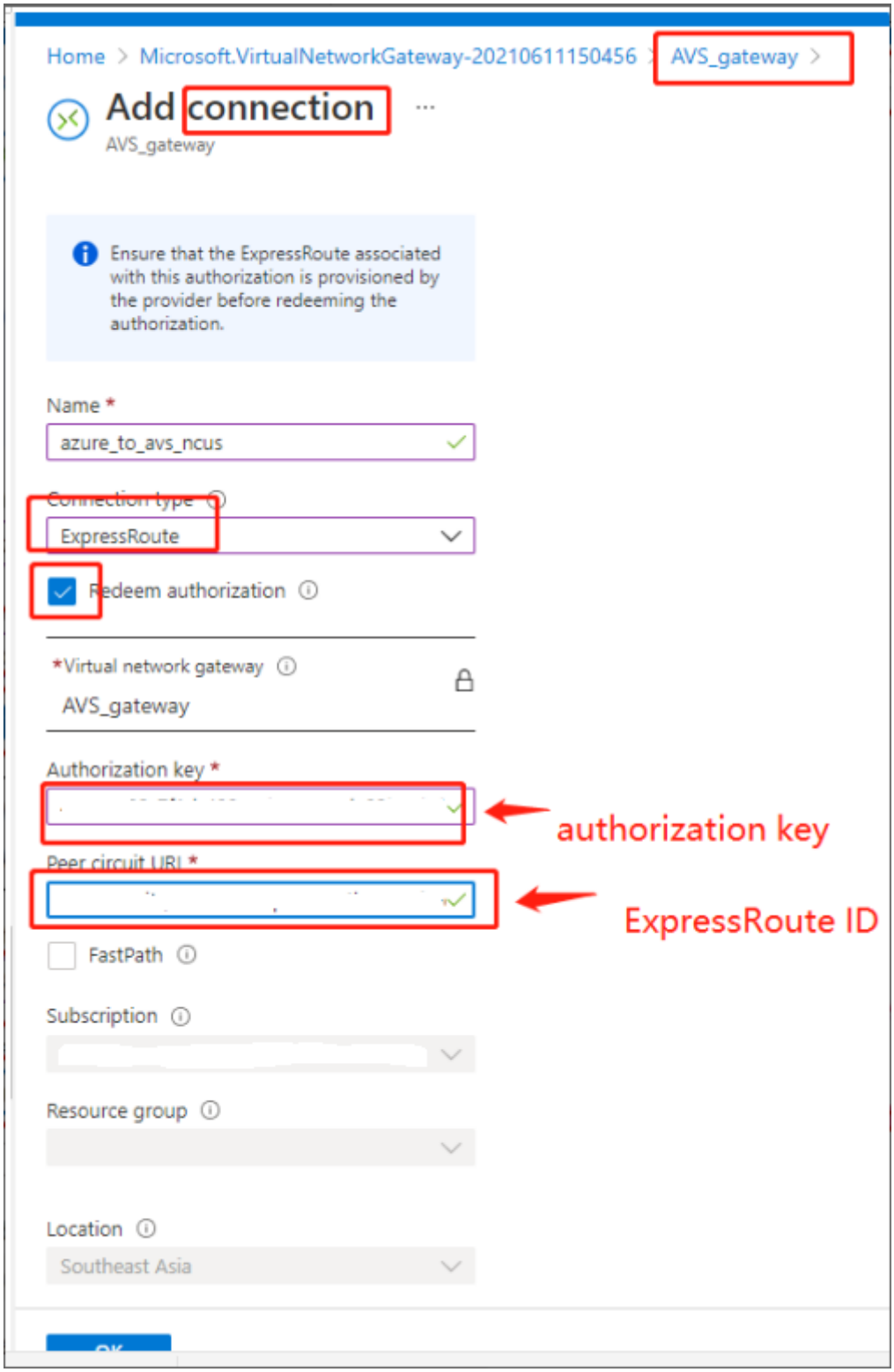
1. Demandez une clé d'autorisation ExpressRoute.

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**.

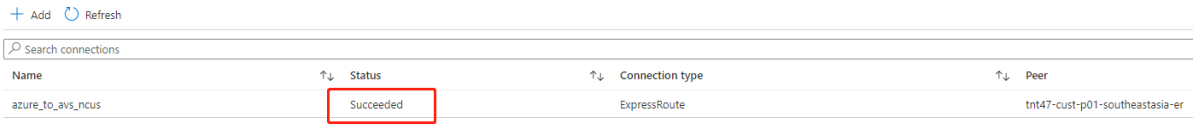


Après avoir demandé une clé d'autorisation :

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**.



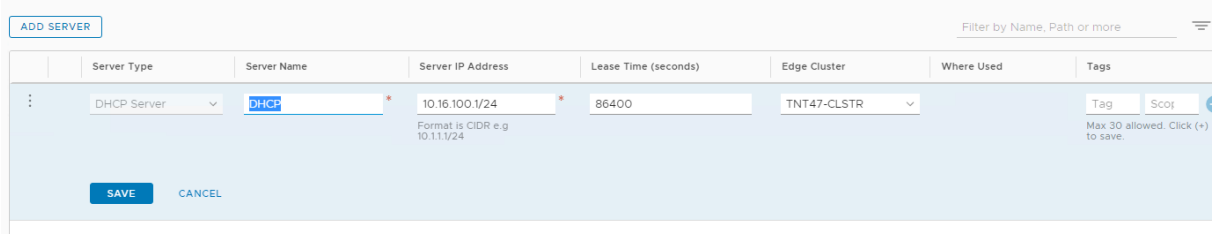
La connexion est établie entre votre circuit ExpressRoute et votre réseau virtuel :



Configurer DHCP pour la solution Azure VMware Après avoir connecté ExpressRoute à la passerelle virtuelle, configurez DHCP.

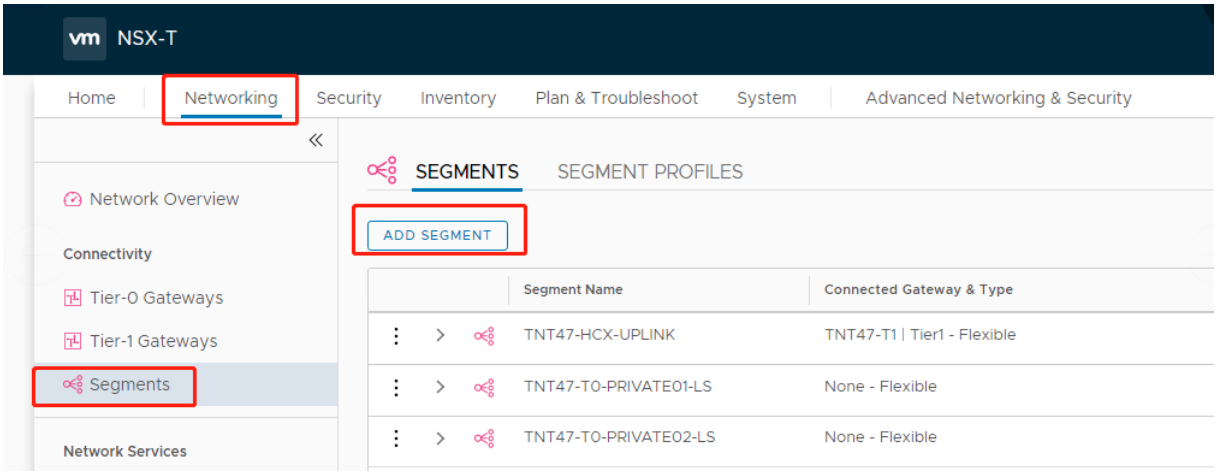
Utiliser NSX-T pour héberger votre serveur DHCP Dans NSX-T Manager :

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**.



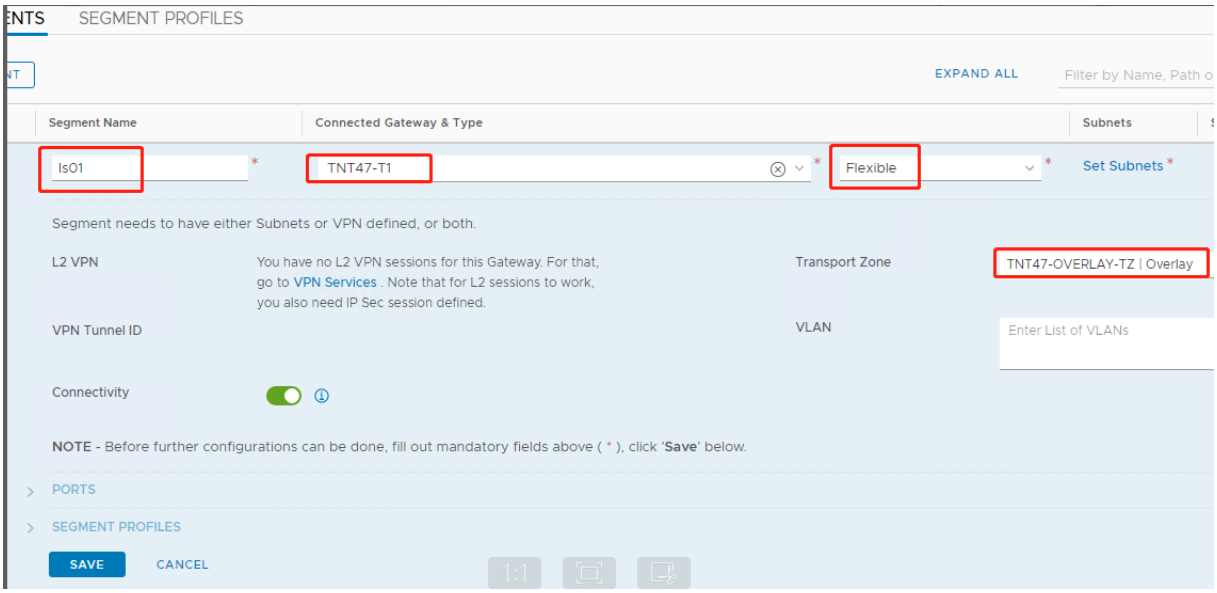
Ajouter un segment réseau dans la solution Azure VMware Après avoir configuré DHCP, ajoutez un segment de réseau.

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**.



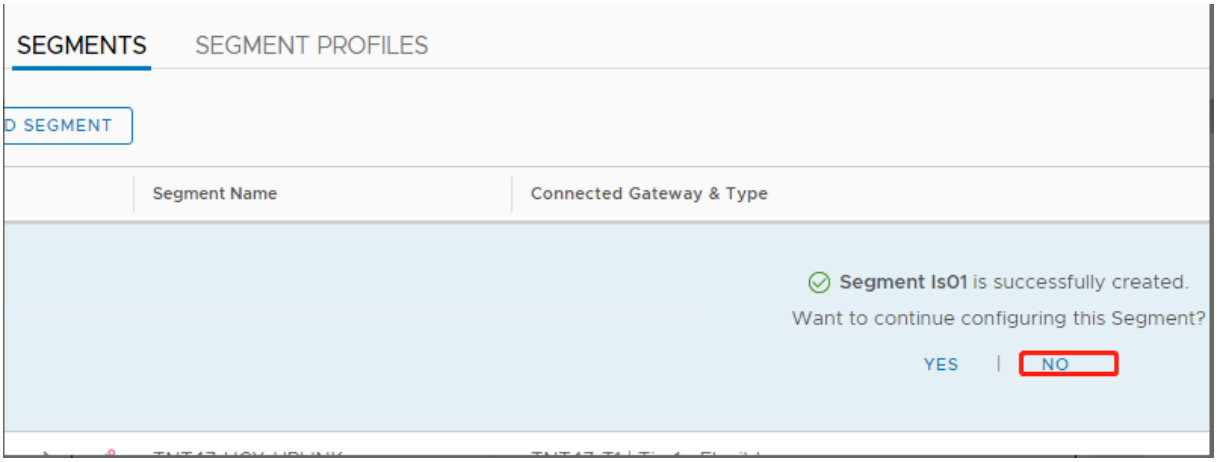
Dans la section **Subnets** :

1. Entrez l'adresse IP de la passerelle.
2. Sélectionnez **Add**.

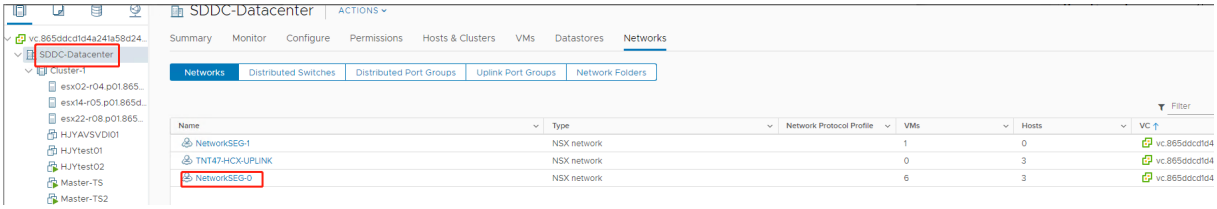
> **Important :**
>
> Cette adresse IP de segment doit appartenir à l'adresse IP de la passerelle Azure, 10.15.0.0/22.

La plage DHCP doit appartenir à l'adresse IP du segment :

Sélectionnez **No** pour refuser l'option de continuer à configurer le segment :



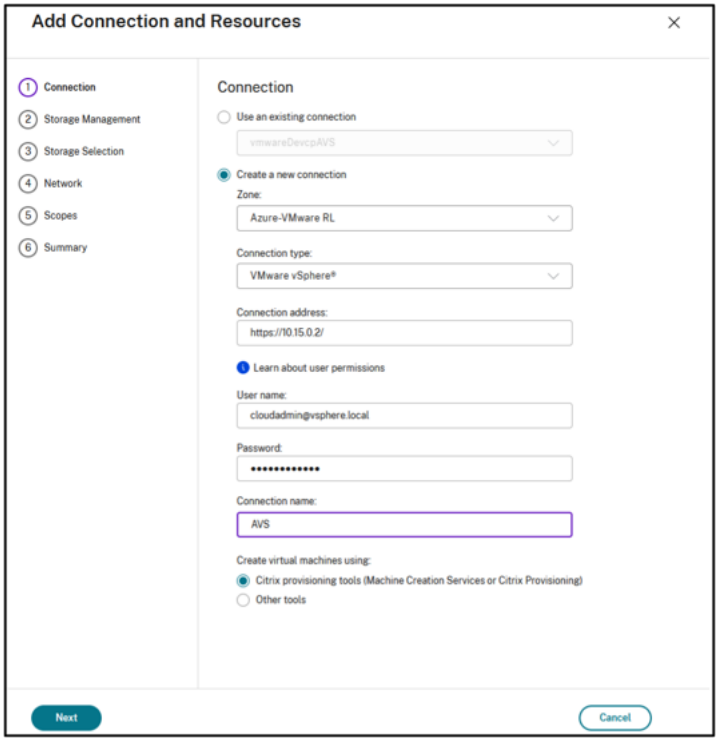
Dans vCenter, sélectionnez **Networking > SDDC-Datacenter** :



Vérifier l'environnement Azure AVS Configurez l'emplacement des ressources du cloud privé AVS et installez deux connecteurs cloud.

Créer la connexion AVS dans Citrix Studio

1. Créez une machine dans vCenter et installez les connecteurs cloud sur la machine. Consultez Configurer des instances.
2. Dans **Gérer > Configuration complète**, sélectionnez Hébergement dans le panneau de gauche.
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.

Google Cloud VMware Engine

Citrix DaaS 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. Avant de poursuivre la création du cloud privé, préparez les conditions suivantes :

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.

   > **Remarque :**
   >
   > Le déploiement HCX ne s'appliquequ'à la version 1.0 du plan IP.

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.
   > - Le déploiement HCX ne s'appliquequ'à la version 1.0 du plan IP.

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 le 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.

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. L'emplacement du VPN doit être le même que celui de la région du cloud privé. 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**.

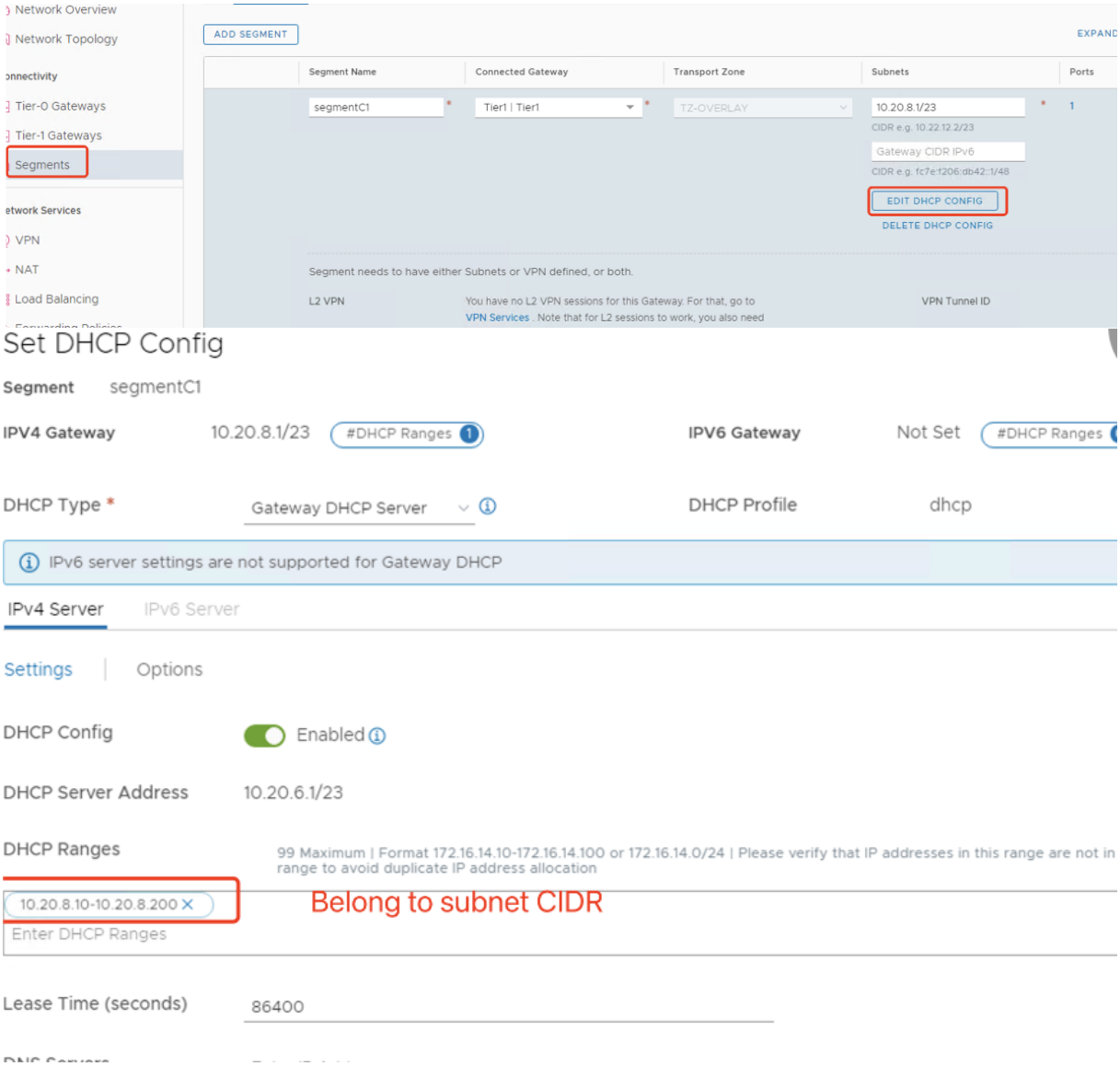
Vous pouvez désormais créer un segment de réseau dans NSX-T. Pour plus d'informations sur DHCP dans NSX-T, consultez la documentation VMware relative à DHCP.

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.

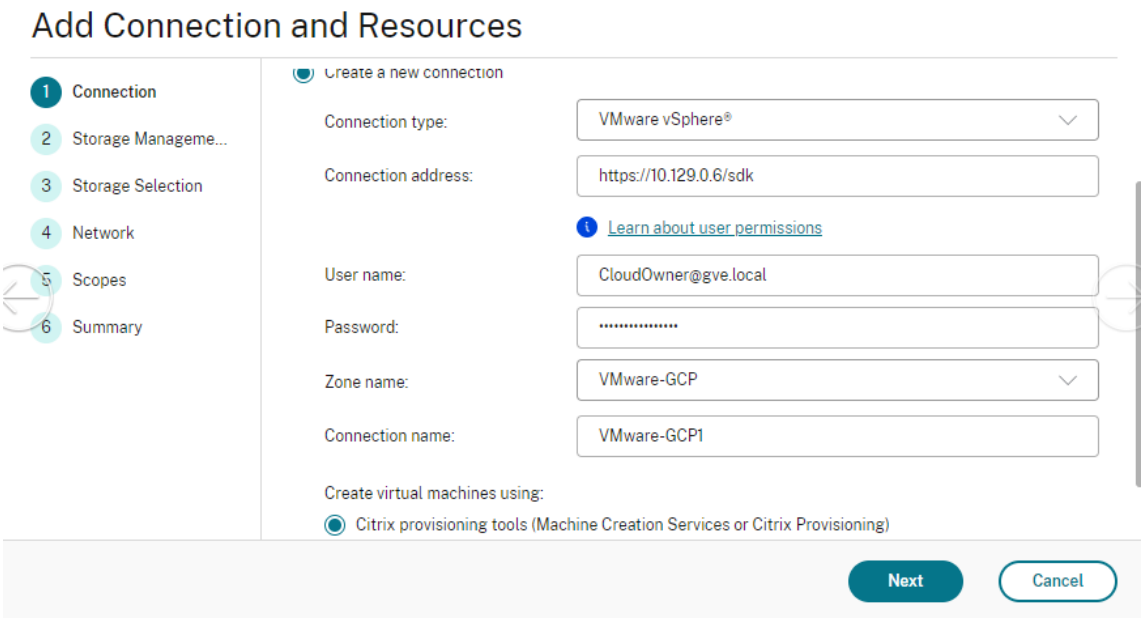
Dans une région donnée, vous pouvez configurer au plus 100 itinéraires uniques entre VMware Engine et votre réseau VPC à l'aide d'un accès aux services privés. Cela inclut, par exemple, les plages d'adresses IP de gestion du cloud privé, les segments de réseau de charge de travail NSX-T et les plages 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 et installez les connecteurs cloud sur la machine. Consultez Configurer des instances.
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.

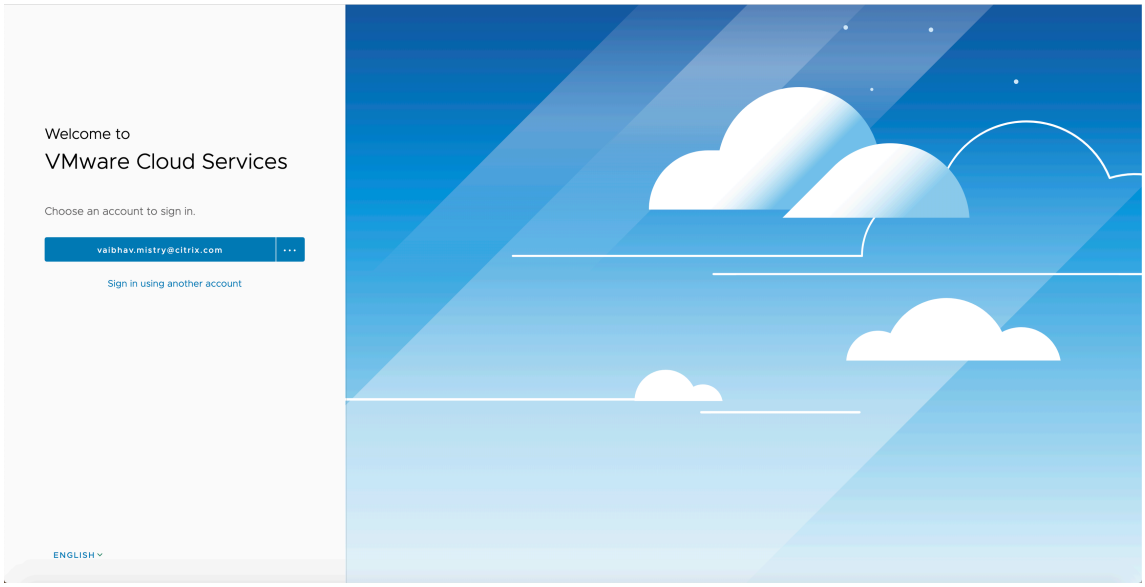
Cloud VMware sur Amazon Web Services (AWS)

VMware Cloud on Amazon Web Services (AWS) vous permet de migrer des charges de travail Citrix sur site basées sur VMware vers AWS Cloud et votre environnement principal Citrix Virtual Apps and Desktops vers Citrix DaaS.

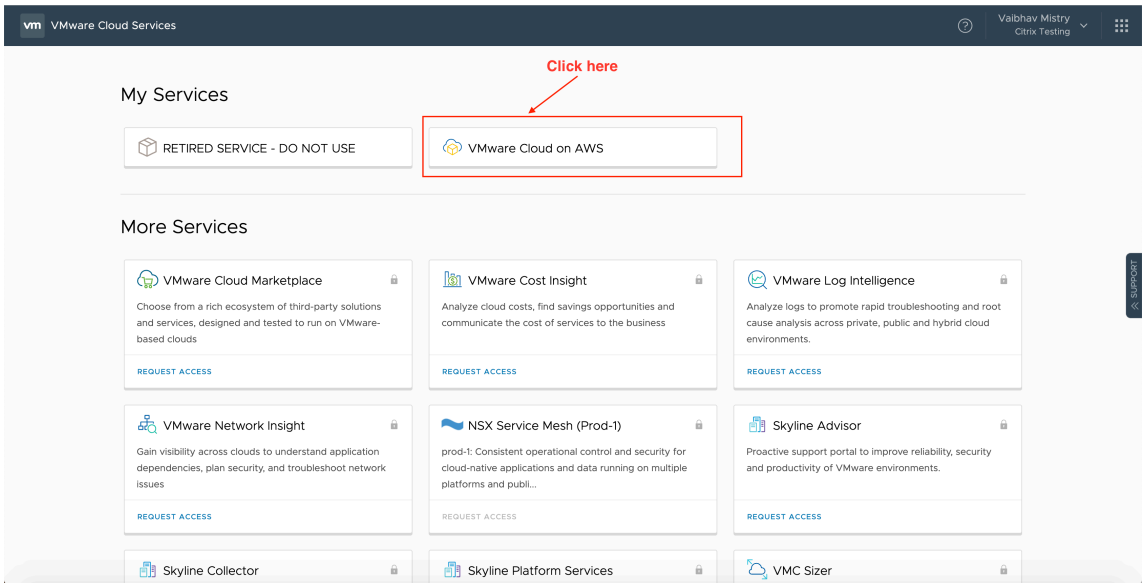
Cet article décrit la procédure à suivre pour configurer un cloud VMware sur AWS.

Accéder à l'environnement cloud VMware

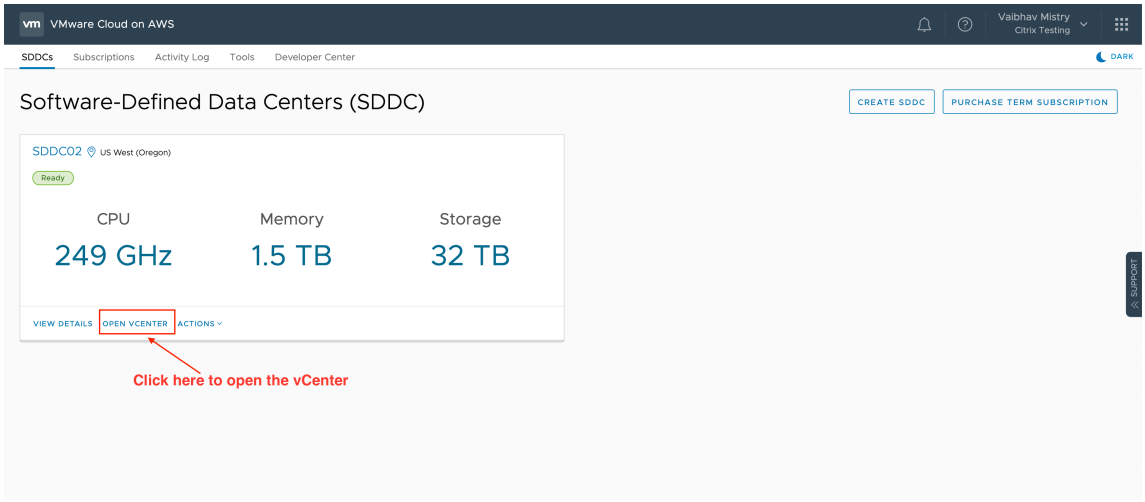
1. Connectez-vous aux services cloud VMware à l'aide de l'URL https://console.cloud.vmware.com/.

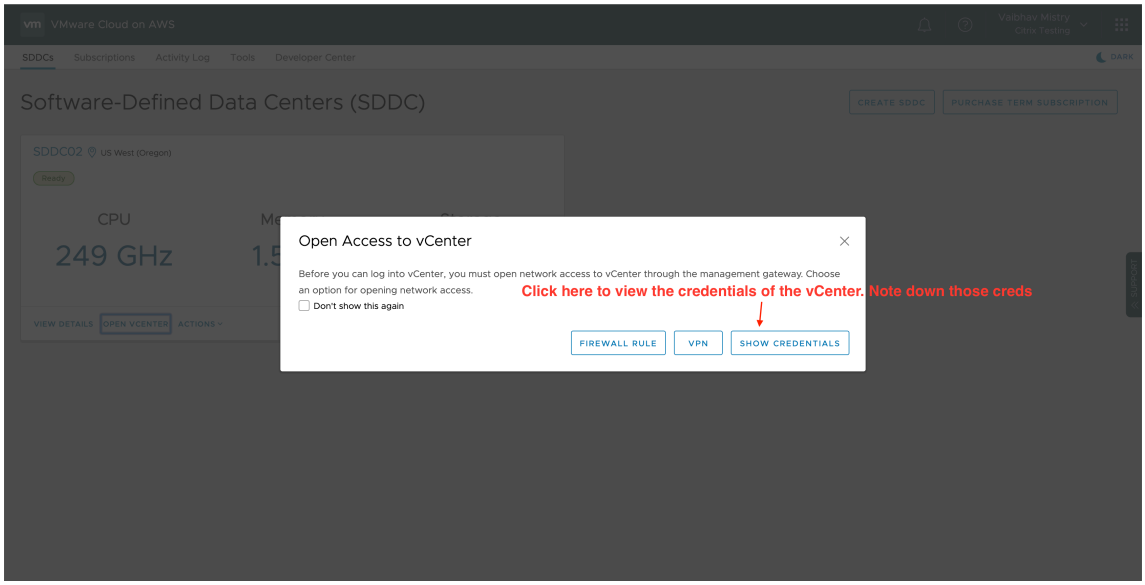


2. Cliquez sur **VMware Cloud on AWS**. La page Software-Defined Data Centers (SDDC) s'affiche.

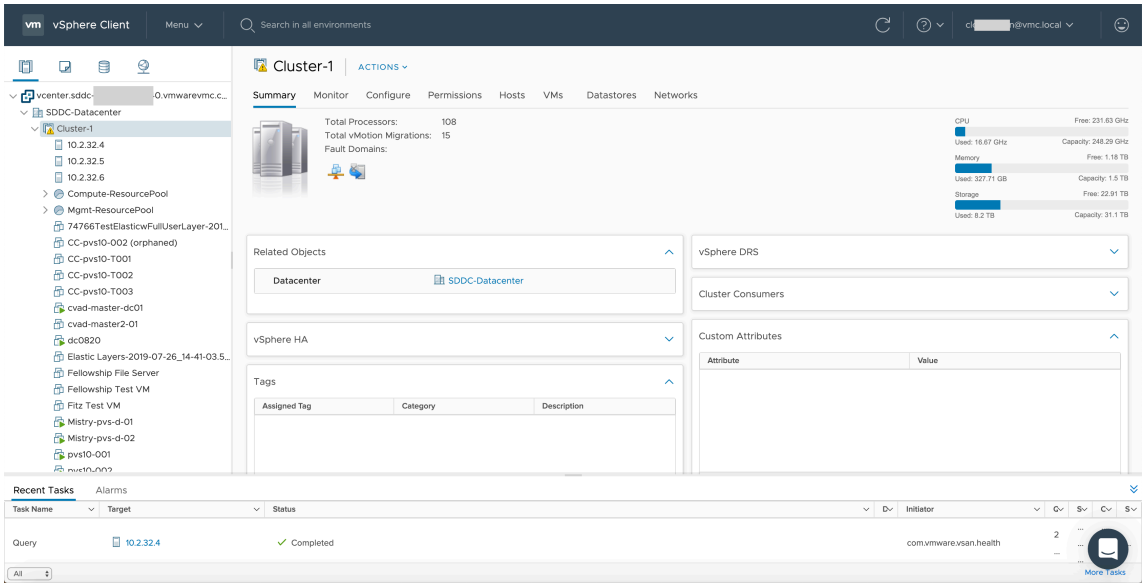


3. Cliquez sur **OPEN VCENTER**, puis sur **SHOW CREDENTIALS**. Notez les informations d'identification pour une utilisation ultérieure.





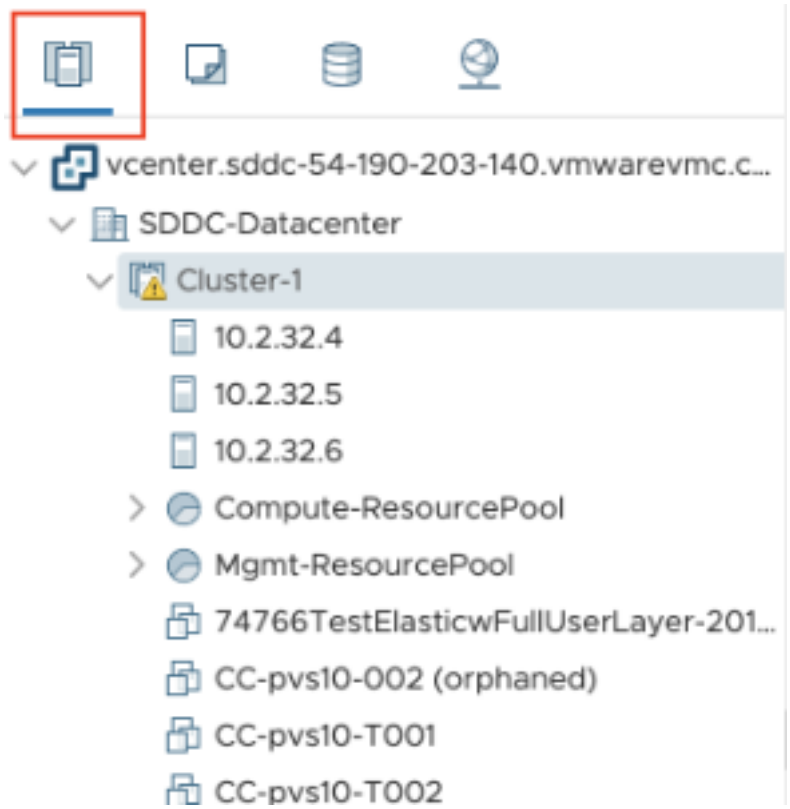
4. Ouvrez un navigateur Web et entrez l'URL de vSphere Web Client.
5. Entrez les informations d'identification que vous avez notées et cliquez sur **Login**. La page Web du client vSphere est similaire à l'environnement local.



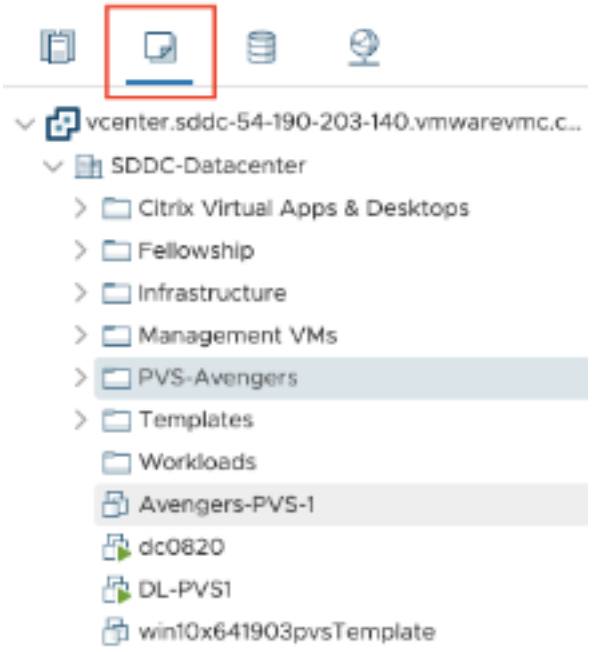
À propos de l'environnement cloud VMware

La page Web du client vSphere propose quatre vues.

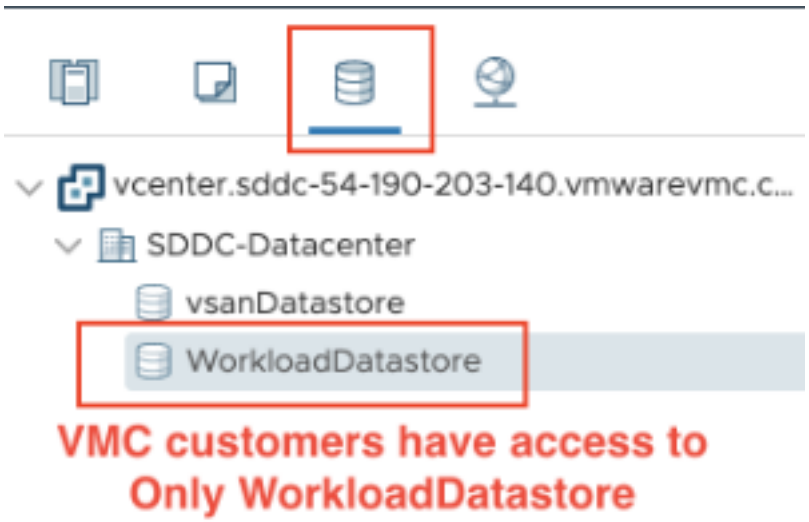
- Vue Hôte et cluster : vous ne pouvez pas créer de nouveau cluster, mais l'administrateur du cloud peut créer plusieurs pools de ressources.



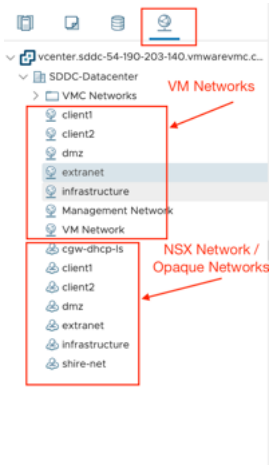
- Vue VM et modèle : l'administrateur du cloud peut créer de nombreux dossiers.



- 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

- Pour un simple déploiement de validation de principe, installez un VDA sur une machine destinée à fournir des applications ou un bureau à vos utilisateurs.

- Pour créer et gérer une connexion, consultez la section Connexion aux solutions partenaires et cloud VMware.
- Passez en revue toutes les étapes du processus d'installation et de configuration.

Informations supplémentaires

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

Environnement de virtualisation XenServer

January 25, 2024

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

Pour configurer XenServer, consultez la section Ajouter un type de ressource.

Autres ressources

- Pour un simple déploiement de validation de principe, installez un VDA sur une machine destinée à fournir des applications ou un bureau à vos utilisateurs.
- Pour créer et gérer des connexions, consultez la section Connexion à XenServer.
- Passez en revue toutes les étapes du processus d'installation et de configuration.

Informations supplémentaires

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

Considérations sur le dimensionnement et la scalabilité des Cloud Connector

January 25, 2024

Lorsque vous évaluez le dimensionnement et la scalabilité de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), tenez compte de tous les composants. Effectuez des recherches et des tests sur la configuration des Citrix Cloud Connector et du StoreFront de manière à déterminer celle qui répond le mieux à vos besoins spécifiques. Des ressources insuffisantes pour le dimensionnement et la scalabilité auront un impact négatif sur les performances de votre déploiement.

> **Remarque :**
>
> - Ces recommandations s'appliquent à Citrix DaaS Standard pour Azure en plus de Citrix DaaS.
> - Les tests et les recommandations présentés dans cet article sont des directives destinées à vous aider à démarrer vos tests. Nous vous recommandons d'effectuer les tests dans votre environnement afin de valider le dimensionnement approprié du connecteur.

Cet article fournit des détails sur les capacités maximales testées, ainsi que des recommandations sur les meilleures pratiques en matière de configuration de la machine Cloud Connector. Les tests ont été réalisés sur des déploiements configurés avec StoreFront et cache d'hôte local (LHC).

Les informations fournies s'appliquent aux déploiements dans lesquels chaque emplacement de ressources contient des charges de travail VDI ou des charges de travail RDS. Pour les emplacements de ressources qui contiennent des charges de travail mixtes VDI et RDS, contactez Citrix Consulting Services.

Le Cloud Connector lie vos charges de travail à Citrix DaaS de la manière suivante :

- Fournit un proxy pour la communication entre vos VDA et Citrix DaaS
- Fournit un proxy pour la communication entre Citrix DaaS et votre Active Directory (AD) et les hyperviseurs
- Dans les déploiements qui incluent des serveurs StoreFront, le Cloud Connector sert de broker de session temporaire pendant les pannes du cloud, fournissant aux utilisateurs un accès continu aux ressources

Il est important que vos Cloud Connector soient correctement dimensionnés et configurés pour répondre à vos besoins spécifiques.

Chaque ensemble de Cloud Connector est affecté à un emplacement de ressources (également appelé zone). Un emplacement de ressources est une séparation logique qui spécifie les ressources qui communiquent avec cet ensemble de Cloud Connector. Au moins un emplacement de ressources est requis par domaine pour communiquer avec Active Directory (AD).

Chaque catalogue de machines et chaque connexion d'hébergement sont affectés à un emplacement de ressources.

Pour les déploiements avec plusieurs emplacements de ressources, attribuez des catalogues de machines et des VDA aux emplacements de ressources afin d'optimiser la capacité du LHC à négocier les

connexions pendant les pannes. Pour plus d'informations sur la création et la gestion des emplacements de ressources, consultez la section Se connecter à Citrix Cloud. Pour des performances optimales, configurez vos Cloud Connector sur des connexions à faible latence vers des VDA, des serveurs AD et des hyperviseurs.

Processeurs et systèmes de stockage recommandés

Pour des performances similaires à celles observées dans ces tests, utilisez des processeurs modernes prenant en charge les extensions SHA. Les extensions SHA réduisent la charge cryptographique sur le processeur. Les processeurs recommandés sont les suivants :

- Advanced Micro Devices (AMD) Zen et processeurs plus récents
- Intel Ice Lake et processeurs plus récents

Les processeurs recommandés fonctionnent efficacement. Vous pouvez utiliser des processeurs plus anciens, mais cela peut entraîner une augmentation de la charge du processeur. Pour compenser ce comportement, nous vous recommandons d'augmenter le nombre de processeurs virtuels.

Les tests décrits dans cet article ont été réalisés avec des processeurs AMD EPYC et Intel Cascade Lake.

Les Cloud Connector ont une charge cryptographique importante lorsqu'ils communiquent avec le cloud. Les Cloud Connector utilisant des processeurs avec des extensions SHA ont une charge de processeur plus faible, ce qui se traduit par une utilisation plus faible du processeur par le service LSASS (Local Security Authority Subsystem Service).

Citrix recommande d'utiliser un système de stockage moderne avec des opérations d'E/S par seconde (IOPS) adéquates, en particulier pour les déploiements qui utilisent le LHC. Les disques SSD (Solid State Drive) sont recommandés, mais des niveaux de stockage cloud premium ne sont pas nécessaires. Des IOPS plus élevées sont nécessaires pour les scénarios LHC dans lesquels le Cloud Connector exécute une petite copie de la base de données. Cette base de données est régulièrement mise à jour en fonction des modifications apportées à la configuration du site et fournit des fonctionnalités de négociation à l'emplacement des ressources en cas de panne de Citrix Cloud.

Configuration de calcul recommandée pour le cache d'hôte local

Le cache d'hôte local (LHC) fournit une haute disponibilité en permettant aux opérations de négociation de connexion dans un déploiement de se poursuivre lorsqu'un Cloud Connector ne peut pas communiquer avec Citrix Cloud.

Les Cloud Connector exécutent Microsoft SQL Express Server LocalDB, qui est automatiquement installé lorsque vous installez le Cloud Connector. La configuration du processeur du Cloud Connector, en particulier le nombre de cœurs disponibles pour SQL Express Server LocalDB, affecte directement

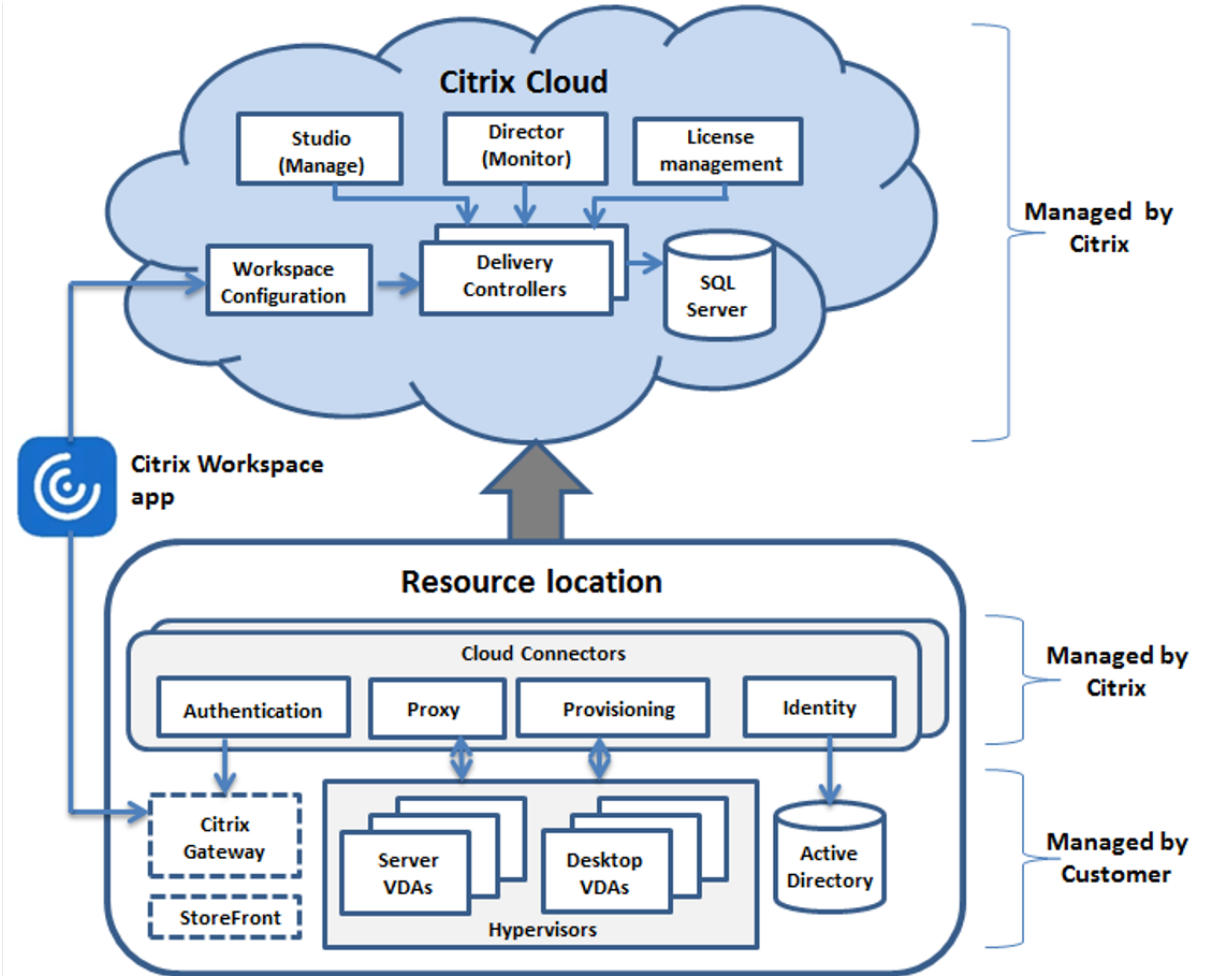
les performances du LHC. Le nombre de cœurs de processeur disponibles pour SQL Server Express Server LocalDB affecte les performances du LHC encore plus que l'allocation de mémoire. Cette surcharge du processeur est observée uniquement en mode LHC lorsque Citrix DaaS n'est pas accessible et que le broker LHC est actif. Pour tout déploiement utilisant le LHC, Citrix recommande quatre cœurs par socket, avec un minimum de quatre cœurs de processeur par Cloud Connector. Pour plus d'informations sur la configuration des ressources de calcul pour SQL Express Server LocalDB, consultez Limites de capacité de calcul des éditions SQL Server.

Si les ressources de calcul disponibles pour SQL Express Server LocalDB sont mal configurées, les temps de synchronisation de la configuration peuvent être augmentés et les performances pendant les pannes peuvent être réduites. Dans certains environnements virtualisés, la capacité de calcul peut dépendre du nombre de processeurs logiques et non des cœurs de processeur.

Résumé des résultats des tests

Tous les résultats présentés sont basés sur un environnement de test tel que configuré dans les sections détaillées de cet article. Les résultats présentés ici concernent un seul emplacement de ressources. Des configurations de système différentes peuvent donner des résultats différents.

Cette illustration donne une présentation graphique de la configuration testée.



Ce tableau fournit un guide rapide pour dimensionner votre emplacement de ressources. 10 000 est la valeur maximale pour un seul emplacement de ressources. Reportez-vous à la section Limites pour plus d'informations sur les limites d'emplacement de ressources.

> **Remarque :**
>
> Le dépassement de cette limite peut entraîner des problèmes de connectivité et de performances en cas de panne. Par conséquent, vous ne devez pas dépasser la limite recommandée, car cela peut entraîner le non-enregistrement de VDA.

Les résultats sont basés sur des tests internes de Citrix. Les configurations décrites ont été testées avec différentes charges de travail, notamment des tests de lancement de session à haut débit et des tempêtes d'enregistrement.

	Moyen	Élevé	Maximum
VDA	1000 VDI ou 250 RDS	5000 VDI ou 500 RDS	10 000 VDI ou 1 000 RDS

	Moyen	Élevé	Maximum
Connexions d'hébergement	20	40	40
Processeurs pour connecteurs	4 processeurs virtuels	4 processeurs virtuels	8 processeurs virtuels
Mémoire pour connecteurs	6 Go	8 Go	10 Go

Méthodologie des tests

Des tests ont été effectués pour ajouter de la charge et mesurer les performances des composants de l'environnement. Les composants ont été surveillés en collectant des données de performance et la durée des procédures (telles que le temps de connexion et le délai d'enregistrement). Parfois, des outils de simulation propriétaires Citrix sont utilisés pour simuler des VDA et des sessions. Ces outils sont conçus pour utiliser les composants Citrix de la même manière que des sessions et des VDA traditionnels, sans avoir à héberger de sessions et VDA réels. Les tests ont été réalisés à la fois en mode négociation cloud et en mode LHC pour des scénarios avec Citrix StoreFront.

Les recommandations relatives au dimensionnement de Cloud Connector dans cet article sont basées sur les données collectées à partir de ces tests.

Les tests suivants ont été effectués :

- **Tempête de connexion de session/lancement :** test qui simule des périodes de connexion très élevées.
- **Tempête d'enregistrement de VDA :** test qui simule des périodes d'enregistrement de VDA très élevées. Par exemple, après un cycle de mise à niveau ou une transition entre le mode négociation cloud et le mode cache d'hôte local.
- **Tempête d'action d'alimentation de VDA :** test qui simule un volume élevé d'actions d'alimentation de VDA.

Scénarios et conditions de test

Ces tests ont été réalisés avec le LHC configuré. Pour plus d'informations sur l'utilisation du LHC, consultez l'article Cache d'hôte local. Le LHC nécessite un serveur StoreFront sur site. Pour obtenir des informations détaillées sur StoreFront, consultez la documentation produit StoreFront.

Recommandations pour les configurations StoreFront :

- Si vous avez plusieurs emplacements de ressources avec un seul serveur ou groupe de serveurs StoreFront, activez l'option de vérification de l'intégrité avancée pour le magasin StoreFront. Consultez la section Exigences de StoreFront dans l'article Cache d'hôte local
- Pour des taux de lancement de session plus élevés, utilisez un groupe de serveurs StoreFront. Consultez Configurer des groupes de serveurs dans la documentation produit StoreFront.

Conditions d'essai :

- Les exigences en matière de processeur et de mémoire concernent uniquement le système d'exploitation de base et les services Citrix. Les applications et services tiers peuvent nécessiter des ressources supplémentaires.
- Les VDA sont des machines virtuelles ou physiques exécutant Citrix Virtual Delivery Agent.
- Les tests sont effectués à l'aide de Windows VDA seulement.
- L'alimentation de tous les VDA testés était gérée à l'aide de Citrix DaaS.
- Des charges de travail de 1 000 à 10 000 serveurs VDI et de 250 à 1 000 serveurs RDS avec 1 000 à 20 000 sessions ont été testées.
- Les sessions RDS ont été testées avec jusqu'à 20 000 par emplacement de ressources.
- Les tests ont été effectués à l'aide d'un Cloud Connector à la fois en fonctionnement normal et en cas de panne. Citrix recommande d'utiliser au moins deux composants Cloud Connector pour garantir une haute disponibilité. En mode panne, un seul des connecteurs est utilisé pour les enregistrements et la négociation des connexions des VDA.
- Les tests ont été réalisés avec le Cloud Connector configuré avec les processeurs Intel Cascade Lake.
- Les sessions ont été lancées via un seul serveur Citrix StoreFront.
- Les tests de lancement de sessions de panne du LHC ont été effectués après le réenregistrement des machines.

Le nombre de sessions RDS est une recommandation et non une limite. Testez votre propre limite de sessions RDS dans votre environnement.

> **Remarque :**
>
> Le nombre de sessions et le taux de lancement sont plus importants pour RDS que le nombre de VDA.

Charges de travail moyennes

Ces charges de travail ont été testées avec 4 processeurs virtuels et 6 Go de mémoire.

Charges de travail test	État du site	Durée d'enregistrement du VDA	Utilisation du processeur et de la mémoire	Durée du test de lancement	Utilisation du processeur et de la mémoire pour le lancement	Taux de lancement
1 000 VDI	En ligne	5 minutes	Maximum processeur = 36 %, moyenne processeur = 33 %, maximum mémoire = 5,3 Go	2 minutes	Maximum processeur = 29 %, moyenne processeur = 27 %, maximum mémoire = 3,7 Go	500 par minute
1 000 VDI	Panne	4 minutes	Maximum processeur = 11 %, moyenne processeur = 10 %, maximum mémoire = 4,5 Go	2 minutes	Maximum processeur = 42 %, moyenne processeur = 28 %, maximum mémoire = 4 Go	500 par minute
250 RDS, 5 000 sessions	En ligne	3 minutes	Maximum processeur = 14 %, moyenne processeur = 4 %, maximum mémoire = 3,5 Go	9 minutes	Maximum processeur = 46 %, moyenne processeur = 21 %, maximum mémoire = 3,7 Go	555 par minute

Charges de travail test	État du site	Durée d'enregistrement du VDA	Utilisation du processeur et de la mémoire	Durée du test de lancement	Utilisation du processeur et de la mémoire pour le lancement	Taux de lancement
250 RDS, 5 000 sessions	Panne	3 minutes	Maximum processeur = 15 %, moyenne processeur = 5 %, maximum mémoire = 3,7 Go	9 minutes	Maximum processeur = 51 %, moyenne processeur = 32 %, maximum mémoire = 4,2 Go	555 par minute

Charges de travail importantes

Ces charges de travail ont été testées avec 4 processeurs virtuels et 8 Go de mémoire.

Charges de travail test	État du site	Durée d'enregistrement du VDA	Utilisation du processeur et de la mémoire	Durée du test de lancement	Utilisation du processeur et de la mémoire pour le lancement	Taux de lancement
5 000 VDI	En ligne	3 à 4 minutes	Maximum processeur = 45 %, moyenne processeur = 25 %, maximum mémoire = 7 Go	5 minutes	Maximum processeur = 75 %, moyenne processeur = 55 %, maximum mémoire = 7 Go	1 000 par minute

Charges de travail test	État du site	Durée d'enregistrement du VDA	Utilisation du processeur et de la mémoire	Durée du test de lancement	Utilisation du processeur et de la mémoire pour le lancement	Taux de lancement
5 000 VDI	Panne	4 à 6 minutes	Maximum processeur = 15 %, moyenne processeur = 5 %, maximum mémoire = 7,5 Go	5 minutes	Maximum processeur = 45 %, moyenne processeur = 40 %, maximum mémoire = 7,5 Go	1 000 par minute
500 RDS, 10 000 sessions	En ligne	3 minutes	Maximum processeur = 45 %, moyenne processeur = 25 %, maximum mémoire = 7 Go	10 minutes	Maximum processeur = 75 %, moyenne processeur = 55 %, maximum mémoire = 7 Go	1 000 par minute
500 RDS, 10 000 sessions	Panne	3 minutes	Maximum processeur = 15 %, moyenne processeur = 5 %, maximum mémoire = 7,5 Go	10 minutes	Maximum processeur = 45 %, moyenne processeur = 40 %, maximum mémoire = 7,5 Go	1 000 par minute

Charges de travail maximales

Ces charges de travail ont été testées avec 8 processeurs virtuels et 10 Go de mémoire.

Charges de travail test	État du site	Durée d'enregistrement du VDA	Utilisation du processeur et de la mémoire	Durée du test de lancement	Utilisation du processeur et de la mémoire pour le lancement	Taux de lancement
10 000 VDI	En ligne	3 à 4 minutes	Maximum processeur = 85 %, moyenne processeur = 10 %, maximum mémoire = 8,5 Go	7 minutes	Maximum processeur = 66 %, moyenne processeur = 28 %, maximum mémoire = 7 Go	1 400 par minute
10 000 VDI	Panne	4 à 5 minutes	Maximum processeur = 90 %, moyenne processeur = 17 %, maximum mémoire = 8,2 Go	5 minutes	Maximum processeur = 90 %, moyenne processeur = 45 %, maximum mémoire = 8,5 Go	2 000 par minute
1 000 RDS, 20 000 sessions	En ligne	1 à 2 minutes	Maximum processeur = 60 %, moyenne processeur = 20 %, maximum mémoire = 8,6 Go	17 minutes	Maximum processeur = 66 %, moyenne processeur = 25 %, maximum mémoire = 6,8 Go	1 200 par minute

Charges de travail test	État du site	Durée d'enregistrement du VDA	Utilisation du processeur et de la mémoire	Durée du test de lancement	Utilisation du processeur et de la mémoire pour le lancement	Taux de lancement
1 000 RDS, 20 000 sessions	Panne	3 à 4 minutes	Maximum processeur = 22 %, moyenne processeur = 10 %, maximum mémoire = 8,5 Go	21 minutes	Maximum processeur = 90 %, moyenne processeur = 50 %, maximum mémoire = 7,5 Go	1 000 par minute

> **Remarque :**
>
> Les charges de travail indiquées ici sont les charges maximales recommandées pour un emplacement de ressources. Pour prendre en charge des charges de travail plus importantes, ajoutez d'autres emplacements de ressources.

Utilisation des ressources de synchronisation de la configuration

Le processus de synchronisation de la configuration maintient les Cloud Connector à jour avec Citrix DaaS. Les mises à jour sont automatiquement envoyées aux Cloud Connector pour s'assurer que les Cloud Connector sont prêts à prendre en charge la négociation en cas de panne. La synchronisation de la configuration met à jour la base de données du LHC, SQL Express Server LocalDB. Le processus importe les données dans une base de données temporaire, puis bascule vers cette base de données une fois importées. Cela garantit qu'il existe toujours une base de données LHC prête à prendre le relais.

L'utilisation du processeur, de la mémoire et du disque augmente temporairement pendant l'importation des données dans la base de données temporaire.

Résultats des tests :

- **Durée d'importation des données :** 7 à 10 minutes
- **Utilisation du processeur :**

  - maximum = 25 %
  - moyenne = 15 %

- **Utilisation de la mémoire :**
  - maximum = 9 Go
  - augmentation d'environ 2 Go à 3 Go
- **Utilisation du disque :**
  - Pic de lecture du disque de 4 Mo/s
  - Pic d'écriture sur le disque de 18 Mo/s
  - Pic d'écriture sur le disque de 70 Mo/s pendant le téléchargement et l'écriture de fichiers de configuration XML
  - Pic de lecture du disque de 4 Mo/s à la fin de l'importation
- **Taille de la base de données LHC :**
  - Fichier de base de données de 400 à 500 Mo
  - Base de données de journaux de 200 à 300 Mo

Conditions d'essai :

- Test sur AMD EPYC à 8 processeurs virtuels
- La base de données de configuration de site importée était destinée à un environnement avec un total de 80 000 VDA à l'échelle du site et 300 000 utilisateurs (trois équipes de 100 000 utilisateurs)
- Le temps d'importation des données a été testé sur un emplacement de ressources avec 10 000 VDI

Autres considérations concernant l'utilisation des ressources :

- Pendant l'importation, les données complètes de configuration du site sont téléchargées. Ce téléchargement peut provoquer un pic de mémoire, en fonction de la taille du site.
- Le site testé utilisait environ 800 Mo pour la base de données et les fichiers journaux de base de données combinés. Lors d'une synchronisation de configuration, ces fichiers sont dupliqués avec une taille combinée maximale d'environ 1 600 Mo. Assurez-vous que votre Cloud Connector dispose de suffisamment d'espace disque pour les fichiers dupliqués. Le processus de synchronisation de configuration échoue si le disque est plein.

Installer des VDA

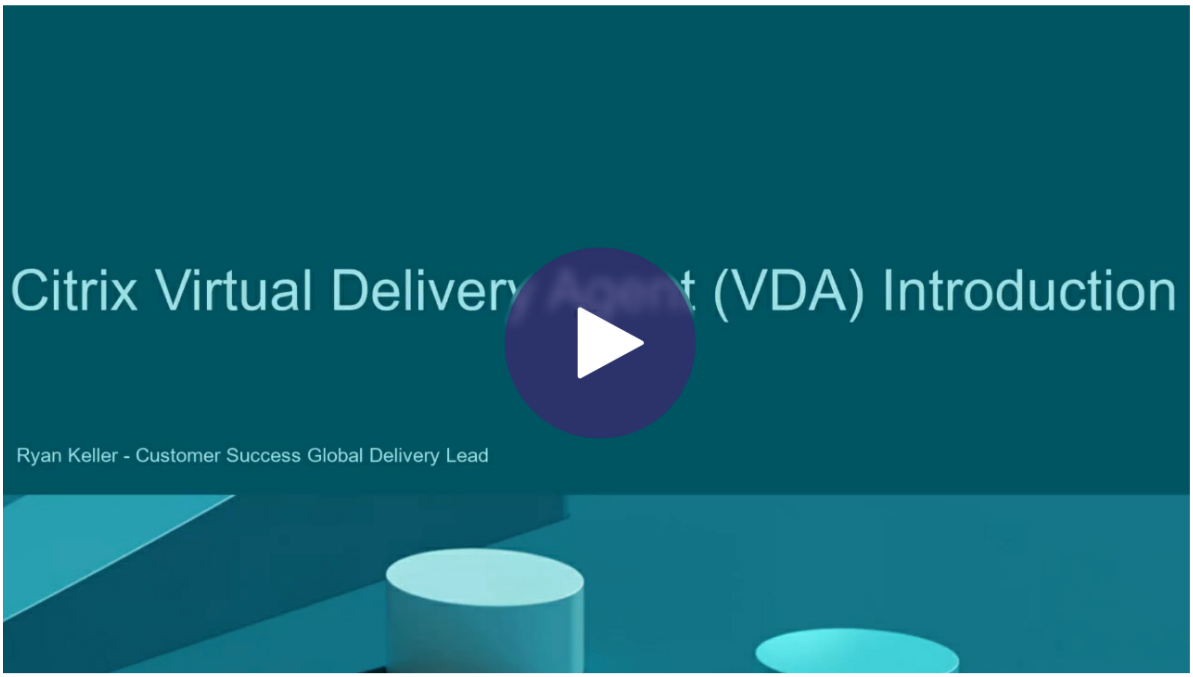
May 17, 2024

Introduction

Cet article commence par une description des VDA Windows et des programmes d'installation de VDA disponibles. Le reste de l'article décrit les étapes de l'assistant d'installation de VDA. Des lignes de commande équivalentes sont fournies. Consultez la section Installer des VDA à l'aide de la ligne de commande pour plus de détails.

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

Consultez une présentation des VDA.



Considérations d'installation

L'article Citrix DaaS décrit ce que sont les VDA et à quoi ils servent. Vous trouverez ci-après plus d'informations.

- **Collection d'analyses :** des données d'analyse sont collectées lorsque vous installez ou 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. De plus, lors d'une installation ou d'une mise à niveau, vous avez la possibilité de vous inscrire à Call Home.

  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.

Pour de plus amples informations sur ces programmes, consultez Citrix Insight Services.

- **Application Citrix Workspace :** l'application Citrix Workspace pour Windows n'est pas installée par défaut lorsque vous installez un VDA. Vous pouvez télécharger et installer ou 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 du Workspace ou d'un serveur StoreFront.
- **Service de spouleur d'impression :** le service de spouleur d'impression Microsoft doit être activé. Vous ne pourrez pas correctement installer un VDA si ce service est désactivé.
- **Microsoft Media Foundation :** la plupart des éditions Windows prises en charge sont fournies avec Media Foundation. Si la machine sur laquelle vous installez un VDA n'est pas dotée de Microsoft Media Foundation (éditions N par exemple), plusieurs fonctionnalités multimédia ne sont pas installées et ne fonctionnent pas.

  - Redirection Flash
  - 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.
- **Groupes d'utilisateurs locaux :** lorsque vous installez le VDA, un nouveau groupe d'utilisateurs locaux appelé Direct Access Users est créé automatiquement. Pour un VDA avec OS monosession, ce groupe s'applique uniquement aux connexions RDP. Pour un VDA avec OS multisession, ce groupe s'applique aux connexions ICA et RDP.
- **Exigences en matière d'adresse Cloud Connector :** le VDA doit avoir au moins une adresse de Cloud Connector valide (dans le même emplacement de ressources) avec laquelle communiquer. Sinon, les sessions ne peuvent pas être établies. Vous spécifiez les adresses de Cloud Connector lorsque vous installez le VDA. Pour plus d'informations sur les autres méthodes permettant de spécifier des adresses de Cloud Connector auprès desquelles les VDA peuvent s'enregistrer, consultez la section Enregistrement de VDA.
- **Considérations sur le système d'exploitation :**

  - Consultez Configuration système requise pour connaître les plates-formes, systèmes d'exploitation et versions pris en charge.
  - Assurez-vous que chaque système d'exploitation dispose des dernières mises à jour.
  - Assurez-vous que les horloges système des VDA sont synchronisées. L'infrastructure Kerberos qui sécurise la communication entre les machines requiert une synchronisation.
  - Le guide d'optimisation pour les machines Windows 10 est disponible dans l'article CTX216252.
  - 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 VDA, un message décrit vos options. Par exemple, si vous tentez d'installer le dernier VDA sur une machine Windows de version plus ancienne, un message vous guide vers l'article CTX139030. Pour de plus amples informations, consultez la section Systèmes d'exploitation antérieurs.

- **MSI installés :** plusieurs MSI sont installés automatiquement lorsque vous installez un VDA. Vous pouvez empêcher l'installation de certains MSI sur la page **Composants supplémentaires** de l'interface graphique ou avec l'option `/exclude` de l'interface de ligne de commande. Pour d'autres, la seule façon d'empêcher leur installation consiste à utiliser l'option `/exclude` de l'interface de ligne de commande.
- **Appartenant au domaine :** assurez-vous que la machine appartient à un domaine avant d'installer le logiciel 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, consultez CTX207624.
- Utilitaire de nettoyage de VDA : pour plus de détails, voir l'article CTX209255.

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 durant l'installation de VDA

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

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

- Assurez-vous qu'une version de Microsoft .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.

Après chaque redémarrage, l'installation du VDA continue. Si vous installez à partir de la ligne de commande, vous pouvez empêcher le redémarrage automatique avec l'option `/noresume`.

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. Ce redémarrage ne peut pas être évité.

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

> **Remarque :**
>
> Cette fonctionnalité n'est disponible que pour les VDA mono-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.

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.

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`).

Pour activer cette fonctionnalité lors de l'installation ou de la mise à niveau d'un VDA mono-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 n'est pas utilisé, mais il est conservé.

- Exécutez un programme d'installation VDA avec l'option `/enablerestore` ou `/enablerestoreclean`.

  - Si vous utilisez l'option `/enablerestorecleanup` et que l'installation ou la mise à niveau se termine correctement, le point de restauration 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 de VDA

Les programmes d'installation de VDA peuvent être téléchargés directement depuis la console Citrix Cloud.

Par défaut, les fichiers contenus dans les programmes d'installation auto-extractibles sont extraits dans le dossier `Temp`. 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 avec OS multi-session.

VDAWorkstationSetup.exe installe un VDA avec OS mono-session.

VDAWorkstationCoreSetup.exe installe un VDA avec 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. Ce programme d'installation déploie uniquement les services fondamentaux nécessaires aux connexions VDA. Par conséquent, il ne prend en charge qu'un sous-ensemble des options qui sont valides avec le programme d'installation VDAWorkstationSetup.

Ce programme d'installation pour la version actuelle n'installe pas ou ne contient pas les composants utilisés pour :

- App-V.
- Profile Management. L'exclusion de Citrix Profile Management de l'installation affecte les écrans de Surveillance.
- Machine Identity Service.
- Application Citrix Workspace pour Windows.
- Outils de prise en charge Citrix.
- Citrix Files pour Windows.
- Citrix Files pour Outlook.
- Cache en écriture des E/S de MCS pour optimiser le stockage.

Ce programme d'installation n'installe pas et ne contient pas l'application Citrix Workspace pour Windows.

Ce programme d'installation installe automatiquement le fichier MSI de redirection du contenu du navigateur. L'installation automatique s'applique aux VDA versions 2003 et ultérieures prises en charge.

L'utilisation de `VDAWorkstationCoreSetup.exe` équivaut à l'utilisation du programme d'installation de `VDAWorkstationSetup.exe` 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 des options `/components vda` et `/exclude "Citrix Personalization for App-V - VDA""Personal vDisk ""Machine Identity Service""Citrix Profile Management""Citrix Profile Management WMI Plugin""Citrix Supportability Tools"" Citrix Files for Windows""Citrix Files for Outlook""Citrix MCS IODriver"`.

Si vous installez un VDA avec le programme d'installation `VDAWorkstationCoreSetup.exe` et que vous mettez à niveau ce VDA à l'aide du programme d'installation `VDAWorkstationSetup.exe` à une date ultérieure, vous avez la possibilité d'installer les composants/fonctionnalités omis.

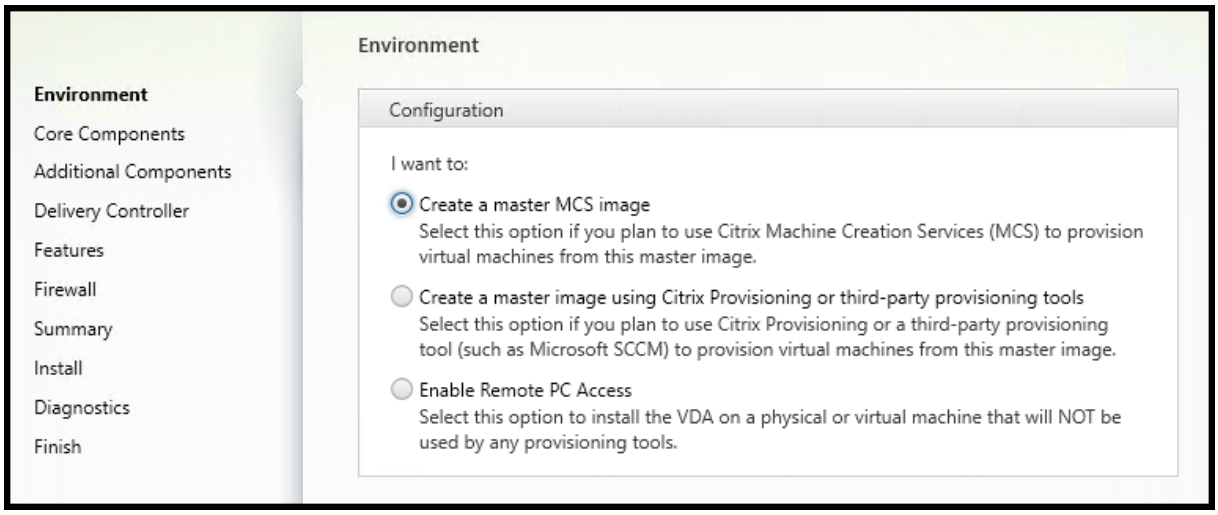
Étape 1. Télécharger le logiciel du produit et démarrer l'assistant

1. Sur la machine sur laquelle vous installez le VDA, connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez Citrix DaaS dans la liste **Mes services**.
3. Sur le côté droit, cliquez sur **Téléchargements** et sélectionnez **Télécharger VDA**. Vous serez redirigé vers la page de téléchargement du VDA. Recherchez le programme d'installation du VDA que vous souhaitez et sélectionnez **Télécharger fichier**.

4. Une fois le téléchargement terminé, cliquez avec le bouton droit sur le fichier et sélectionnez **Exécuter en tant qu'administrateur.** L'assistant d'installation démarre.

Subsidiairement aux étapes 1 à 3, vous pouvez télécharger le VDA directement à partir de la page de téléchargement de Citrix.

Étape 2. 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.

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`

- **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 VM, si vous envisagez d'utiliser Citrix Provisioning ou des outils tiers (tels que Microsoft System Center Configuration Manager). Utilisez cette option pour les machines virtuelles précédemment provisionnées qui ont été démarrées à partir d'un disque de lecture/écriture Citrix Provisioning.

  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.

  Option de ligne de commande : `/remotepc`

- (Apparaît uniquement sur les machines avec OS multi-session) **Activer Remote PC Access** : sélectionnez cette option pour installer un VDA sur une machine physique à utiliser avec Remote PC Access.

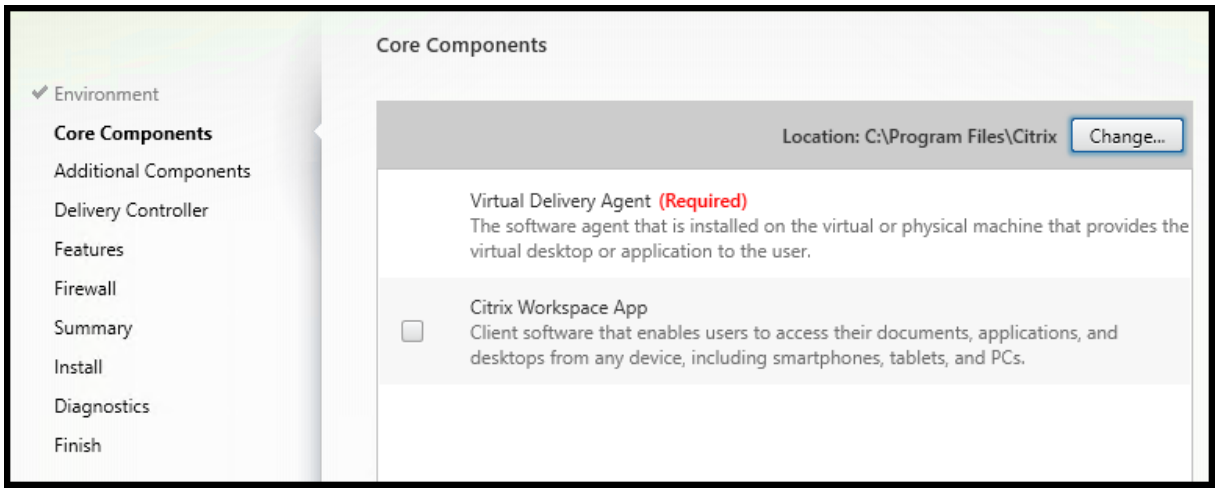
  Option de ligne de commande : `/remotepc`

Sélectionnez **Suivant**.

Cette page ne s'affiche pas :

- Lors de la mise à niveau d'un VDA.
- Lors de l'utilisation du programme d'installation `VDAWorkstationCoreSetup.exe`.

Étape 3. 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 d'exécution pour le service réseau.

  Option de ligne de commande : `/installdir`

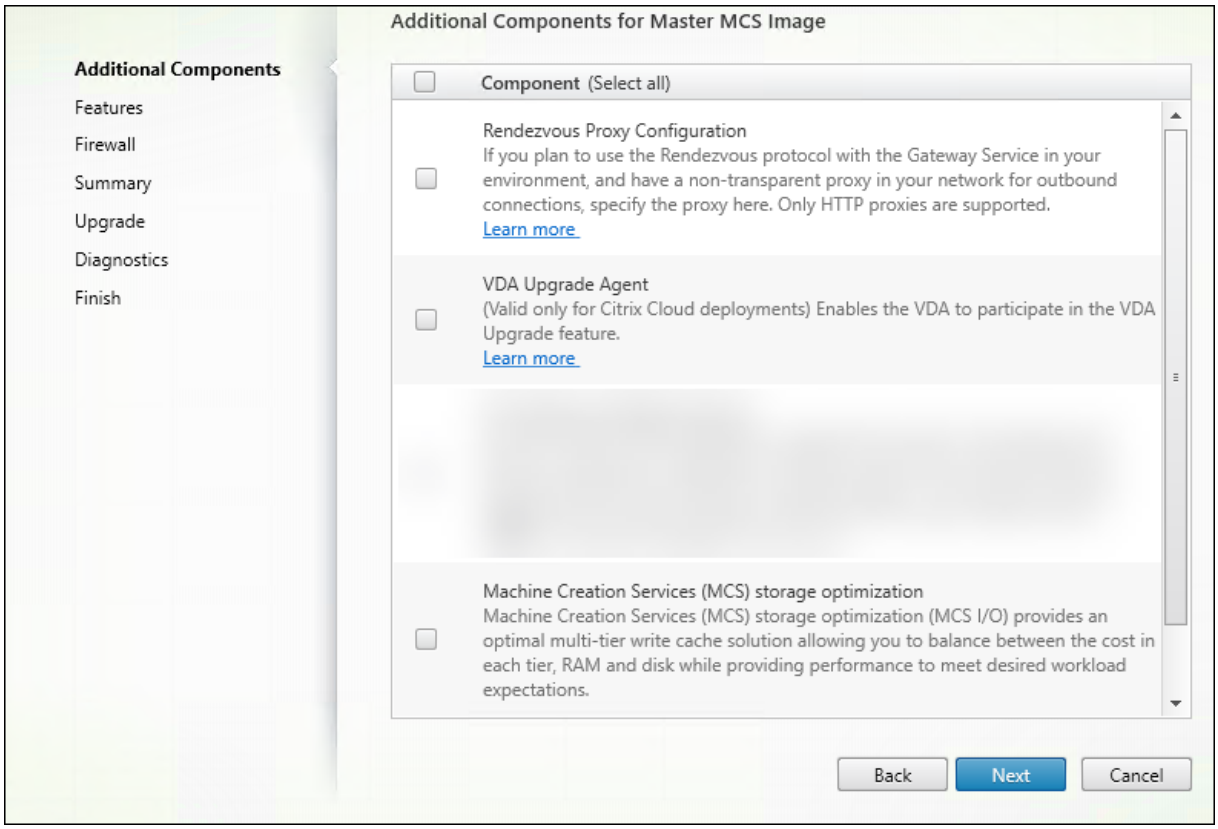
- **Composants :** par défaut, l'application Citrix Workspace pour Windows n'est pas installée avec le VDA. Si vous utilisez le programme d'installation `VDAWorkstationCoreSetup.exe`, l'

application Citrix Workspace pour Windows n'est jamais installée, donc cette case à cocher n'est pas affichée.

Option de ligne de commande : `/components vda,plugin` pour installer le VDA et l'application Citrix Workspace pour Windows.

Sélectionnez **Suivant**.

Étape 4. 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 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 App-V	Non sélectionné	Non sélectionné
Couche de personnalisation de l'utilisateur	Non sélectionné	Non affiché car non valide pour ce cas d'utilisation
Outils de prise en charge Citrix	Sélectionné	Non sélectionné
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
Citrix Files pour Windows	Non sélectionné	Non sélectionné
Citrix Files pour Outlook	Non sélectionné	Non sélectionné
Optimisation du stockage MCS (Machine Creation Services)	Non sélectionné	Non sélectionné
Configuration du protocole Rendezvous	Non sélectionné	Non sélectionné

Cette page ne s'affiche pas :

- Lors de l'utilisation du 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.
- Lors de la mise à niveau d'un VDA, si 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.

La liste des composants peut inclure :

- **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 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 Supportability Tools :** installe le MSI qui contient les outils de prise en charge Citrix.

  Option de ligne de commande : `/includeadditional "Citrix Supportability Tools"` pour permettre l'installation du composant, `/exclude "Citrix Supportability Tools"` 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 de l'installation affecte la surveillance et la résolution des problèmes des VDA dans Citrix Cloud.

  - Sur les pages **Détails de l'utilisateur** et **Point de terminaison**, les panneaux **Surveiller**, **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 Plugin"` pour permettre l'installation du composant, `/exclude "Citrix Profile Management WMI Plugin"` pour empêcher l'installation du composant

- **Agent de mise à niveau de VDA :** (valide uniquement pour les déploiements de Citrix DaaS) permet au VDA de participer à la fonctionnalité 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

- **Citrix Files pour Windows :** ce composant permet aux utilisateurs de se connecter à leur compte Citrix Files. Ils peuvent ensuite interagir avec Citrix Files via un lecteur mappé dans le système de fichiers Windows, sans nécessiter une synchronisation complète de leur contenu.

  Options de ligne de commande : `/includeadditional "Citrix Files for Windows"` pour permettre l'installation du composant, `/exclude "Citrix Files for Windows"` pour empêcher l'installation du composant

- **Citrix Files pour Outlook :** vous permet de contourner les restrictions de taille de fichier et de renforcer la sécurité de vos pièces jointes ou e-mails en les envoyant via Citrix Files. Vous pouvez fournir une demande de chargement de fichiers sécurisé directement dans votre e-mail. Pour plus d'informations, consultez Citrix Files for Outlook.

  Options de ligne de commande : `/includeadditional "Citrix Files for Outlook"` pour permettre l'installation du composant, `/exclude "Citrix Files for Outlook"` pour empêcher l'installation du composant

- **Optimisation du stockage MCS (Machine Creation Services) :** installe le pilote 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 Citrix Gateway Service dans votre environnement et si votre réseau possède un proxy non transparent pour les connexions sortantes. Seuls les proxys HTTP sont pris en charge.

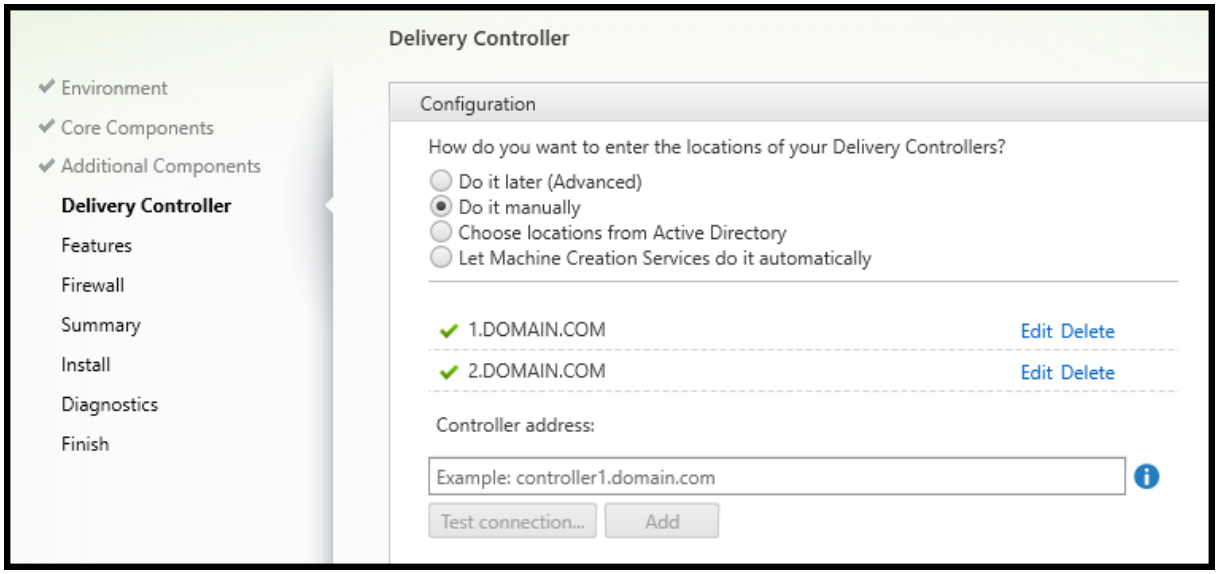
  Si vous installez ce composant, spécifiez l'adresse du proxy ou le chemin d'accès au fichier PAC sur la page **Configuration du proxy Rendezvous** . Pour plus d'informations sur les fonctionnalités, consultez Protocole Rendezvous.

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.

  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.

Étape 5. Adresses de Cloud Connector



Sur la page **Delivery Controller**, sélectionnez **Effectuer manuellement**. Entrez le nom DNS d'un Cloud Connector installé, puis sélectionnez **Ajouter**. Si vous avez installé des Cloud Connector supplémentaires dans l'emplacement de ressources, ajoutez leurs noms DNS.

Sélectionnez **Suivant**.

Considérations :

- L'adresse peut contenir uniquement des caractères alphanumériques.
- L'enregistrement du VDA requiert que les ports de pare-feu utilisés pour communiquer avec le Cloud Connector soient ouverts. Ce paramètre est activé par défaut sur la page **Pare-feu** de l'assistant.

Option de ligne de commande : `/controllers`

Étape 6. Configuration du proxy

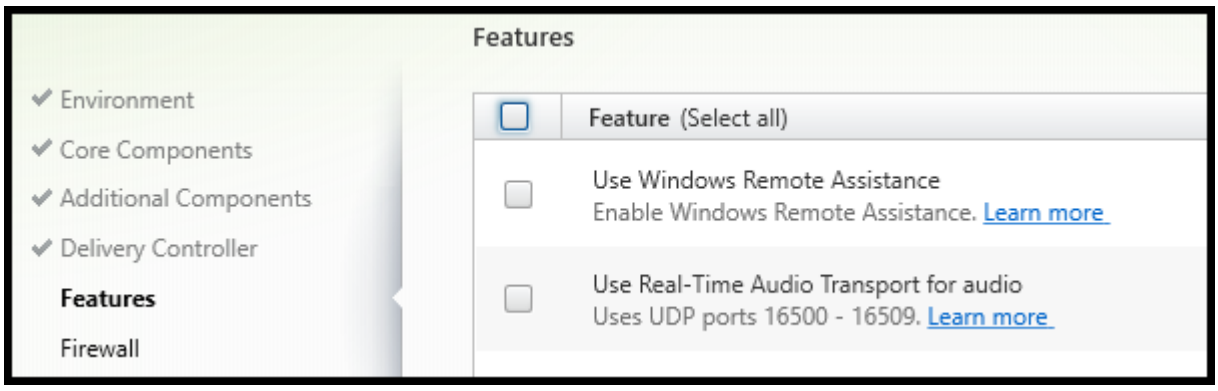
La page **Configuration du proxy Rendezvous** s'affiche uniquement si vous avez activé la case à cocher **Configuration du proxy Rendezvous** sur la page **Composants supplémentaires**.

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 7. Activer ou désactiver des fonctionnalités



Sur la page **Fonctionnalités**, utilisez les cases à cocher pour activer ou désactiver les fonctionnalités que vous souhaitez utiliser.

- **Use Windows Remote Assistance :** lorsque cette option est activée, l'Assistance à distance Windows est utilisée avec la fonctionnalité d'observation utilisateur du composant Director dans Citrix Cloud. 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 uniquement si votre déploiement utilise Citrix DaaS. (Valeur par défaut = désactivé)

  Option de ligne de commande : `/xendesktopcloud`

Sélectionnez **Suivant**.

Si cette page contient une fonctionnalité nommée **E/S de MCS**, ne l'utilisez pas. La fonctionnalité E/S de MCS est configurée sur la page **Composants supplémentaires**.

Étape 8. Ports du pare-feu

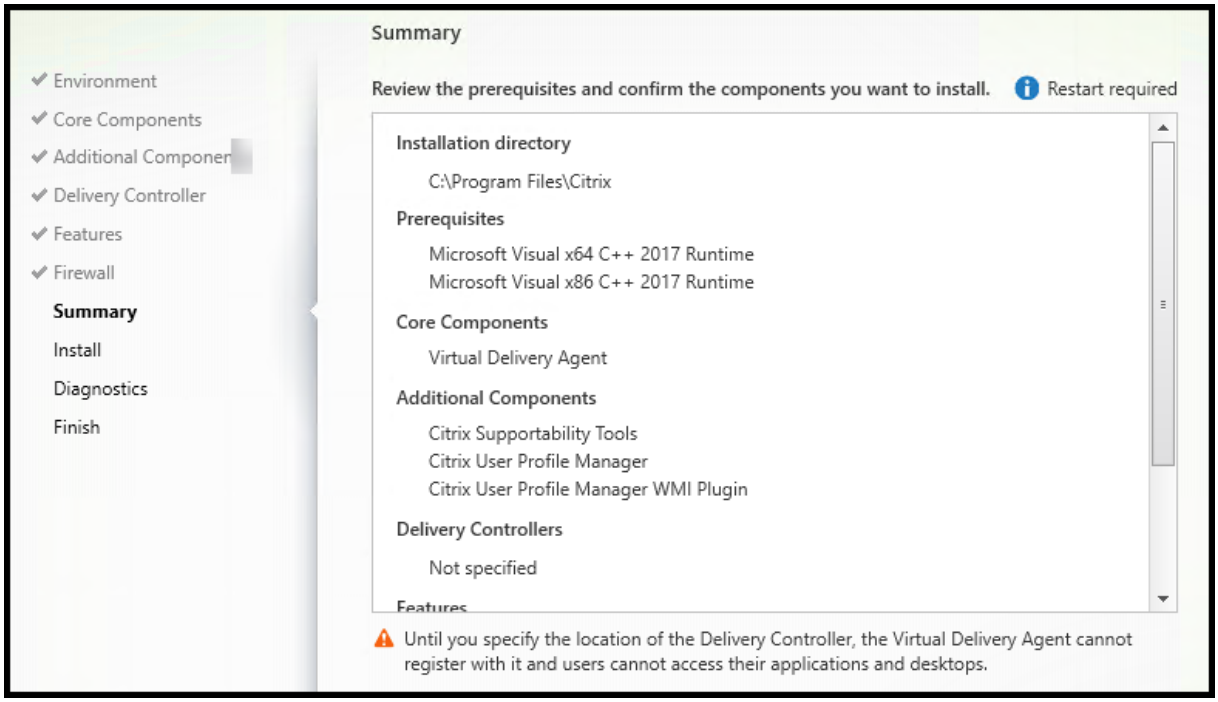
La page **Pare-feu** indique les ports que le VDA et les Cloud Connector utilisent pour communiquer entre eux. Par défaut, ces ports sont ouverts automatiquement si le service Pare-feu Windows est en cours d'exécution, même si le pare-feu n'est pas activé. Ce paramètre par défaut convient à la plupart des déploiements.

Pour obtenir des informations sur le port, consultez la section Ports réseau.

Sélectionnez **Suivant**.

Option de ligne de commande : `/enable_hdx_ports`

Étape 9 –Vérifier les composants requis et confirmer l'installation

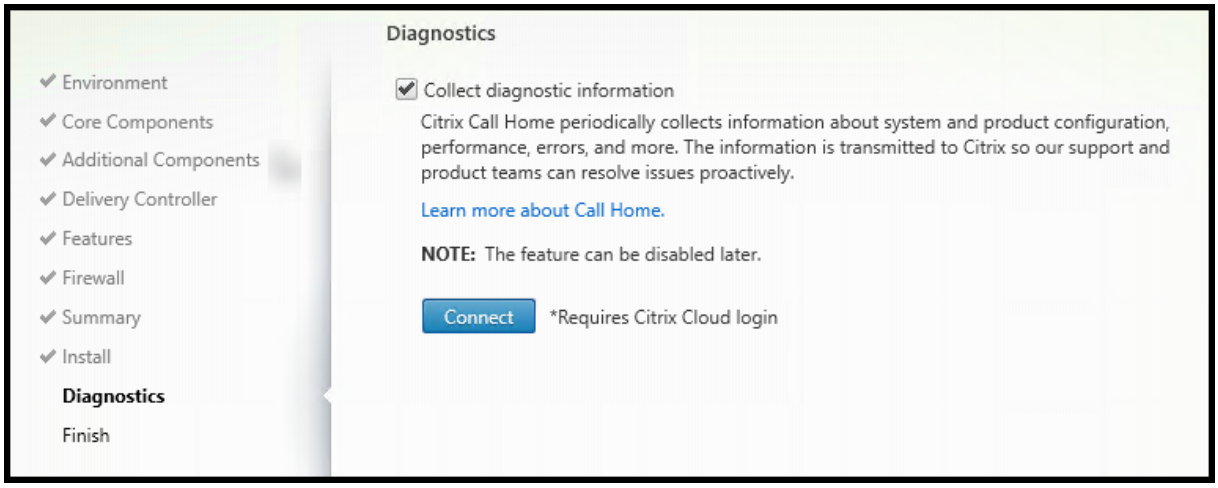


La page **Résumé** répertorie les éléments qui seront installés. Vous pouvez revenir sur les pages précédentes de l'assistant et modifier les réglages, si nécessaire.

(VDA mono-session uniquement) Activez la case à cocher **Enable automatic restore if update fails** (Activer la restauration automatique si la mise à jour échoue) pour activer la fonctionnalité de restauration en cas d'échec. Pour plus d'informations, consultez la section Restauration en cas d'échec de l'installation ou de la mise à niveau.

Lorsque vous êtes prêt, sélectionnez **Installer**.

Étape 10. Diagnostics

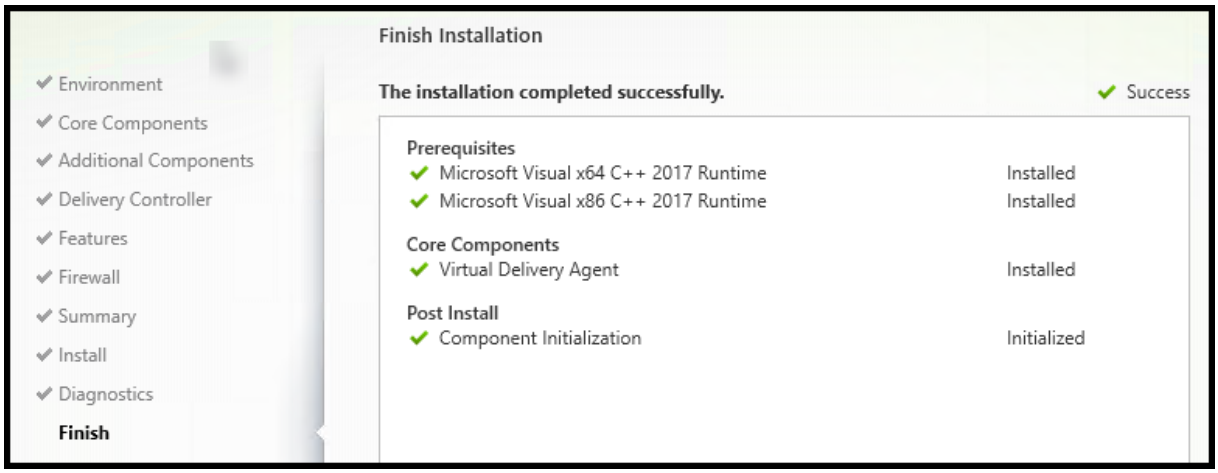


Sur la page **Diagnostics**, indiquez si vous souhaitez participer au programme Citrix Call Home. Si vous choisissez de participer (valeur par défaut), sélectionnez **Connecter**. Lorsque vous y êtes invité, saisissez vos informations d'identification de compte Citrix.

Une fois que vos informations d'identification sont validées (ou si vous choisissez de ne pas participer au programme), sélectionnez **Suivant**.

Pour plus d'informations, consultez Call Home.

Étape 11. Terminer cette installation



La page **Terminer** contient des coches vertes pour tous les éléments pré-requis et composants installés et initialisés avec succès.

Sélectionnez **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.

(Si vous installez un VDA sur des machines individuelles (plutôt qu'une image), répétez les étapes ci-dessus pour installer un VDA sur d'autres machines, si nécessaire.)

Dépannage

Dans l'écran **Gérer Configuration complète** d'un groupe de mise à disposition, l'entrée **Version de VDA installée** dans le panneau des 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.

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 ultérieurement (modifier les informations) un VDA installé :

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, modifiez tous les paramètres disponibles.

Personnaliser le port pour communiquer avec les Cloud Connector

Vous pouvez personnaliser le port que les VDA utilisent pour communiquer avec les Cloud Connector en fonction de vos exigences de sécurité spécifiques. Cette fonctionnalité est utile si votre équipe chargée de la sécurité n'autorise pas l'ouverture du port par défaut (port 80) ou si le port par défaut est déjà utilisé.

Pour personnaliser le port, procédez comme suit :

1. Ajoutez le numéro de port du contrôleur sur les Citrix Cloud Connector.
2. Ajoutez le numéro de port du VDA sur les VDA.

Ajouter le numéro de port du contrôleur sur les Citrix Cloud Connector

Accédez au Citrix Cloud Connector et exécutez les deux commandes PowerShell suivantes :

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort <port number>`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort <port number> -ConfigureFirewall`

Exemple :

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort 18000`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort 18000 -ConfigureFirewall`

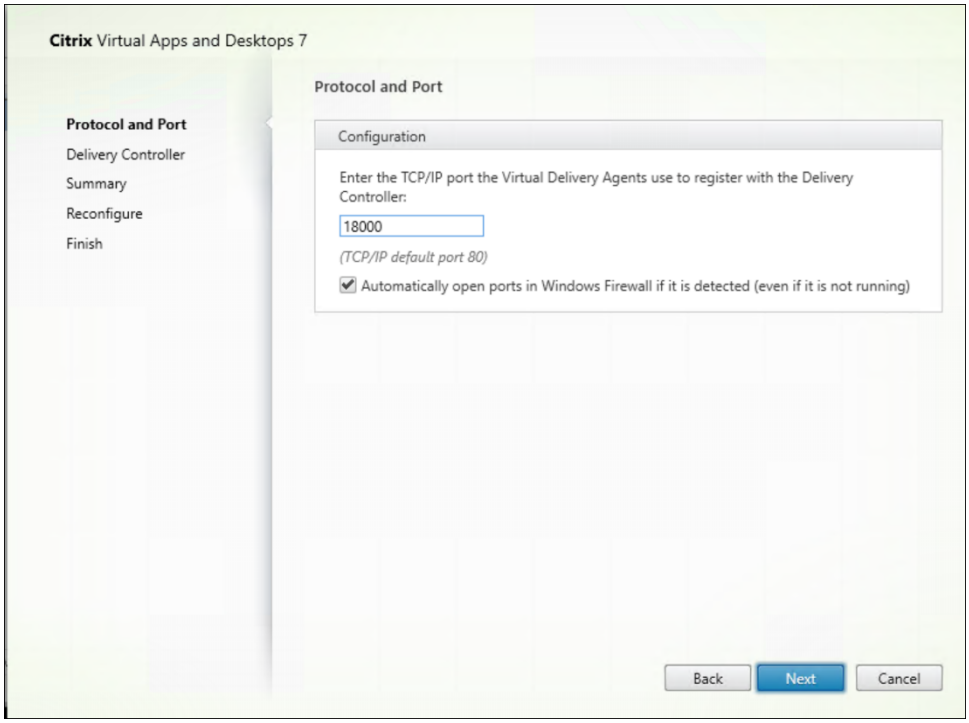
Lorsque vous personnalisez le port, tenez compte des points suivants :

- Vous devez utiliser le même numéro de port dans les deux commandes.
- Vous devez exécuter les deux commandes *sur tous les Cloud Connector*.
- Pour communiquer avec succès avec les Cloud Connector, assurez-vous que tous les VDA utilisent le même numéro de port.
- Le port que vous configurez est conservé lors des mises à jour de connecteur.

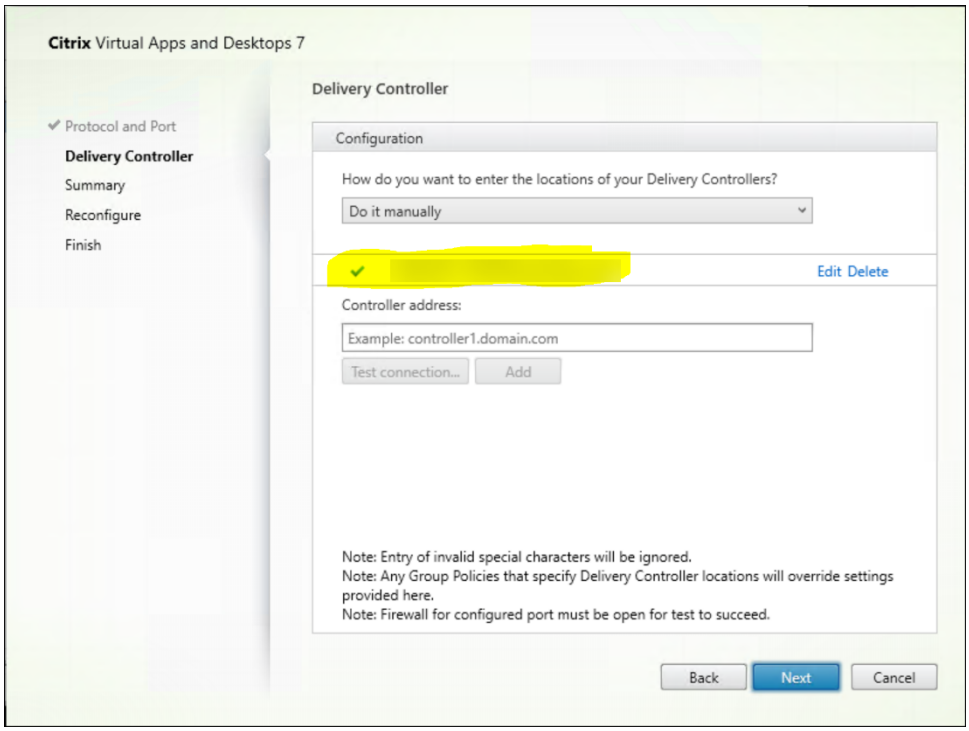
Ajouter le numéro de port du VDA sur les VDA

Installez le VDA avec les paramètres par défaut et configurez-le comme suit. Si le VDA est déjà installé, suivez les étapes ci-dessous.

1. Sur le VDA, ouvrez **XenDesktopVdaSetup.exe**, qui se trouve dans `C:\Program Files\Citrix\XenDesktopVdaSetup\XenDesktopVdaSetup.exe`.
2. Sur la page **Protocole et port**, ajoutez le numéro de port personnalisé.



3. Sur la page **Delivery Controller**, entrez le nom de domaine complet du Controller.



4. Cliquez sur **Suivant** pour passer à l'assistant afin de terminer la configuration.

Les numéros de port sont ensuite reconfigurés avec succès.

> **Remarque :**
>
> Le message d'erreur suivant peut s'afficher lorsque vous testez une connexion au Controller : Instance en cours d'exécution du Controller introuvable sur < adresse du Controller que vous avez saisie >. Si l'adresse est correcte, vous pouvez ignorer le message.

Dépannage

Pour vérifier si les ports personnalisés sont correctement configurés, accédez au Cloud Connector et effectuez les étapes de dépannage suivantes :

1. Vérifiez que les deux clés de registre suivantes existent.

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   Nom : CustomVDAPortNumber
   Type : REG_DWORD
   Données : 18000

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   Nom : CustomVDAPortNumberHA
   Type : REG_DWORD
   Données : 18000

2. Exécutez la commande suivante pour créer un fichier .txt.

   - `netsh http show urlacl > <filepath>.txt`

   Exemple :

   - `netsh http show urlacl > c:\reservations.txt`

3. Ouvrez le fichier .txt et vérifiez les quatre URL suivantes pour vous assurer que le port correct est utilisé.

   - `http://+:18000/Citrix/CdsController/IRegistrar/`
   - `http://+:18000/Citrix/CdsController/ITicketing/`
   - `http://+:18000/Citrix/CdsController/IDynamicDataSink/`
   - `http://+:18000/Citrix/CdsController/INotifyBroker/`

4. Vérifiez que les deux règles de pare-feu suivantes sont créées et que les ports requis sont ouverts.

   - Citrix XaXdProxy
   - Citrix Broker Service (TCP-In)

Autres informations

- Après avoir installé un VDA, vous pouvez vérifier l'état et la disponibilité du site et de ses composants avec une vérification de l'état du cloud.

Autres ressources

Créez des catalogues de machines.

Pour passer en revue l'ensemble du processus de configuration, reportez-vous à la section Planifier et créer un déploiement.

Installer des VDA à l'aide de la ligne de commande

June 8, 2023

Introduction

Cet article explique comment installer, mettre à niveau et personnaliser des VDA sur des machines avec systèmes d'exploitation Windows.

Cet article explique comment émettre des commandes d'installation de VDA. Avant de commencer l'installation, consultez la section Installer des VDA pour en savoir plus sur l'installation, les programmes d'installation et les informations que vous spécifiez pendant l'installation.

Installer un VDA à partir de la ligne de commande

Pour installer un VDA (et voir le progrès d'exécution des commandes et les valeurs de retour), vous devez disposer d'autorisations d'administrateur élevées ou utiliser **Exécuter en tant qu'administrateur**.

1. Sur la machine sur laquelle vous installez le VDA, connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.
3. Sur le côté supérieur droit, cliquez sur **Téléchargements** et sélectionnez **Télécharger VDA**. Vous serez redirigé vers la page de téléchargement du VDA. Recherchez le programme d'installation du VDA que vous souhaitez et cliquez sur **Télécharger fichier**.
4. Une fois le téléchargement terminé, exécutez le programme d'installation. Utilisez les options décrites dans cet article.

- Pour le VDA pour OS multi-session, exécutez `VDAServerSetup.exe`
- Pour le VDA pour OS mono-session, exécutez `VDAWorkstationSetup.exe`
- Pour le VDA pour services de base OS mono-session, exécutez `VDAWorkstationCoreSetup.exe`

Pour extraire les fichiers avant de les installer, utilisez `/extract` avec le chemin d'accès absolu, par exemple : `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`. (Le répertoire doit exister. Sinon, l'extrait 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`

Options de ligne de commande pour installer un VDA

Les options suivantes sont valides avec une ou plusieurs des commandes : `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` et `VDAWorkstationCoreSetup.exe`.

- **/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, spécifiez `/components vda,plugins`.

  Si l'option `plugins` 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 `VDAWorkstationCoreSetup.exe`. Ce programme d'installation ne peut pas installer l'application Citrix Workspace.

- **/controllers** "*controller* [*controller*]…"

  Noms de domaines complets (FQDN) séparés par des espaces et entourés de guillemets droits des Citrix Cloud Connector avec lesquels le VDA peut communiquer. 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 utilisés par le VDA, spécifiez l'option /`enable_hdx_ports`, en plus de l'option /`enable_hdx_udp_ports`.

- **/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 de l'Assistance à distance Windows pour l'utiliser avec les fonctions **Surveiller**. 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 gérée par MCS nécessite le composant Machine Identity Service. Les valeurs autorisées sont :

  - Machine Identity Service
  - Citrix Profile Management
  - Plug-in WMI de Citrix Profile Management
  - Citrix Personalization pour AppV –VDA
  - Outils de prise en charge Citrix
  - Pilote E/S de MCS Citrix
  - Agent de mise à niveau de Citrix VDA
  - Citrix Rendezvous V2

  L'exclusion de Citrix Profile Management de l'installation (`/exclude "Citrix Profile Management"`) affecte la surveillance et le dépannage des VDA à partir de l'onglet **Surveiller**. 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 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 envisagez d'utiliser MCS pour provisionner des machines virtuelles, n'excluez pas Machine Identity Service.

  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 `VDAWorkstationCoreSetu .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. Les noms des composants sont sensibles à la casse.

  Cette option peut être utile lorsque vous créez un déploiement Remote PC Access et souhaitez installer des composants qui ne sont pas inclus par défaut. Les valeurs autorisées sont :

  - Citrix Profile Management
  - Plug-in WMI de Citrix Profile Management
  - Citrix Personalization pour AppV –VDA
  - Outils de prise en charge Citrix
  - Pilote E/S de MCS Citrix
  - Agent de mise à niveau de Citrix VDA
  - Citrix Rendezvous V2
  - Couche de personnalisation de l'utilisateur
  - Outil d'enregistrement de VDA Citrix WebSocket

  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 VM. Définit le VDA comme image. 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).

- **/no_mediafoundation_ack**

  Reconnaît que Microsoft Media Foundation n'est pas installé, et que plusieurs fonctionnalités multimédias de HDX ne sont pas installées et ne fonctionnent pas. Si cette option est omise et Media Foundation n'est pas installé, l'installation de VDA échoue. La plupart des éditions Windows prises en charge sont fournies avec Media Foundation, à l'exception des éditions N.

- **/nodesktopexperience**

  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.

- **/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*"

  Valide uniquement si la commande contient `/includeadditional "Citrix Rendezvous V2"`. 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).

  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.

- **/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.

- **/remove**

  Supprime les composants spécifiés avec l'option `/components`.

- **/removeall**

  Supprime le VDA. Ne supprime pas l'application Citrix Workspace (si elle est installée).

- **/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 un serveur Windows pris en charge. Évitez cette option lors de l'installation d'un VDA multi-session sur un serveur Windows. Avant d'utiliser cette option, consultez la section Server VDI.

- **/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 **Gérer > Configuration complète**. 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 VM. Remplace la détection par le programme d'installation d'une machine physique, où les informations du BIOS transmises aux VM 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 : Installer un VDA

- **Installer un VDA sur un OS multi-session.** La commande suivante installe un VDA sur un OS multi-session.

  ```
  VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com"/
  enable_hdx_ports /masterimage
  ```

  Le VDA sera utilisé comme image.

- **Installer un VDA d'OS multi-session ou un VDA d'OS mono-session.** La commande suivante installe un VDA d'OS multi-session ou un VDA d'OS mono-session.

  ```
  VDAServerSetup_XXXX.exe /quiet /controllers "ddc1.abc.com",
  "ddc2.abc.com"/enable_hdx_ports /enable_Remote_Assistance /
  enable_real_time_transport /enable_ss_ports /noreboot
  ```

  Séparez le nom de domaine complet de chaque Delivery Controller par une virgule. Notez que `XXXX` représente la version du VDA.

- **Installer un VDA Core Services sur un OS mono-session.** La commande suivante installe un VDA Core Services sur un OS mono-session à utiliser dans un déploiement VDA ou Remote PC Access.

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.
  domain.com"/enable_hdx_ports /noreboot
  ```

  L'application Citrix Workspace et les autres services non fondamentaux ne sont pas installés. L'adresse d'un Cloud Connector est spécifiée, et les ports du Service de pare-feu Windows sont automatiquement ouverts. L'administrateur gère les redémarrages.

Personnaliser un VDA à l'aide de la ligne de commande

Une fois que vous avez installé un VDA, vous pouvez personnaliser plusieurs paramètres. Exécutez `XenDesktopVDASetup.exe`, en utilisant une ou plusieurs des options suivantes.

- `/reconfigure` (option requise lors de la personnalisation d'un VDA)
- `/h` ou `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

Autres ressources

- Créer des catalogues de machines
- Pour passer en revue l'ensemble du processus de configuration, reportez-vous à la section Planifier et créer un déploiement.

Créer et gérer des connexions et des ressources

February 21, 2024

Introduction

La configuration d'une connexion implique de sélectionner un type de connexion dans la liste des hyperviseurs et des services cloud pris en charge, puis de choisir les ressources réseau et de stockage appropriées pour cette connexion.

> **Remarque :**
>
> Vous devez disposer de tous les privilèges d'administrateur pour effectuer les tâches liées à la gestion des connexions et des ressources.

Où trouver des informations sur les types de connexion

L'article Configuration système requise fournit une liste des hyperviseurs et des versions de services cloud pris en charge, ainsi que des liens vers des articles pour chaque hôte spécifique.

Stockage hôte

Un produit de stockage est pris en charge s'il est géré par un hyperviseur pris en charge. Le support Citrix aide uniquement les fournisseurs de produits de stockage à dépanner, résoudre et documenter ces problèmes, ainsi que les solutions, dans le centre de connaissances si nécessaire.

Lors du provisioning de machines, les données sont classées par type :

- Système d'exploitation (OS) : inclut des images
- Données temporaires : toutes les données non persistantes écrites sur les machines provisionnées avec MCS (Machine Creation Services), les fichiers de pages Windows et les données synchronisées avec ShareFile. Ces données sont supprimées chaque fois qu'une machine redémarre. Si l'image de base inclut des données de profil utilisateur, ces données restent persistantes. Si une solution de profil utilisateur centralisée est utilisée, les données du profil utilisateur sont synchronisées avec le magasin de profils externe. Les données de profil utilisateur mises en cache localement sont supprimées à chaque redémarrage de la machine.

L'allocation de ressources de stockage distinctes pour différents types de données permet de minimiser la charge du système et d'améliorer les performances IOPS (opérations d'entrée/sortie par seconde) sur chaque périphérique de stockage. Cette allocation stratégique permet d'utiliser de manière optimale les ressources disponibles de l'hôte. Cela permet également de sélectionner le support de stockage le plus adapté en fonction des besoins spécifiques de chaque type de données, par exemple une plus grande persistance ou résilience pour certains types de données.

- Options de stockage local et partagé : les ressources de stockage peuvent être soit centralisées, c'est-à-dire séparées d'un hôte et utilisées par tous les hôtes, soit localisées sur un hyperviseur spécifique. Les options de centralisation incluent les volumes partagés en cluster Windows, qui peuvent être dotés ou non d'un espace de stockage supplémentaire rattaché, ou les appliances des fournisseurs de stockage. Les solutions de stockage centralisées peuvent proposer des fonctionnalités d'optimisation avancées, telles que des chemins de contrôle de stockage spécifiques à l'hyperviseur, et un accès direct aux plug-ins.

- Avantages et inconvénients du stockage local : le stockage local de données temporaires permet d'éviter les connexions réseau pour accéder au stockage partagé, réduisant ainsi la charge IOPS sur les ressources partagées. L'utilisation du stockage local peut s'avérer une alternative rentable au stockage centralisé qui peut être plus coûteux. Ces avantages doivent être pondérés par rapport à la disponibilité d'un stockage suffisant sur les serveurs hyperviseur.

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. Ces données ne nécessitent pas de persistance ni autant de résilience que les données dans le stockage partagé. Ceci s'appelle la *mise en cache des 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. Gardez à l'esprit que 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 : si vous utilisez des volumes de stockage en cluster (CSV), Microsoft System Center Virtual Machine Manager n'autorise pas la création de disques de mise en cache des données temporaires sur le stockage local.

Si vous stockez les données temporaires localement, vous pouvez activer et configurer des valeurs autres que les valeurs par défaut pour la taille de disque et de mémoire de chaque VM lorsque vous créez un catalogue de machines qui utilise cette connexion. Toutefois, les valeurs par défaut sont adaptées au type de connexion et s'avèrent suffisantes dans la plupart des cas.

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 offre IntelliCache. Cela peut également réduire 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 et les autres données d'OS sont transférées vers tous les hyperviseurs utilisés dans le site, aussi bien pour la création initiale d'une machine que pour les mises à jour futures des images. Cela 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.

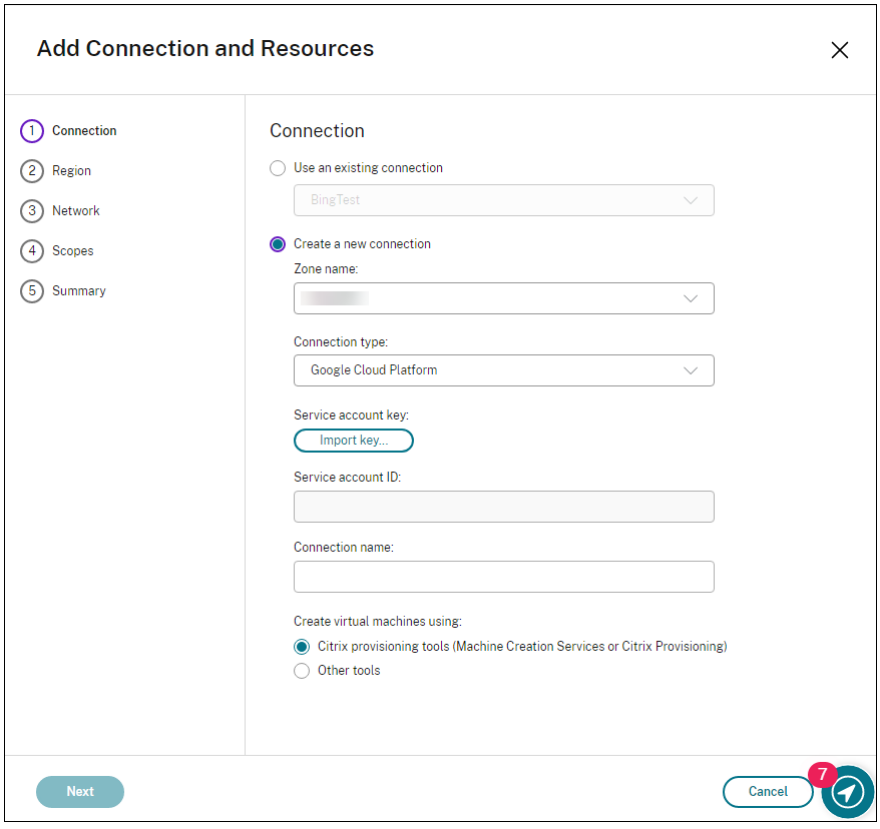
Créer une connexion et des ressources

> **Important :**
>
> Les ressources hôte (stockage et réseau) dans votre emplacement de ressources doivent être disponibles avant de créer une connexion.

1. Connectez-vous à Citrix Cloud.
2. Accédez au menu en haut à gauche et sélectionnez **Mes services > DaaS**.
3. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
4. Sélectionnez **Ajouter des connexions et des ressources** dans le volet Actions.
5. L'assistant vous guide tout au long de la procédure de configuration décrite dans les étapes suivantes. Le contenu de la page dépend du type de connexion sélectionné. Après avoir suivi les étapes de chaque page, sélectionnez **Suivant** jusqu'à la page **Résumé**.

> **Remarque :**
>
> Le contenu de chaque page de l'assistant varie en fonction du type de connexion que vous avez sélectionné.

Étape 1. Connexion



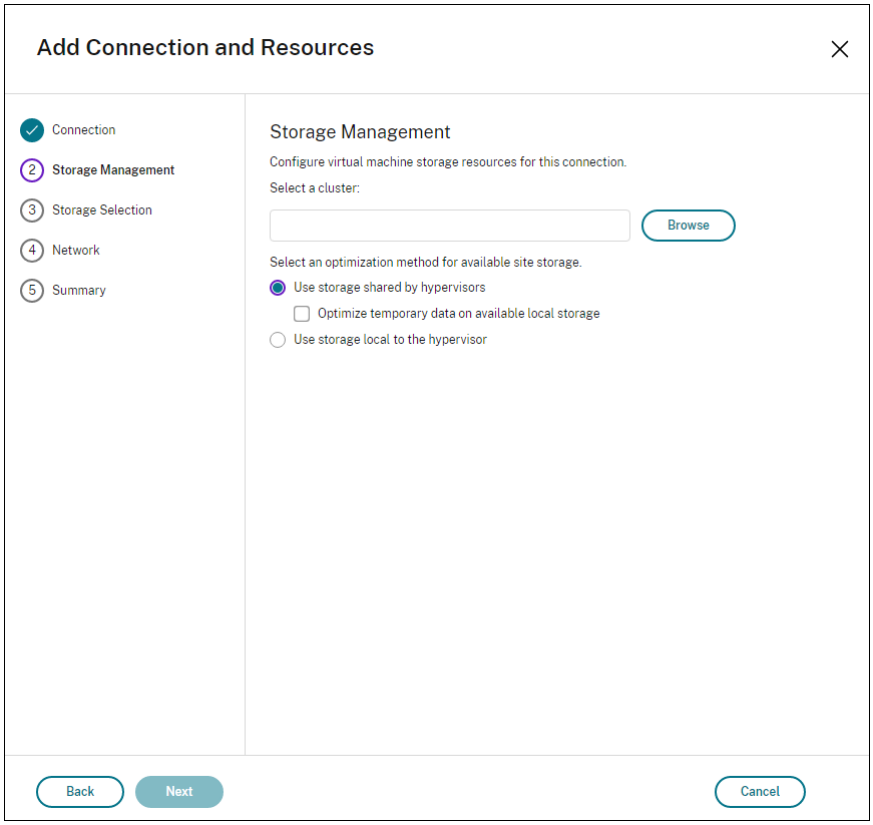
Sur la page **Connexion** :

- 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 une zone dans le champ **Nom de la zone**. Les options correspondent à tous les emplacements de ressources que vous avez configurés.
- Sélectionnez un hyperviseur ou un service cloud dans le champ **Type de connexion**. Les options incluent tous les hyperviseurs et services cloud compatibles avec Citrix :
  - Pour un emplacement de ressources dépourvu de connecteurs cloud accessibles, seuls les hyperviseurs et les services cloud prenant en charge les déploiements sans connecteur sont disponibles.
  - Pour un emplacement de ressources doté de connecteurs cloud accessibles, seuls les hyperviseurs et les services cloud dont les plug-ins sont correctement installés sur ces connecteurs sont disponibles.

  Vous pouvez également utiliser la commande PowerShell `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` (false ou true) pour obtenir la liste des hyperviseurs et des services cloud disponibles.
- Entrez un nom pour la connexion. Ce nom s'affiche sur l'écran **Hébergement**.
- Choisissez un outil pour créer des machines virtuelles.

> **Remarque :**
>
> Les informations sur la page **Connexion** diffèrent en fonction de l'hôte ou du type de connexion que vous utilisez. Par exemple, lorsque vous utilisez Azure Resource Manager, vous pouvez utiliser un principal de service existant ou en créer un nouveau. Pour plus de détails, consultez l'article Connexion à Microsoft Azure.

Étape 2. Gestion du stockage



Pour de plus amples informations sur les types et méthodes de gestion du stockage, consultez la section Stockage hôte.

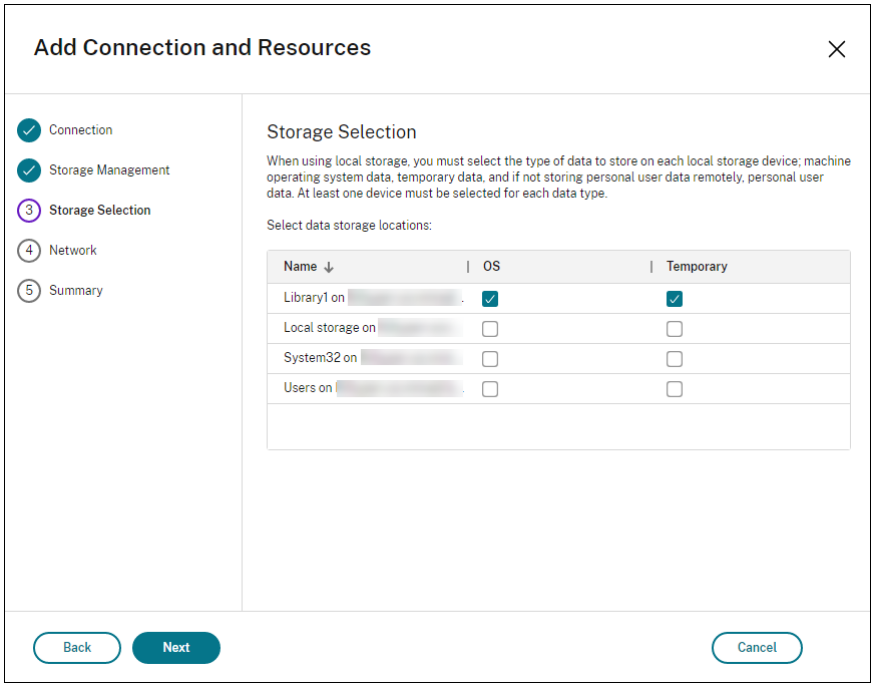
Si vous configurez une connexion à un hôte Hyper-V ou VMware, sélectionnez un nom de cluster. D'autres types de connexion ne nécessitent pas de nom de cluster.

Sélectionnez une méthode de gestion du stockage : stockage partagé par les hyperviseurs ou stockage local sur l'hyperviseur.

Pour plus d'informations, consultez les sections Stockage partagé par les hyperviseurs et Stockage local de l'hyperviseur.

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.

Étape 3. 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. Vous devez sélectionner 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.

Vous pouvez obtenir plus d'options de configuration sur la page **Sélection du stockage** si vous avez choisi **Utiliser le stockage partagé par les hyperviseurs** et sélectionné **Optimiser les données temporaires sur le stockage local disponible** sur la page **Gestion du stockage**. Par exemple, vous pouvez sélectionner les périphériques de stockage locaux (dans le même pool d'hyperviseurs) à utiliser pour les données temporaires.

Le nombre de périphériques de stockage actuellement sélectionnés est affiché (dans le diagramme, « 1 périphérique de stockage sélectionné »). Lorsque vous placez le curseur sur cette entrée, les noms des périphériques sélectionnés s'affichent (sauf si aucun périphérique n'est configuré).

1. Sélectionnez **Sélectionner** pour modifier les périphériques de stockage à utiliser.
2. Dans la boîte de dialogue **Sélectionner un stockage**, activez ou désactivez les cases du périphérique de stockage, puis sélectionnez **OK**.

Étape 4. Région

> **Remarque :**
>
> La page **Région** ne s'affiche que pour certains types d'hôtes.

La région sélectionnée indique où les machines virtuelles seront déployées. Dans l'idéal, choisissez une région proche de l'endroit où les utilisateurs accéderont à leurs applications.

Étape 5. Réseau

Entrez un nom pour les ressources. Ce nom apparaît dans la console Gérer pour identifier la combinaison stockage et réseau associée à la connexion.

Sélectionnez un ou plusieurs réseaux que les machines virtuelles utiliseront.

Certains types de connexions (telles que Azure Resource Manager) dressent également la liste des sous-réseaux que les machines virtuelles utiliseront. Sélectionnez un ou plusieurs sous-réseaux.

Étape 6. Résumé

Vérifiez vos sélections. Si vous souhaitez apporter des modifications, revenez sur les pages précédentes de l'assistant. Lorsque vous avez terminé votre évaluation, sélectionnez **Terminer**.

> **Remarque :**
>
> - Si vous stockez les données temporaires localement, vous pouvez configurer des valeurs autres que les valeurs par défaut pour le stockage des données temporaires lorsque vous créez le catalogue de machines qui utilisent cette connexion.
> - Une étendue n'est pas affichée pour les administrateurs avec accès complet. Pour plus d'informations, consultez Administrateurs, rôles et étendues.

Modifier les paramètres de connexion

Vous ne pouvez pas utiliser cette procédure pour :

- Renommer une connexion ou en créer une nouvelle.
- Modifier les paramètres du processeur graphique pour une connexion. Les catalogues accédant à cette ressource doivent utiliser une image appropriée spécifique au processeur graphique. Si vous souhaitez modifier les paramètres GCP (Google Cloud Platform), vous devez donc créer une nouvelle connexion au lieu de modifier une connexion existante.

Modifier une connexion

1. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
2. Sélectionnez la connexion, puis sélectionnez **Modifier la connexion** dans le volet Actions.
3. Accédez à la page **Propriétés de connexion** pour modifier l'adresse de connexion et les informations d'identification. Modifiez l'adresse uniquement si la machine hôte actuelle possède une nouvelle adresse. La saisie de l'adresse d'une autre machine rompt les catalogues de machines de la connexion.
   - Sélectionnez **Modifier les paramètres...**, puis saisissez les 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. Pour plus d'informations, consultez la section Créer une connexion à XenServer.

4. Accédez à la page **Avancé** pour modifier les paramètres et spécifier un nombre maximum d'actions simultanées (ou de machines simultanées) par connexion d'hébergement. 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 possède des valeurs par défaut qui sont appropriées pour la plupart des cas. En général, elles n'ont pas besoin d'être changées.
   - Les paramètres **Actions simultanées (tous types)** et **Mises à jour d'inventaire Personal vDisk simultanées** définissent 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 du support Citrix.

5. Accédez à la page **Étendue** pour sélectionner une ou plusieurs étendues pour cet hôte.

   > **Remarque :**
   >
   > Une étendue n'est pas affichée pour les administrateurs avec accès complet. Par définition, ces administrateurs ont accès à tous les objets de services d'abonnements et Citrix Cloud gérés par le client.

   Pour plus d'informations, consultez Administrateurs, rôles et étendues.

6. Accédez à la page **Locataires partagés** pour ajouter des locataires et des abonnements qui partagent Azure Compute Gallery avec l'abonnement de cette connexion.

   a) Entrez le **Secret d'application** de 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.
   b) Ajoutez des locataires et des abonnements partagés. Vous pouvez ajouter jusqu'à huit locataires partagés. Pour chaque locataire, vous pouvez ajouter jusqu'à huit abonnements.

7. Cliquez sur **Enregistrer** puis 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.

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. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
2. 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. Vus 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

> **Attention :**
>
> 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 pouvez supprimer le catalogue. Avant de supprimer un catalogue, assurez-vous qu'il n'est pas utilisé par d'autres connexions.

1. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
2. Sélectionnez la connexion, puis sélectionnez **Supprimer la connexion** dans la barre d'actions.
3. 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 une connexion

1. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
2. Sélectionnez la connexion, puis **Renommer la connexion**.

Tester une connexion

1. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
2. Sélectionnez la connexion, puis **Tester la connexion**.

Afficher les détails des machines sur une connexion

1. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.

2. 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 nouvelle 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, sélectionnez **Développement**, puis sélectionnez les propriétés et les opérateurs dans les listes.

Gérer les machines sur une connexion

1. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
2. Sélectionnez une connexion, puis sélectionnez **Afficher les machines**dans la barre d'actions.
3. Sélectionnez l'une des options suivantes dans la barre d'actions. Some actions might not be available, depending on the machine state and the connection host type.

    - **Démarrer :** démarre la machine si celle-ci est hors tension ou suspendue.
    - **Suspendre :** pause la machine sans la fermer et actualise la liste de machines.
    - **Arrêter :** requiert la fermeture du système d'exploitation.
    - **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 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 précédemment.)
    - **Supprimer du groupe de mise à disposition :** la suppression d'une machine d'un groupe de mise à disposition n'est pas supprimée du 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, les données temporaires et les données personnelles (PvD) 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. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
2. Sélectionnez la connexion, puis sélectionnez **Modifier le stockage** dans la barre d'actions.
3. Dans le panneau de gauche, sélectionnez le type de données : système d'exploitation ou temporaires.
4. Cochez ou décochez les cases à cocher d'un ou plusieurs périphériques de stockage pour le type de données sélectionné.
5. Sélectionnez **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 d'un périphérique actuellement **en cours d'utilisation**, son état passera à **Remplacé**. Les machines existantes continueront d'utiliser ce périphérique de stockage (et peuvent y écrire des données). Ainsi, cet emplacement peut devenir saturé même après qu'il cesse d'être utilisé pour créer des machines.

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 cloud.

Suivez les étapes indiquées sur Citrix DaaS :

1. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau 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 Citrix pour 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.

Modifier les réseaux de ressources

Vous pouvez changer de réseau pour une connexion. Procédez comme suit :

1. Accédez à **Gérer > Configuration complète > 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 la page.

Supprimer, renommer ou test des ressources

1. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
2. Sélectionnez les ressources cibles sous la connexion, puis sélectionnez l'entrée appropriée dans le volet d'actions :

   - **Supprimer des ressources**
   - **Renommer des ressources**
   - **Tester des ressources**

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.

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.
- En cas de charge de travail potentiellement importante, environ 2 000 enregistrements sont affichés comme étant orphelins.

Affichage de la liste des ressources orphelines

Pour afficher la liste des ressources orphelines

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*`.
3. 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-->
   ```

Affichage de la liste des ressources orphelines à partir d'un ID d'abonnement

Pour afficher la liste des ressources orphelines à partir d'un ID d'abonnement, procédez comme suit :

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*`.
3. 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 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
  - Connexion à XenServer

Si vous êtes dans le processus de déploiement initial, créez un catalogue de machines.

Connexion à AWS

May 17, 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. Consultez la page Environnements de virtualisation AWS.

Créer une connexion

Lorsque vous créez une connexion à partir de l'interface Configuration complète :

- 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. Citrix DaaS ne peut donc pas utiliser le

fichier pour remplir les champs Clé API et 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`.

Limitation

Si vous modifiez le nom d'un VPC (cloud privé virtuel) AWS dans la console AWS, l'unité d'hébergement existante dans Citrix Cloud est démontée. Lorsque l'unité d'hébergement est démontée, vous ne pouvez pas créer de catalogues ou ajouter des machines à des catalogues existants. Pour résoudre le problème, renommez le VPC AWS par son nom d'origine.

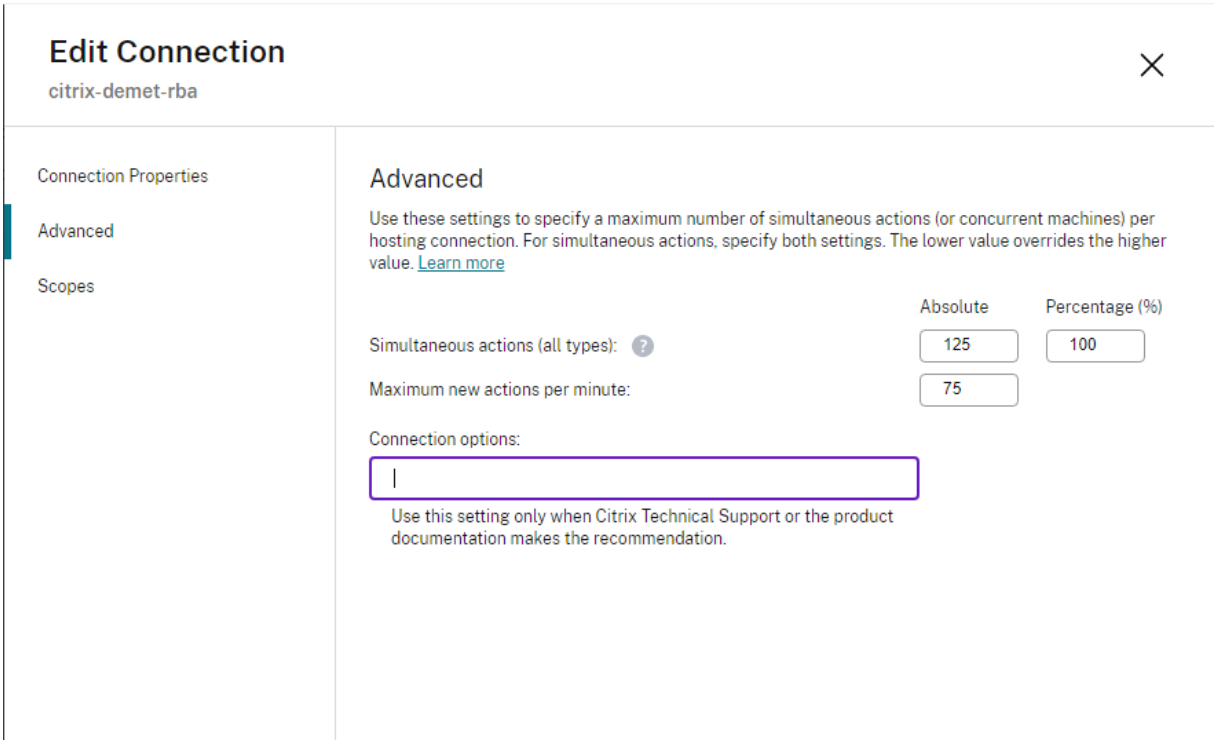
Valeurs par défaut des connexions hôtes

Lorsque vous créez des connexions hôtes dans l'interface Configuration complète de l'environnement cloud AWS, les valeurs par défaut suivantes sont affichées :

Option	Absolu	Pourcentage
Actions simultanées (tous types)	125	100
Nouvelles actions maximales par minute	150	S/O
Opérations de provisioning simultanées maximales	100	S/O

MCS prend en charge 100 opérations de provisioning simultanées maximum par défaut.

Vous pouvez configurer ces valeurs en accédant à la section **Avancé** de Citrix Studio sur l'écran **Modifier la connexion** :



Vous pouvez également utiliser le SDK Remote PowerShell pour définir le nombre maximal d'opérations simultanées pour des paramètres optimaux pour votre environnement.

Utilisez la propriété personnalisée PowerShell, `MaximumConcurrentProvisioningOperations`, pour spécifier le nombre maximal d'opérations de provisioning AWS simultanées.

Avant la configuration :

- Assurez-vous d'avoir installé le SDK PowerShell pour le cloud.
- La valeur par défaut de `MaximumConcurrentProvisioningOperations` est 100.

Procédez comme suit pour personnaliser la valeur `MaximumConcurrentProvisioningOperations` :

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Entrez `cd xdhyp:\Connections\`.
4. Entrez `dir` pour afficher la liste des connexions.
5. Modifiez ou initialisez la chaîne Custom Properties :
    - Si la chaîne Custom Properties contient une valeur, copiez-la dans le Bloc-notes. Ensuite, remplacez la propriété `MaximumConcurrentProvisioningOperations` par la valeur de votre choix. Vous pouvez saisir une valeur comprise entre 1 et 1 000.

Par exemple, <Property xsi:type="IntProperty"Name="MaximumConcurrentProvis
"Value="xyz"/>.

- Si la chaîne Custom Properties est vide/nulle, vous devez initialiser la chaîne en saisissant la syntaxe appropriée pour le schéma et la propriété MaximumConcurrentProvisioningOperat
.

6. Dans la fenêtre **PowerShell**, collez les propriétés Custom Properties modifiées à partir du Bloc-notes et affectez une variable aux propriétés Custom Properties modifiées. Si vous avez initialisé les propriétés Custom Properties, ajoutez les lignes suivantes après la syntaxe :

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
   citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
   org/2001/XMLSchema-instance"><Property xsi:type="IntProperty"
   Name="MaximumConcurrentProvisioningOperations" Value="100"/></
   CustomProperties>'.
   ```

   Cette chaîne définit la propriété MaximumConcurrentProvisioningOperations sur 100. Dans la chaîne Custom Properties, vous devez définir la propriété MaximumConcurrentProvision sur une valeur qui correspond à vos besoins.

7. Entrez Get-XDAuthentication, ce qui vous invite à saisir vos informations d'identification.
8. Exécutez $cred = Get-Credential, ce qui peut vous demander uniquement un mot de passe (ou un nom et un mot de passe). Vous pouvez également être invité à saisir l'ID de l'application et le secret associé. Pour les connexions utilisant l'authentification basée sur les rôles, **role_based_auth** est à la fois le nom et le mot de passe. Sinon, entrez l'ID et le code secret de l'API AWS.
9. Exécutez set-item -PSPath 'XDHyp:\Connections<connection-name>'-CustomProperties $customProperties -username $cred.username -Securepassword $cred.password. Vous devez définir *<connection-name>* sur le nom de la connexion.
10. Entrez dir pour vérifier la chaîne CustomProperties mise à jour.

Configurer des groupes de sécurité par interface réseau

Lorsque vous modifiez une connexion hôte, vous pouvez désormais configurer le nombre maximum de groupes de sécurité autorisés par l'interface réseau élastique (ENI) à l'aide d'une commande PowerShell. Pour obtenir des informations sur les valeurs de quota des groupes de sécurité AWS, consultez Groupes de sécurité.

Pour configurer des groupes de sécurité par interface réseau, procédez comme suit :

1. Ouvrez une fenêtre PowerShell.

2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Exécutez `cd xdhyp:\Connections\`.
4. Exécutez `dir` pour répertorier les connexions.
5. Exécutez la commande PowerShell suivante pour configurer les groupes de sécurité par interface réseau :

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws
    -Name "Citrix_MachineManagement_Options" -Value "
    AwsMaxENISecurityGroupLimit=<number>"
<!--NeedCopy-->
```

> **Remarque :**
>
> Si vous ne définissez aucune valeur pour `AwsMaxENISecurityGroupLimit`, la valeur par défaut de 5 est utilisée.

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.

URL de point de terminaison de service non standard

Il peut arriver que vous n'ayez pas besoin de l'URL de point de terminaison de service AWS automatiquement choisie pour la connexion. Dans de tels cas, vous pouvez utiliser le SDK Citrix Cloud et PowerShell pour créer une connexion avec une URL de point de terminaison de service non standard. Par exemple, pour créer une connexion à l'aide de l'URL de point de terminaison de service `https://ec2.cn-north-1.amazonaws.com.cn`:

1. Configurez le Cloud Connector hébergé par AWS et assurez-vous qu'il dispose d'une connectivité.
2. Exécutez les commandes PowerShell suivantes pour afficher la liste des Cloud Connector.


```
1  PS C:> asnp citrix.*
2  PS C:> Get-XDAuthentication
3  PS C:> Get-ConfigEdgeServer
4 <!--NeedCopy-->
```

3. Recherchez le ZoneUid dans le Cloud Connector nouvellement créé et saisissez-le dans les commandes PowerShell suivantes. Remplacez les éléments en italique par les valeurs respectives.

```
PS C:\> $hyp= New-Item -Path xdhyp:\Connections -ZoneUidZoneUid-
Name"My New Connection"-ConnectionType "AWS"-HypervisorAddress @
("https://ec2.cn-north-1.amazonaws.com.cn")-UserName"APIkey" -
Password"API Secret" -Persist
PS C:\> New-BrokerHypervisorConnection -HypHypervisorConnectionUid
 $hyp. HypervisorConnectionUid
```

4. Actualisez l'onglet **Configuration complète > Hébergement** pour vérifier que la connexion EC2 a été créée.
5. Ajoutez un emplacement de ressources à l'aide de la nouvelle connexion.

Définir les autorisations IAM

Utilisez les informations de cette section pour définir les autorisations IAM pour Citrix DaaS 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 la page 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** puis **Sélectionner**.
5. Tapez un nom pour la stratégie **Autorisations**.
6. Dans la section **Document de stratégie**, entrez les autorisations appropriées.

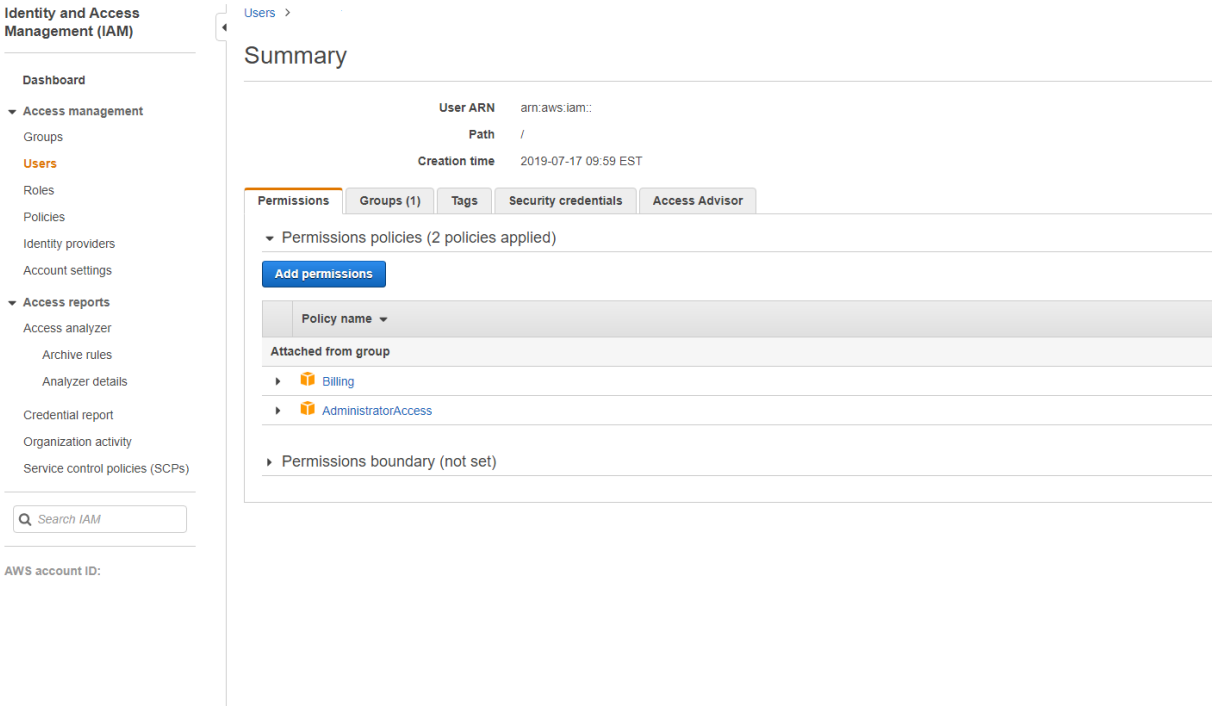
Une fois les informations de stratégie saisies, sélectionnez **Continuer** pour terminer l'application de la stratégie d'autorisations IAM au groupe d'utilisateurs. Les utilisateurs du groupe sont autorisés à effectuer uniquement les actions requises pour Citrix DaaS.

> **Important :**
>
> Utilisez le texte de stratégie fourni dans l'exemple ci-dessus pour répertorier les actions qu'un service Citrix DaaS effectuent 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.

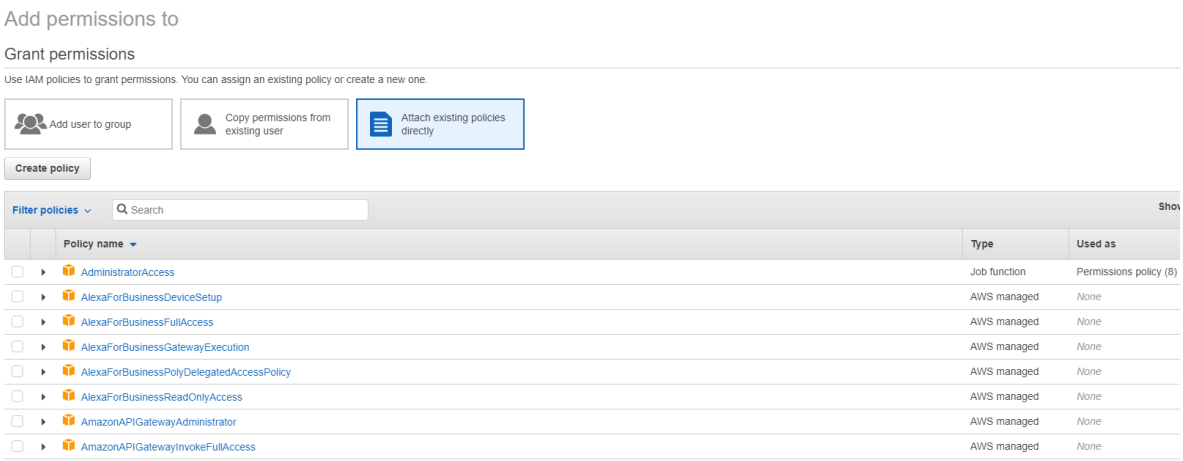
Ajouter des autorisations IAM

Ajoutez les autorisations dans la section **IAM** d'AWS Management Console :

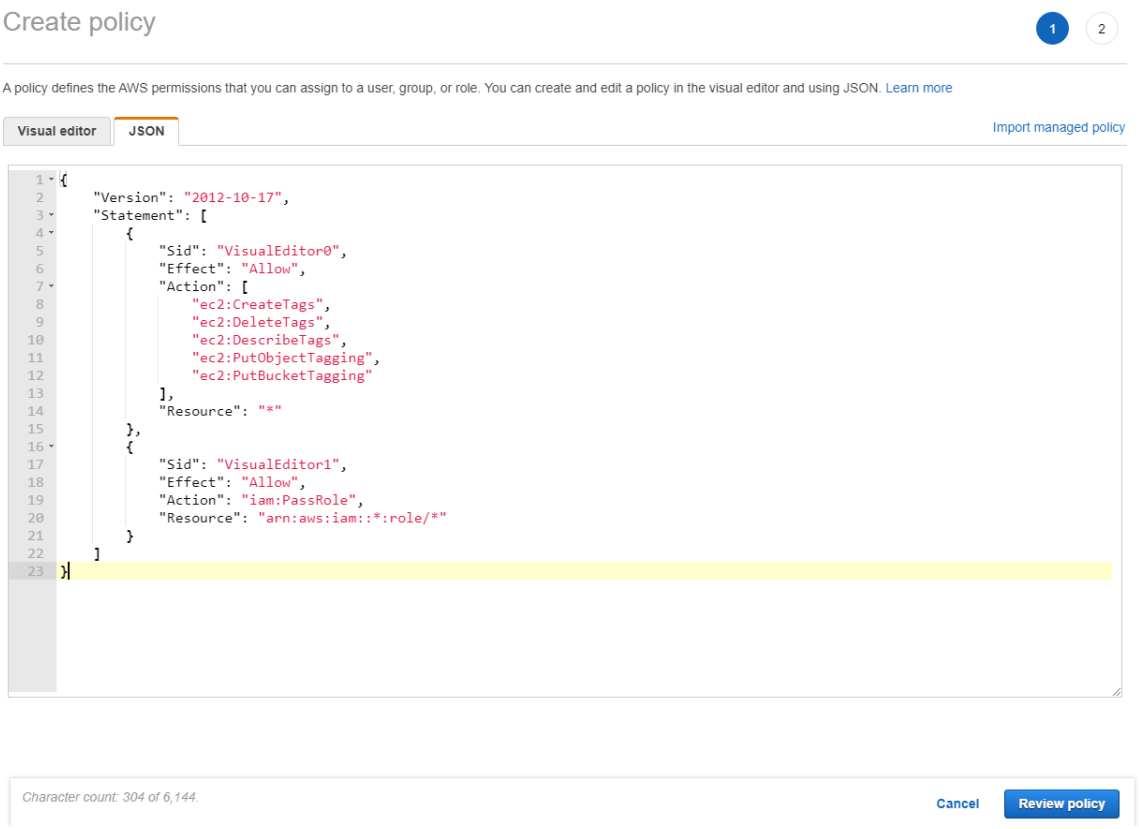
1. Dans le panneau **Summary**, sélectionnez l'onglet **Permissions**.
2. Sélectionnez **Add permissions**.



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. Pour plus d'informations, consultez la page À propos des autorisations AWS.

Autorisations AWS requises

Cette section contient la liste complète des autorisations AWS. Utilisez l'ensemble complet d'autorisations indiqué dans la section pour que la fonctionnalité fonctionne correctement.

> **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 obtenues auprès d'AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

Gestion de l'alimentation des machines virtuelles

Les instances de machine sont sous tension ou hors tension.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
```



```
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }

    ]
 }

<!--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:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",
                "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 nouvelle VM à des catalogues de machines existants sans aucun travailleur de volume, tel que l'AMI, ou aucune VM de travailleur de volume.
> - Si vous supprimez un catalogue existant qui utilise un travailleur de volume, tous les artefacts sont supprimés, y compris ceux liés au travailleur de volume.

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:GenerateDataKey",
                 "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:GenerateDataKey",
                 "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 ou 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 l'instance ec2 de Cloud Connector lors de la configuration du Cloud Connector. À l'aide de Citrix Studio, ajoutez la connexion d'hébergement et fournissez le 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:DescribeSpotInstanceRequests",
                    "ec2:DescribeInstanceCreditSpecifications",
                    "ec2:DescribeInstanceAttribute",
                    "ec2:GetLaunchTemplateData",
                    "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": "*"
        }
,
```



```
116          {
117
118              "Effect": "Allow",
119              "Action": "iam:PassRole",
120              "Resource": "arn:aws:iam::*:role/*"
121           }
122
123      ]
124  }
125
126  <!--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.
- Utilisez les autorisations `ec2:CreateNetworkInterface` et `ec2:DeleteNetworkInterface` uniquement si vous employez la méthode du travailleur de volume.

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

- Créer et gérer des connexions et des ressources
- Environnements de virtualisation AWS

Connexion à des environnements Google Cloud

April 19, 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. Consultez la page Environnements de virtualisation Google Cloud.

Ajouter une connexion

Dans l'interface Configuration complète, suivez les instructions sous Créer et gérer des connexions et des ressources. La procédure suivante vous guide tout au long de la configuration d'une connexion d'hébergement :

1. Dans **Gérer > Configuration complète**, 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**.

    - **Nom de la zone**. Sélectionnez une zone (équivalent à un emplacement de ressources) dans laquelle vous souhaitez que vos ressources hôtes résident. Les zones sont créées automatiquement lorsque vous créez un emplacement de ressources et que vous y ajoutez un Cloud Connector. Pour plus d'informations, consultez la section Zones.
    - **Type de connexion** : sélectionnez **Google Cloud Platform** dans le menu.
    - **Clé du compte de service** : importez la clé contenue dans votre fichier d'informations d'identification Google (.json). Vous pouvez coller la clé à partir du fichier d'informations d'identification ou accéder au fichier d'informations d'identification. Pour coller la clé, procédez comme suit :

        a) Localisez le fichier d'identification
        b) Ouvrez le fichier avec le Bloc-notes (ou tout autre éditeur de texte)
        c) Copiez le contenu.
        d) Retournez à la page **Connexion**, sélectionnez **Ajouter clé**, collez le contenu, puis sélectionnez **Terminé**.

    - **ID du compte de service** : Le champ est automatiquement rempli avec les informations de la clé du compte de service.
    - **Nom de la connexion** : Tapez un nom pour la connexion.

- **Acheminez le trafic via des Citrix Cloud Connector**. Pour acheminer les requêtes d'API via un composant Citrix Cloud Connector disponible, cochez cette case. Vous pouvez également cocher la case **Activer Google Cloud Build pour utiliser des pools privés** afin d'obtenir un niveau de sécurité supplémentaire.

  Vous pouvez également activer cette fonctionnalité à l'aide de PowerShell. Pour plus d'informations, consultez la section Créer un environnement sécurisé pour le trafic géré par GCP.

> **Remarque :**
>
> Cette option n'est disponible que lorsque des Citrix Cloud Connector sont actifs dans votre déploiement. Actuellement, cette fonctionnalité n'est pas prise en charge pour les Connector Appliance.

- **Créez des machines virtuelles à l'aide de**. Sélectionnez une méthode pour créer des machines virtuelles.

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.

Créer un environnement sécurisé pour le trafic géré par GCP

Vous ne pouvez autoriser que 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 :

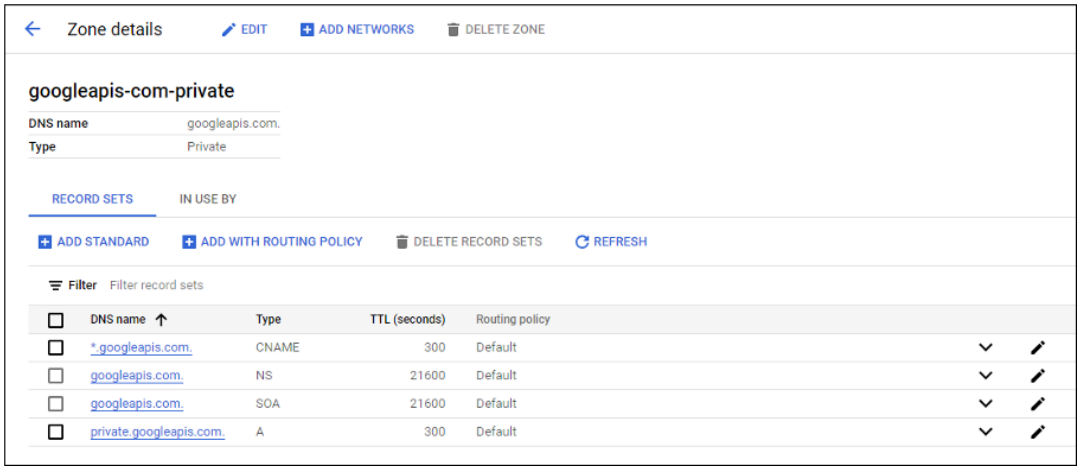
1. Installez Cloud Connector dans le VPC sur lequel vous souhaitez appliquer les contrôles de service du VPC. Consultez Contrôles de service du VPC pour plus d'informations.
2. Ajoutez `ProxyHypervisorTrafficThroughConnector` dans `CustomProperties` en cas de déploiement de Citrix Cloud. Si vous utilisez 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.

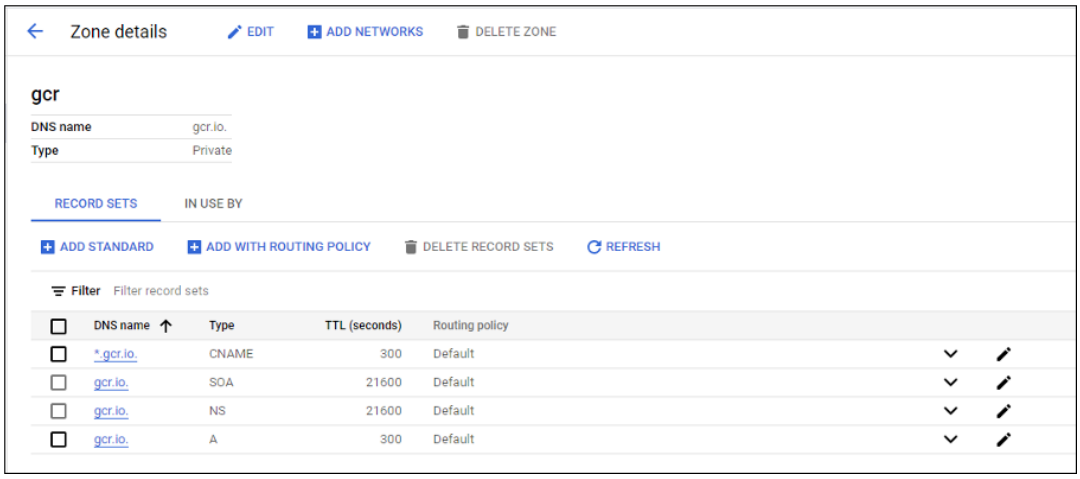
> **Remarque :**
>
> Actuellement, cette fonctionnalité n'est pas prise en charge pour Connector Appliance.

Conditions requises pour créer un environnement sécurisé pour le trafic géré par GCP

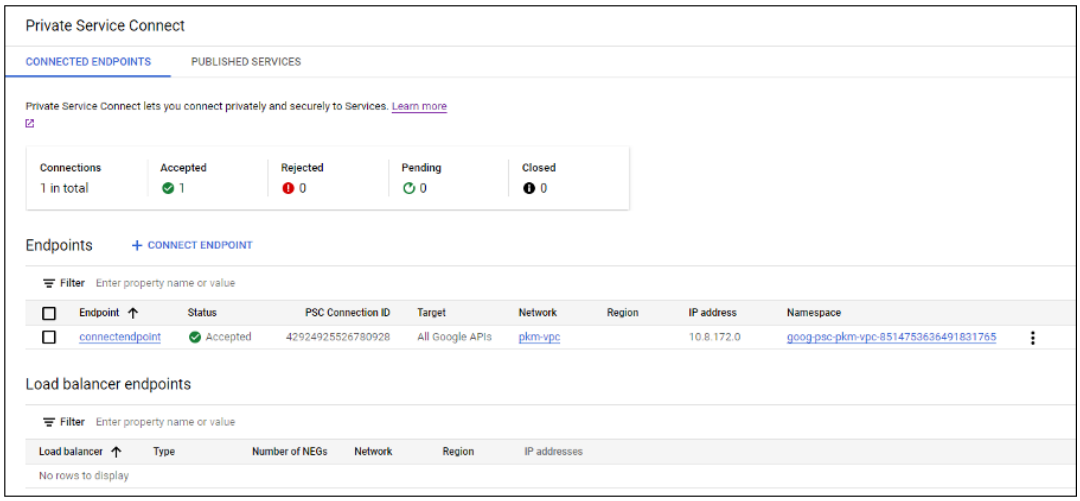
Les conditions requises pour créer un environnement sécurisé pour le trafic géré par GCP sont les suivantes :

- 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.

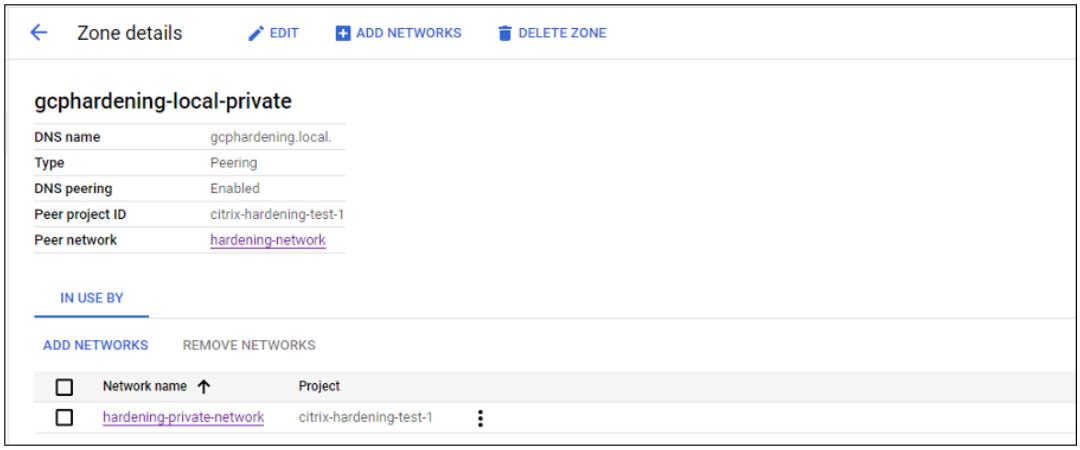




- Configurez la traduction d'adresses réseau (NAT) privée ou utilisez une connexion de service privée. Pour plus d'informations, consultez la section Accéder aux API Google via des points de terminaison.



- 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 proxy

Pour activer le proxy, 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 comme suit :
   - En cas de déploiement dans le cloud (à l'aide de pools publics) : ajoutez un paramètre de propriété `<Property xsi:type="StringProperty"Name="ProxyHypervisorTraffic "Value="True"/>` à `CustomProperties` pour activer le proxy. 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="
   ProxyHypervisorTrafficThroughConnector" Value="True"/>
</CustomProperties>
<!--NeedCopy-->
```

Autorisez la règle d'entrée pour le compte du service Cloud Build dans le périmètre du service VPC. Par exemple :

```
Ingress Rule 1
From:
Identities:
<ProjectID>@cloudbuild.gserviceaccount.com
Source > All sources allowed
To:
Projects =
All projects
Services =
Service name: All services
<!--NeedCopy-->
```

Pour plus d'informations sur le périmètre du service VPC, consultez la section Détails et configuration du périmètre de service.

- Dans le cas d'un pool de travailleurs privés lors d'un déploiement dans le cloud, ajoutez les paramètres de propriété `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector"Value="True"/>` et `<Property xsi:type="StringProperty"Name="UsePrivateWorkerPool "Value="True"/>` à `CustomProperties` pour activer le proxy. 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="
   ProxyHypervisorTrafficThroughConnector" Value="True"/>
<Property xsi:type="StringProperty" Name="
   UsePrivateWorkerPool" Value="True"/>
</CustomProperties>
<!--NeedCopy-->
```

5. Dans la fenêtre PowerShell, attribuez une variable aux propriétés personnalisées modifiées. Par exemple :
   `$customProperty = '<CustomProperties...</CustomProperties>'`.
6. Exécutez `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`.

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 des services 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
```



```
34  storage.buckets.create
35  storage.buckets.get
36  storage.buckets.list
37  storage.objects.create
38  storage.objects.delete
39  storage.objects.get
40  storage.objects.list
41  <!--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 : 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 :

```
1  resourcemanager.projects.get
2  storage.objects.create
3  storage.objects.get
4  storage.objects.list
5  <!--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 :

```
1  compute.firewalls.list
2  compute.networks.list
3  compute.subnetworks.list
4  compute.subnetworks.use
5  resourcemanager.projects.get
6  <!--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

- Créer et gérer des connexions et des ressources
- Environnements de virtualisation Google Cloud.

Connexion à HPE Moonshot

May 17, 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 :

- Interface Configuration complète
- Commandes PowerShell

Créez une connexion à l'aide de l'interface Configuration complète

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 :

- DaaS reçoit un certificat public signé par une autorité de certification contenant des erreurs : un message d'erreur apparaît. Suivez les instructions qui s'affichent à l'écran pour résoudre le problème. Sinon, vous ne pourrez pas poursuivre la création de la connexion.
- DaaS 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. DaaS fera alors confiance au certificat et enregistrera 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
<!--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 l'interface Configuration complète
- Mettre à jour la valeur de l'empreinte numérique à l'aide de commandes PowerShell

Résoudre les problèmes liés aux certificats

DaaS 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 Le certificat reçu est privé, signé par une autorité de certification, ou a expiré.	Cliquez sur la connexion et sélectionnez l'onglet **Dépannage**. Consultez les détails de l'erreur et résolvez le problème. 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 :

```
1 Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
2 <!--NeedCopy-->
```

2. Mettez à jour la valeur de l'empreinte numérique. Par exemple :

```
1 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, voir Créer un catalogue de machines HPE Moonshot.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Environnements de virtualisation HPE Moonshot

Connexion à Microsoft Azure

May 17, 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. Consultez la page Environnements de virtualisation 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 Configuration complète
- 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 Configuration complète
- 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

Avant de commencer, tenez compte des points suivants :

- Citrix recommande d'utiliser les principaux de service avec un rôle *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.
- Après vous être authentifié auprès d'Azure pour la première fois, une application multi-locataire appartenant à Citrix (ID : `08b70dc3-76c5-4611-ba7d-3312ba36cb2b`) est invitée sur votre Azure Active Directory au nom du compte authentifié. Citrix utilise cette application pour créer des principaux de service et accorder les autorisations appropriées pour le provisioning de la charge de travail et la gestion des appareils Azure AD si vous sélectionnez **Activer la gestion des appareils connectés à Azure AD** sur la page **Détails de connexion**.
- 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 Configuration complète

> **Important :**
>
> Cette fonctionnalité n'est pas encore disponible pour les abonnements Azure Chine.

Avec Configuration complète, 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. Les 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**, créez un principal de service et définissez le nom de la connexion comme suit :

   a) Pour accorder à la connexion l'autorisation de nettoyer automatiquement les appareils joints à Azure AD obsolètes, sélectionnez **Activer la gestion des appareils joints à Azure AD**. Nous vous recommandons de sélectionner cette option si vous souhaitez créer des machines jointes à Azure AD via cette connexion. Pour plus d'informations, consultez Activer la gestion des appareils joints à Azure AD.

   b) 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 `\/;:#.*?=<>|[]{ } "'()'`.

   a) Sélectionnez **Créer**, puis entrez le nom d'utilisateur et le mot de passe du compte Azure Active Directory.

   b) Sélectionnez **Se connecter**.

   c) Sélectionnez **Accepter** pour accorder à Citrix DaaS les autorisations indiquées. Azure crée un principal de service qui permet à Citrix DaaS de gérer les ressources Azure pour le compte de l'utilisateur spécifié.

   d) Une fois que vous avez sélectionné **Accepter**, vous êtes redirigé vers la page **Détails de la connexion**.

   > **Remarque :**
   >
   > Une fois que vous vous êtes authentifié auprès d'Azure, les boutons **Créer** et **Utiliser existant** disparaissent. La mention **Connexion établie** accompagnée d'une coche verte indique que la connexion à votre abonnement Azure a réussi.

e) Pour acheminer les requêtes d'API vers Azure via des composants Citrix Cloud Connector, cochez la case **Acheminer le trafic via des Citrix Cloud Connector**.

Vous pouvez également activer cette fonctionnalité à l'aide de PowerShell. Pour plus d'informations, consultez la section Créer un environnement sécurisé pour le trafic géré par Azure.

> **Remarque :**
>
> Cette option n'est disponible que lorsque des Citrix Cloud Connector sont actifs dans votre déploiement. Actuellement, cette fonctionnalité n'est pas prise en charge pour les Connector Appliance.

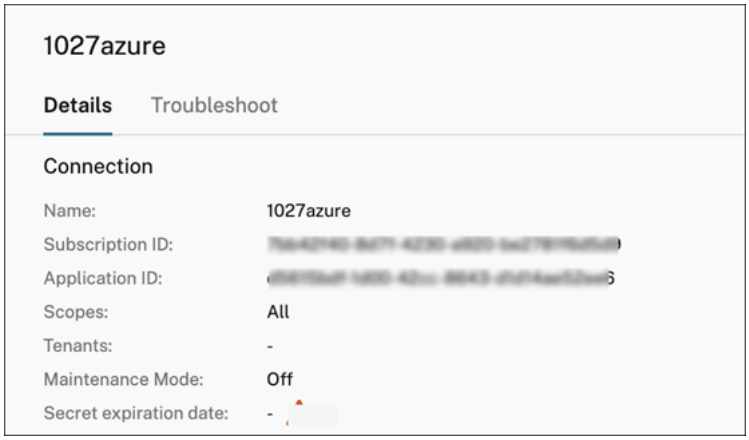
f) Sélectionnez **Suivant**.

> **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.

4. Configurez les ressources pour la connexion comme suit :
   - 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.
5. 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 :

1. Connectez-vous à votre abonnement Azure Resource Manager.

   ```
   Connect-AzAccount
   ```

2. Sélectionnez l'abonnement Azure Resource Manager sur lequel vous souhaitez créer le principal de service.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

3. Créez l'application dans votre locataire AD.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

4. Créez un principal de service.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```


5. Attribuez un rôle au principal de service.

```
New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
 $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
```

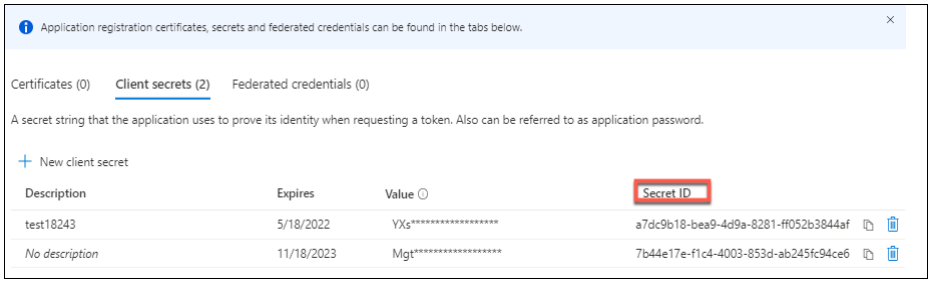
6. Dans la sortie de la fenêtre de la console PowerShell, notez la valeur ApplicationId. Vous fournissez cet ID lors de la création de la connexion hôte.

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 l'interface Configuration complète 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 Configuration complète.

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**. Entrez 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 comme suit :

   - 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 la gestion des appareils joints à Azure AD
- Gérer le principal de service d'une connexion hôte existante
- 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
- Créer un environnement sécurisé pour le trafic géré par Azure
- 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.

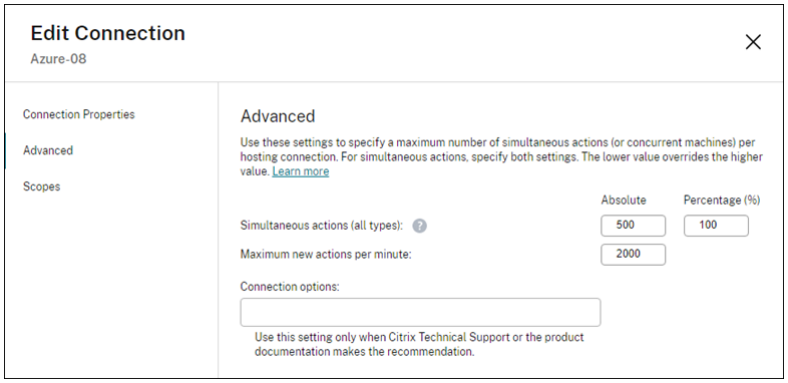
Pour aider à atténuer ces problèmes, Citrix DaaS vous permet de supprimer la limitation interne de MCS pour utiliser une plus grande partie du quota de demandes disponible d'Azure.

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 l'interface Configuration complète pour configurer les opérations Azure pour une connexion hôte donnée :

1. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
2. Sélectionnez une connexion liée à Azure pour la modifier.
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 la gestion des appareils joints à Azure AD

Dans Azure, les appareils joints à Azure AD obsolètes peuvent empêcher de nouvelles machines de rejoindre Azure AD, ce qui affecte leur fonctionnement. Pour éviter d'éventuels problèmes, vous pouvez autoriser les connexions à gérer les appareils joints à Azure AD. Avec cette autorisation, les connexions peuvent automatiquement nettoyer les appareils joints à Azure AD obsolètes.

> **Remarque :**
>
> Les appareils joints à Azure AD ne peuvent pas être supprimés d'Azure AD lorsque vous supprimez des machines ou des catalogues de machines.

1. Dans **Gérer > Configuration complète**, sélectionnez "Hébergement"dans le panneau de gauche.
2. Sélectionnez la connexion, puis sélectionnez **Modifier la connexion** dans le volet Actions.
3. Sélectionnez **Propriétés de connexion** dans le volet de gauche.
4. Sur la page **Propriétés de connexion** qui s'affiche, procédez comme suit :
   a) Sélectionnez **Activer la gestion des appareils connectés à Azure AD**.
   b) Cliquez sur **Enregistrer**.

c) Dans la fenêtre de connexion Azure qui s'affiche, entrez votre mot de passe d'abonnement, puis cliquez sur **Se connecter**.

Une fois la connexion terminée, vous êtes redirigé vers la liste des connexions et des ressources d'hébergement. Cliquez sur la connexion dans la liste, puis sur l'onglet **Détails** dans le volet inférieur. Vous pouvez voir que le champ **Gestion des appareils joints à Azure AD** indique **Activé**.

Lorsque vous activez la gestion des appareils joints à Azure AD avec Configuration complète, vous devez vous authentifier auprès d'Azure AD quelle que soit la méthode de création de connexion hôte choisie (créer une nouvelle connexion ou utiliser une connexion existante). Le rôle d'**administrateur d'appareils cloud** intégré à Azure AD est attribué au principal du service. Pour adopter les autorisations minimales pour la gestion des appareils joints à Azure AD, vous pouvez supprimer manuellement l'attribution du rôle d'**administrateur d'appareils cloud** au principal de service et créer un rôle personnalisé Azure AD qui inclut uniquement les autorisations minimales et l'attribuer au principal de service.

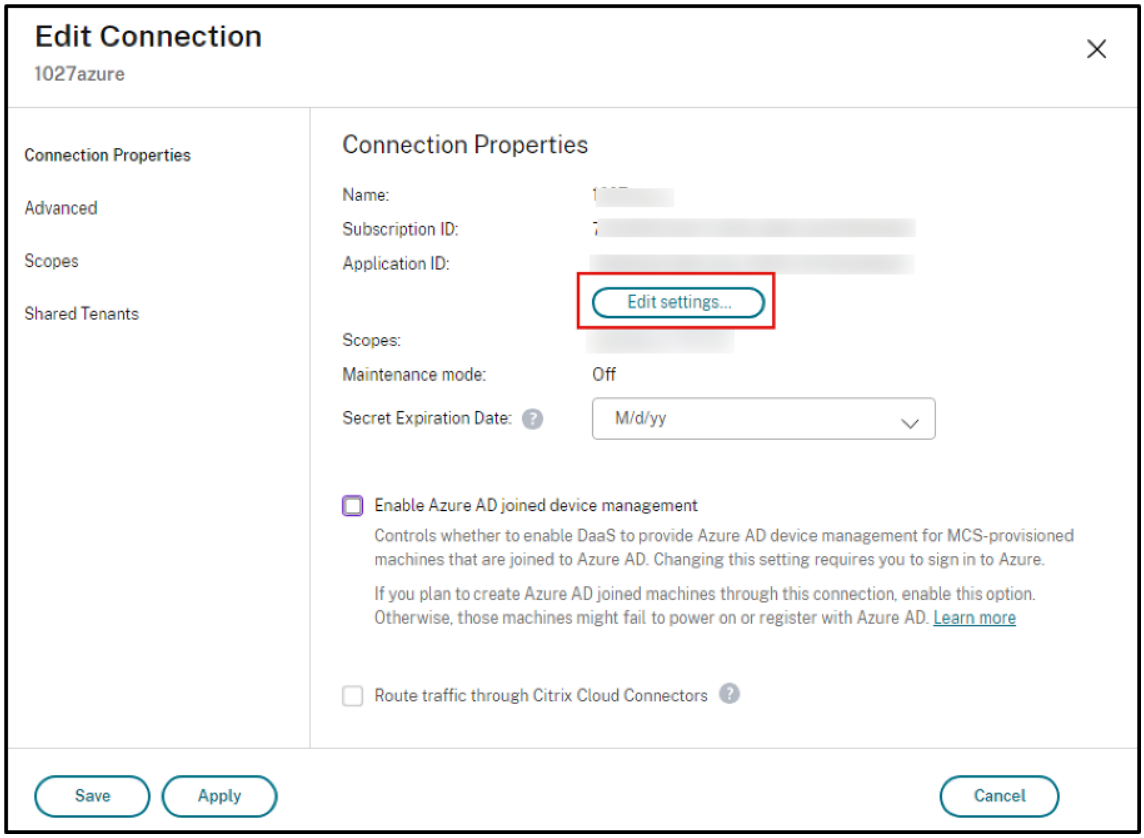
> **Remarque :**
>
> - Les autorisations minimales pour la gestion des appareils joints à Azure AD sont les autorisations Azure AD et non les autorisations Azure Resource Manager. Elles ne peuvent pas être attribuées explicitement à un principal de service. Vous devez créer un rôle personnalisé dans Azure AD qui inclut ces autorisations et l'attribuer au principal du service. Voir Créer et attribuer un rôle personnalisé dans Azure Active Directory pour plus de détails.
> - Pour créer un rôle personnalisé dans Azure AD, vous avez besoin d'une licence Azure AD Premium P1 ou P2.

Gérer le principal de service d'une connexion hôte existante

Après avoir créé une connexion hôte qui utilise un principal de service, vous pouvez choisir de la modifier de façon à :

- obtenir un nouveau principal de service ;
- utiliser un principal de service existant

1. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.
2. Sélectionnez la connexion, puis sélectionnez **Modifier la connexion** dans le volet Actions.
3. Sélectionnez **Propriétés de connexion** dans le volet de gauche.
4. Sur la page **Propriétés de la connexion**, cliquez sur **Modifier les paramètres**. Vous pouvez désormais choisir de créer un principal de service ou d'utiliser un principal de service existant.



- Cliquez sur **Créer un principal de service** pour créer un principal de service. Suivez les instructions pour vous connecter à votre compte utilisateur Azure AD. Citrix utilise l'ID de l'application multi-locataire `08b70dc3-76c5-4611-ba7d-3312ba36cb2b` pour créer un principal de service pour la connexion hôte existante et accorder les autorisations appropriées.

  Si vous sélectionnez **Activer la gestion des appareils connectés à Azure AD** sur la page **Propriétés de la connexion**, le rôle d'administrateur des appareils cloud intégrés à Azure AD est attribué au principal de service nouvellement créé.

- Cliquez sur **Utiliser existant** pour utiliser un principal de service existant pour cette connexion hôte. Il existe toutefois deux scénarios :

  - Si vous sélectionnez **Activer la gestion des appareils connectés à Azure AD**, vous êtes invité à vous connecter à votre compte utilisateur Azure AD. Citrix utilise alors l'ID de l'application multi-locataire `08b70dc3-76c5-4611-ba7d-3312ba36cb2b` pour attribuer le rôle d'administrateur des appareils cloud intégrés à Azure AD au principal de service existant.
  - Si vous ne sélectionnez pas **Activer la gestion des appareils connectés à Azure AD**, vous n'êtes pas invité à vous connecter à votre compte utilisateur Azure AD. Vous devez alors entrer l'ID de l'application et la clé secrète du principal de service existant.

Pour en savoir plus sur l'activation de la gestion des appareils connectés à Azure AD, consultez Activer la gestion des appareils connectés à Azure AD.

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.

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.

Ajouter des locataires partagés à une connexion à l'aide de la configuration complète

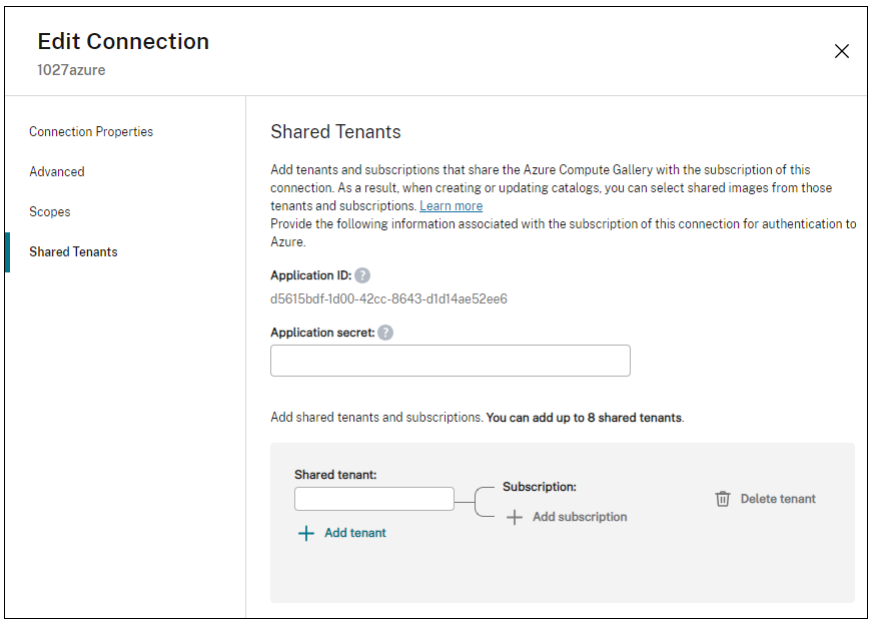
Lorsque vous créez ou mettez à jour des catalogues de machines dans l'interface Configuration complète, vous pouvez sélectionner des images partagées à partir de différents locataires et abonnements Azure (partagées via la galerie Azure Compute Gallery). Cette fonctionnalité exige que vous fournissiez 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 **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.

2. Sélectionnez la connexion, puis sélectionnez **Modifier la connexion** dans le volet Actions.



3. Dans **Locataires partagés**, procédez comme suit :

   a) Fournissez l'ID d'application et le secret d'application associés à l'abonnement de la connexion. DaaS utilise ces informations pour s'authentifier auprès d'Azure AD.
   b) 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/.

Créer un environnement sécurisé pour le trafic géré par Azure

MCS permet d'acheminer le trafic réseau (appels d'API de Citrix Cloud vers l'hyperviseur Azure) via les Cloud Connectors de votre environnement. Cette implémentation vous permet de verrouiller votre

abonnement Azure pour autoriser le trafic réseau à partir d'adresses IP spécifiques. Pour ce faire, ajoutez `ProxyHypervisorTrafficThroughConnector` dans `CustomProperties`. Après avoir défini les propriétés personnalisées, vous pouvez configurer des stratégies Azure pour avoir un accès privé aux disques gérés par Azure.

Si vous configurez la stratégie Azure pour créer automatiquement des accès au disque pour chaque nouveau disque afin d'utiliser des points de terminaison privés, vous ne pouvez pas charger ou télécharger plus de cinq disques ou instantanés en même temps avec le même objet d'accès au disque imposé par Azure. Cette limite s'applique à chaque catalogue de machines si vous configurez la politique Azure au niveau du groupe de ressources, et à tous les catalogues de machines si vous configurez la politique Azure au niveau de l'abonnement.
Si vous ne configurez pas la stratégie Azure pour créer automatiquement des accès au disque pour chaque nouveau disque afin d'utiliser des points de terminaison privés, la limite de cinq opérations simultanées n'est pas appliquée.

> **Remarque :**
>
> Actuellement, cette fonctionnalité n'est pas prise en charge pour Connector Appliance. Pour connaître les limites d'Azure liées à cette fonctionnalité, consultez Restreindre l'accès à l'importation/exportation pour les disques gérés à l'aide d'Azure Private Link.

Activer le proxy Pour activer le proxy, définissez les propriétés personnalisées comme suit sur la connexion hôte :

1. Ouvrez une fenêtre PowerShell à l'aide du Remote PowerShell SDK. Pour plus d'informations, consultez https://docs.citrix.com/en-us/citrix-daas/sdk-api.html#citrix-virtual-apps-and-desktops-remote-powershell-sdk/.
2. Exécutez les commandes suivantes :

```
Add-PSSnapin citrix*.
cd XDHyp:\Connections\
dir
<!--NeedCopy-->
```

3. Copiez `CustomProperties` depuis la connexion vers un bloc-notes et ajoutez le paramètre de propriété `<Property xsi:type="StringProperty"Name="ProxyHypervisorTrafficTh "Value="True"/>` à `CustomProperties` pour activer le proxy. 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="SubscriptionId" Value="
    4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<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="5cxxxxx
   -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
   ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>
<!--NeedCopy-->
```

4. Dans la fenêtre PowerShell, attribuez une variable aux propriétés personnalisées modifiées. Par exemple :

```
$customProperty = '<CustomProperties xmlns:xsi="http://www.w3.org
   /2001/XMLSchema-instance" xmlns="http://schemas.citrix.com
   /2014/xd/machinecreation">
<Property xsi:type="StringProperty" Name="SubscriptionId" Value
   ="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<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="5cxxxxx
   -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
   ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Exécutez `$cred = Get-Credential`. Si vous y êtes invité, fournissez les informations d'identification de connexion. Les informations d'identification sont l'ID d'application Azure et le code secret.

6. Exécutez `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password`.

   > **Important :**
   >
   > Si vous recevez un message indiquant que `SubscriptionId` manque, remplacez tous les guillemets doubles (“) par un guillemet inverse suivi de guillemets doubles (‘”) dans la propriété personnalisée. 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=`"SubscriptionId`"
   Value=`"4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx`" />
```



```
<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=`"5
    cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx`" />
<Property xsi:type=`"StringProperty`" Name=`"
    ProxyHypervisorTrafficThroughConnector`" Value=`"True`" />
</CustomProperties>
<!--NeedCopy-->
```

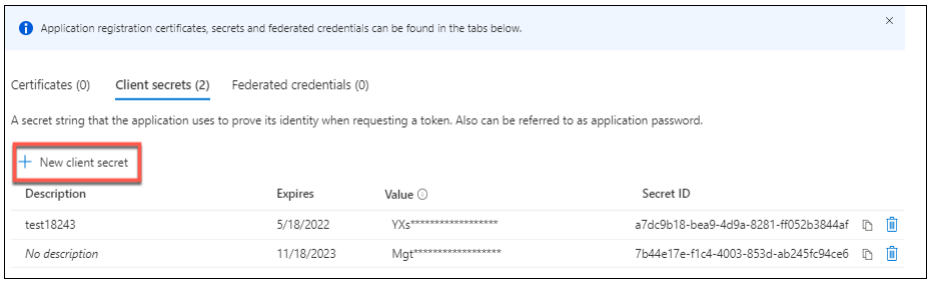
7. Exécutez `dir` pour vérifier les paramètres `CustomProperties` mis à jour.

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 l'interface Configuration complète 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**.

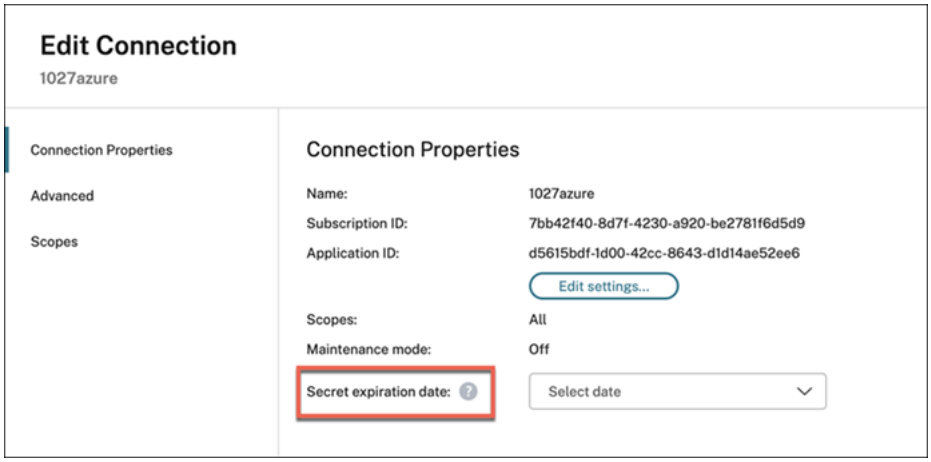
> **Remarque :**
>
> Veillez à enregistrer le secret client car vous ne pouvez pas le récupérer ultérieurement.

6. Copiez la valeur du secret client et la date d'expiration.

7. Dans l'interface Configuration complète, 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 l'interface Configuration complète 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 détaille 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 accordées. Cette section répertorie les autorisations minimales par action.

Création d'une connexion hôte Ajoutez une connexion hôte à l'aide des informations obtenues auprès d'Azure.

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
"Microsoft.Resources/providers/read",
```



```
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/tenants/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",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
<!--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 les images principales sont des disques gérés 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.Resources/tags/read",
"Microsoft.Resources/tags/write",
"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.Compute/locations/publishers/artifacttypes/types/versions/
   read",
"Microsoft.Compute/skus/read",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Features/providers/features/read",
"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",
"Microsoft.Network/locations/usages/read",
<!--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 provenant d'Azure Compute Gallery (anciennement 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, un instantané ou un disque dur virtuel se trouvant 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",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
<!--NeedCopy-->
```

- Si vous utilisez le groupe de ressources géré par Citrix :

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
<!--NeedCopy-->
```

- Si vous placez l'image principale dans Azure Compute Gallery (anciennement Shared Image Gallery) dans un locataire ou un abonnement partagé :

```
"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",
"Microsoft.Resources/subscriptions/read",
<!--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",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
<!--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.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
```



```
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"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",
"Microsoft.Network/locations/usages/read",
<!--NeedCopy-->
```

Gestion des appareils joints à Azure AD Vous trouvez ci-dessous la liste des autorisations minimales requises pour gérer les appareils joints à Azure AD :

```
microsoft.directory/devices/standard/read
microsoft.directory/devices/delete
<!--NeedCopy-->
```

Autorisations générales

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",
```



```
14  "Microsoft.Compute/galleries/read",
15  "Microsoft.Compute/galleries/write",
16  "Microsoft.Compute/hostGroups/hosts/read",
17  "Microsoft.Compute/hostGroups/read",
18  "Microsoft.Compute/hostGroups/write",
19  "Microsoft.Compute/snapshots/beginGetAccess/action",
20  "Microsoft.Compute/snapshots/delete",
21  "Microsoft.Compute/snapshots/endGetAccess/action",
22  "Microsoft.Compute/snapshots/read",
23  "Microsoft.Compute/snapshots/write",
24  "Microsoft.Compute/virtualMachines/deallocate/action",
25  "Microsoft.Compute/virtualMachines/delete",
26  "Microsoft.Compute/virtualMachines/read",
27  "Microsoft.Compute/virtualMachines/restart/action",
28  "Microsoft.Compute/virtualMachines/start/action",
29  "Microsoft.Compute/virtualMachines/write",
30  "Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
       read",
31  "Microsoft.Compute/skus/read",
32  "Microsoft.Compute/virtualMachines/extensions/read",
33  "Microsoft.Compute/virtualMachines/extensions/write",
34  "Microsoft.Network/networkInterfaces/delete",
35  "Microsoft.Network/networkInterfaces/join/action",
36  "Microsoft.Network/networkInterfaces/read",
37  "Microsoft.Network/networkInterfaces/write",
38  "Microsoft.Network/networkSecurityGroups/delete",
39  "Microsoft.Network/networkSecurityGroups/join/action",
40  "Microsoft.Network/networkSecurityGroups/read",
41  "Microsoft.Network/networkSecurityGroups/write",
42  "Microsoft.Network/virtualNetworks/subnets/read",
43  "Microsoft.Network/virtualNetworks/read",
44  "Microsoft.Network/virtualNetworks/subnets/join/action",
45  "Microsoft.Network/locations/usages/read",
46  "Microsoft.Resources/deployments/operationstatuses/read",
47  "Microsoft.Resources/deployments/read",
48  "Microsoft.Resources/deployments/validate/action",
49  "Microsoft.Resources/deployments/write",
50  "Microsoft.Resources/deployments/delete",
51  "Microsoft.Resources/subscriptions/resourceGroups/read",
52  "Microsoft.Resources/subscriptions/resourceGroups/write",
53  "Microsoft.Resources/subscriptions/resourceGroups/delete",
54  "Microsoft.Resources/providers/read",
55  "Microsoft.Resources/subscriptions/locations/read",
56  "Microsoft.Resources/subscriptions/read",
57  "Microsoft.Resources/tags/read",
58  "Microsoft.Resources/tags/write",
59  "Microsoft.Resources/tenants/read",
60  "Microsoft.Resources/templateSpecs/read",
61  "Microsoft.Resources/templateSpecs/versions/read",
62  "Microsoft.Storage/storageAccounts/delete",
63  "Microsoft.Storage/storageAccounts/listKeys/action",
64  "Microsoft.Storage/storageAccounts/read",
65  "Microsoft.Storage/storageAccounts/write",
```



```
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
<!--NeedCopy-->
```

Autorisation Azure AD Si vous créez des catalogues de machines jointes à Azure AD, MCS est responsable de la gestion des appareils Azure AD lorsque vous activez la gestion des appareils joints à Azure AD. Le rôle d'**administrateur d'appareils cloud** intégré à Azure AD offre la meilleure compatibilité à l'avenir, même s'il inclut plus d'autorisations que ce qui est nécessaire avec l'ensemble de fonctionnalités actuel.

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

- Créer et gérer des connexions et des ressources
- Environnements de virtualisation Microsoft Azure Resource Manager

Connexion à Microsoft System Center Virtual Machine Manager

January 25, 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 Virtual Machine Manager (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 administratif 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

- Créer et gérer des connexions et des ressources
- Environnements de virtualisation Microsoft System Center Virtual Machine Manager.

Connexion à Nutanix

January 25, 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 complètent les instructions de la section Créer et gérer des connexions. 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 l'hyperviseur.

  > **Remarque :**
  >
  > Actuellement, le type de connexion **PC Nutanix AHV** 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 vos adresse et nom d'utilisateur, puis importez les clés publiques et privées contenues dans vos fichiers d'informations d'identification Nutanix DRaaS (`.pem`). (Les administrateurs Nutanix DRaaS génèrent les clés publiques et privées dans le cloud Nutanix DRaaS.)

  - Pour importer la clé, recherchez votre fichier d'informations d'identification, ouvrez-le à l'aide du Bloc-notes (ou tout éditeur de texte), puis copiez le contenu. Revenez ensuite à la page **Connexion**, sélectionnez **Importer clé**, collez le contenu, puis sélectionnez **Enregistrer**.

  Attention : ne modifiez pas le contenu des informations d'identification ni leur format.

> **Conseil :**
>
> Si vous déployez des machines en utilisant Nutanix AHV (Prism Element) comme ressource, sélec-

> tionnez 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

- Créer et gérer des connexions et des ressources
- Environnements de virtualisation Nutanix
- Solutions partenaires et cloud Nutanix

Connexion aux solutions partenaires et cloud Nutanix

January 25, 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 DaaS (anciennement Citrix Virtual Apps and Desktops Service) prend en charge la solution partenaire et cloud Nutanix suivante :

- Nutanix Cloud Clusters sur AWS

> **Remarque :**
>
> - Avant de créer une connexion à une solution partenaire et à 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.
> - Pour obtenir les dernières informations sur la configuration de Nutanix sur le cloud, consultez le dernier guide 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. Dans **Gérer > Configuration complète**, sélectionnez **Hébergement** dans le panneau de gauche.

2. 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 :**
>
> Le plug-in Nutanix doit être installé sur toutes les machines virtuelles de connecteur pour que l'option Nutanix soit disponible dans Citrix Studio, même si les plug-ins ne sont pas utilisés 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

- Créer et gérer des connexions et des ressources
- Environnements de virtualisation Nutanix
- Solutions partenaires et cloud Nutanix

Connexion à VMware

May 17, 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.

Autorisations requises

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 opérations Citrix DaaS et les autorisations VMware minimales requises correspondantes.

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
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

SDK	Interface utilisateur
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
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, mise à jour 2, vSphere 5.1, mise à jour 1 et vSphere 6.x, mise à jour 1 : Machine virtuelle > État > Créer un instantané ; vSphere 5.5 : Machine virtuelle > Gestion des snapshots > Créer un instantané ; vSphere 8.0 : Machine virtuelle > Gestion des instantanés > Créer un instantané

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
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

SDK	Interface utilisateur

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

SDK	Interface utilisateur
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
Cryptographic operations.Direct Access	Privileges > All Privileges > Cryptographic operations > Direct Access
Cryptographic operations.Add disk	Privileges > All Privileges > Cryptographic operations > Add disk
Cryptographic operations.Clone	Privileges > All Privileges > Cryptographic operations > Clone
Cryptographic operations.Encrypt	Privileges > All Privileges > Cryptographic operations > Encrypt
Cryptographic operations.Encrypt new	Privileges > All Privileges > Cryptographic operations > Encrypt new
Cryptographic operations.Decrypt	Privileges > All Privileges > Cryptographic operations > Decrypt
Cryptographic operations.Migrate	Privileges > All Privileges > Cryptographic operations > Migrate

SDK	Interface utilisateur
Cryptographic operations.Read KMS information	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
vApp.Export	vApp > Export

> **Remarque :**
>
> `vApp.Export` est nécessaire pour créer des catalogues de machines MCS à l'aide du profil de machine.

Sécuriser les connexions à l'environnement VMware

L'utilisation de connexions HTTPS/SSL à vCenter nécessite que les connexions soient approuvées par Citrix DaaS.

Il existe deux options :

- (Recommandé) L'empreinte numérique SSL est installée sur la base de données Citrix DaaS. Citrix DaaS utilise cette empreinte numérique sur chaque composant Cloud Connector pour approuver les connexions à vCenter.
- (Alternative) Chaque composant Cloud Connector approuve le certificat vCenter et les services disponibles sur Cloud Connector réutilisent cette approbation. Cette approbation peut provenir d'une des sources suivantes :
  - certificat vCenter, émis par l'autorité de certification et approuvé par Windows, résultant en une approbation établie entre Windows et vCenter ;
  - certificat vCenter installé sur Windows, donnant lieu à une approbation établie entre Windows et vCenter

> **Remarque :**
>
> Le certificat vCenter et l'empreinte numérique SSL VMware ne sont pas nécessaires pour VMware Cloud et ses solutions partenaires.

Empreinte numérique SSL VMware

La fonctionnalité d'empreinte numérique SSL VMware résout une erreur fréquemment signalée lors de la création d'une connexion hôte sur un hyperviseur VMware vSphere. Précédemment, les administrateurs devaient créer manuellement une relation d'approbation entre les Delivery Controller gérés par Citrix dans le site et le certificat de l'hyperviseur avant de créer une connexion. La fonctionnalité d'empreinte numérique SSL VMware élimine cette opération manuelle : l'empreinte numérique du certificat non approuvé est stockée dans la base de données du site, de sorte que l'hyperviseur est continuellement identifié comme approuvé par Citrix DaaS, même s'il ne l'est pas par les contrôleurs.

Lors de la création d'une connexion hôte vSphere, 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.

L'empreinte numérique VMware SSL peut être mise à jour ultérieurement à l'aide du kit SDK PowerShell `Set-Item -LiteralPath "<FullPath_to_connection>"-username $cred.username -Securepassword $cred.password -SslThumbprint "<New ThumbPrint>"-hypervisorAddress <vcenter URL>`.

> **Conseil :**
>
> L'empreinte numérique du certificat doit être écrite en lettres majuscules.

Obtenir et importer un certificat

Pour protéger les communications vSphere, Citrix vous recommande d'utiliser HTTPS plutôt que HTTP. HTTPS requiert des certificats numériques. Citrix vous recommande d'utiliser un certificat

numérique émis par une autorité de certification conformément à la stratégie de sécurité de votre organisation.

Si vous ne pouvez pas utiliser un certificat numérique émis par une autorité de certification et que la stratégie de sécurité de votre organisation le permet, vous pouvez utiliser le certificat auto-signé installé par VMware. Ajoutez le certificat VMware vCenter à chaque Cloud Connector.

1. Ajoutez le nom de domaine complet (FQDN) de l'ordinateur exécutant vCenter Server dans le fichier d'hôtes de ce serveur, situé 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 Cloud Connector.
   b) Sur le Cloud Connector, 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, selon votre compte utilisateur, 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) Cliquez sur **Certificat non valide**, puis sur l'onglet **Détails**.
   e) Cliquez sur **Exporter…**
   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 :

   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.

3. Importez le certificat dans le magasin de certificats sur chacun de vos Cloud Connector.

   a) Cliquez sur **Installer le certificat**, sélectionnez **Machine locale**, puis cliquez sur **Suivant**.

b) Sélectionnez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur **Parcourir**. Sur une version ultérieure prise en charge : sélectionnez **Personnes autorisées** et cliquez sur **OK**. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

> **Important :**
>
> 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

- Créer et gérer des connexions et des ressources
- Environnements de virtualisation VMware.
- Solutions VMware Cloud et partenaires

Connexion aux solutions partenaires et cloud VMware

January 25, 2024

Après avoir configuré le cluster Azure VMware Solution (AVS), Google Cloud VMware Engine et VMware Cloud sur AWS, créez les connexions. Consultez la section Connexion aux environnements de virtualisation 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

- Créer et gérer des connexions et des ressources
- Environnements de virtualisation VMware.
- Solutions partenaires et cloud VMware

Connexion à XenServer

April 18, 2024

L'article Créer et gérer des connexions et des ressourcesfournit des instructions détaillées sur la création d'une connexion à l'aide de l'assistant. Avant d'établir une connexion à XenServer (anciennement Citrix Hypervisor), vous devez d'abord terminer la configuration de votre instance de XenServer en tant qu'hôte. Consultez la section Ajouter un type de ressource ou activer un domaine inutilisé dans Citrix Cloud.

Créer une connexion à XenServer

Lorsque vous créez une connexion à XenServer, vous devez fournir les informations d'identification d'un administrateur d'alimentation de VM ou d'un utilisateur de niveau supérieur.

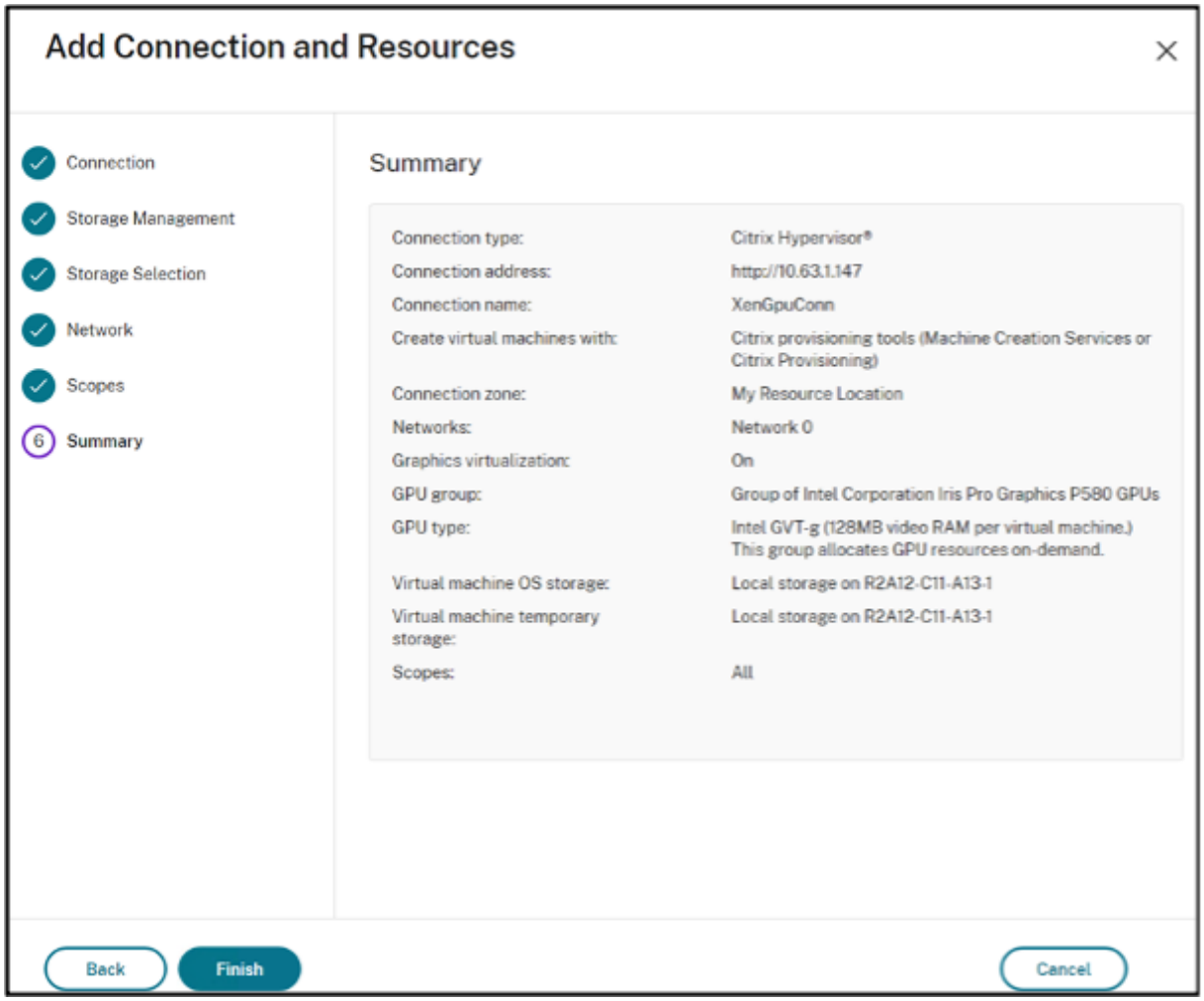
Citrix vous recommande d'utiliser HTTPS pour sécuriser les communications avec XenServer. Pour utiliser HTTPS, vous devez remplacer le certificat SSL par défaut installé sur XenServer. Pour plus d'informations, consultez la section Installer un certificat TLS sur votre serveur.

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.

> **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.

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.)

Si vous vous connectez au XenServer qui prend en charge le processeur graphique virtuel, vous pouvez vérifier le groupe et le type de processeur graphique sur la page **Résumé** de l'assistant de création de connexion.



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.

Remarques importantes :

- Le stockage partagé doit être de type NFS si vous utilisez IntelliCache.

- Afin d'assurer un transfert de données optimal, Citrix vous recommande d'utiliser un périphérique de stockage local à hautes performances.

Pour utiliser la fonctionnalité IntelliCache, activez-la comme indiqué :

- Lors de l'installation de XenServer, sélectionnez **Activer l'allocation dynamique**. Pour plus d'informations sur l'installation de l'hôte XenServer à partir d'un support local, consultez la section Installer l'hôte XenServer. Citrix ne prend pas en charge les pools mixtes de serveurs dont certains ont la fonctionnalité IntelliCache activée et d'autres non.
- Dans Citrix DaaS, IntelliCache est désactivé par défaut. Vous ne pouvez changer ce paramètre que lors de la création d'une connexion XenServer. Vous ne pourrez pas désactiver IntelliCache ultérieurement. Lorsque vous créez une connexion XenServer :
  - Sélectionnez**Partagé**en tant que type de stockage.
  - Cochez la case **Utiliser IntelliCache**.

Pour plus d'informations, consultez l'article 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 ou supprimer des machines virtuelles aux planifications d'instantanés existantes	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 du port de commutateur)
Créer un catalogue de machines	Opérateur de pool : nécessite le verrouillage du port de 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 des informations spécifiques à XenServer, consultez l'article Créer un catalogue XenServer.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Environnements de virtualisation XenServer

Créer des catalogues de machines

June 13, 2024

> **Remarque :**
>
> Cet article explique comment créer des catalogues à l'aide de l'interface Configuration complète. Si vous utilisez Déploiement rapide pour créer des ressources Azure, suivez les instructions dans Création de catalogues avec Déploiement rapide.

Des collections de machines virtuelles ou physiques sont gérées comme une seule entité appelée catalogue de machines. Dans un catalogue de machines, toutes les machines partagent un type de système d'exploitation commun, qui peut être un système d'exploitation multi-session ou mono-session, tel que Windows ou Linux.

L'interface **Gérer > Configuration complète** vous guide pour créer le premier catalogue de machines. Après la création du premier catalogue, vous créez le premier groupe de mise à disposition. Plus tard, vous pourrez modifier le catalogue que vous avez créé et créer des catalogues supplémentaires.

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.

- Si vous utilisez MCS pour provisionner des VM, vous devez fournir une image (ou un instantané) pour créer des machines virtuelles identiques dans le catalogue. Avant de créer le catalogue, vous devez configurer une connexion d'hébergement pour la première fois à l'hyperviseur ou au service cloud de votre choix, puis créer et configurer l'image principale sur celui-ci. La configuration de l'image principale nécessite des tâches telles que la jonction de domaines le cas échéant, l'installation des pilotes requis, la publication d'applications et le déploiement du VDA (Virtual Delivery Agent) sur l'image.
- Une fois l'image principale créée, vous créez le catalogue de machines dans l'interface **Gérer > Configuration complète**. Vous sélectionnez cette image (ou un instantané de cette image), spécifiez le nombre de machines virtuelles à créer dans le catalogue et configurez les informations supplémentaires.

- Si vos machines sont déjà disponibles, vous devez tout de même créer un ou plusieurs catalogues afin d'y importer ces machines virtuelles.

Lorsque vous utilisez MCS pour créer le premier catalogue, vous spécifiez une unité d'hébergement que vous avez créée précédemment. L'unité d'hébergement fournit la configuration des ressources pour vous permettre de créer une machine virtuelle. Plus tard (après avoir créé votre premier catalogue et votre premier groupe de mise à disposition), vous pouvez modifier les informations relatives à cette unité d'hébergement ou à sa connexion hôte parent ou créer d'autres connexions et unités d'hébergement.

Si un composant Cloud Connector ne fonctionne pas correctement, les opérations de provisioning MCS (telles que les mises à jour de catalogue) prennent beaucoup plus de temps que d'habitude et les performances de l'interface de gestion se dégradent considérablement.

Vérification des licences RDS

La création d'un catalogue de machines contenant des machines avec OS multi-session Windows comprend une vérification automatique des licences RDS. Une recherche est effectuée dans le catalogue pour trouver une machine sous tension et enregistrée sur laquelle effectuer la vérification.

- Si une machine sous tension et enregistrée ne peut pas être trouvée, un avertissement s'affiche, indiquant que la vérification des licences RDS ne peut pas être exécutée.
- Si une machine est trouvée, et qu'une erreur est détectée, **Gérer > Configuration complète** affiche un message d'avertissement pour le catalogue de machines contenant le problème détecté. Pour supprimer un avertissement de licence RDS d'un catalogue (afin qu'il n'apparaisse plus sur l'écran), sélectionnez le catalogue. Sélectionnez **Supprimer l'avertissement de licence RDS**. Lorsque vous y êtes invité, confirmez l'action.

Enregistrement de VDA

Un VDA doit être enregistré auprès 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 plusieurs raisons pour lesquelles un VDA peut ne pas être enregistré, un grand nombre d'entre elles pouvant être résolues. Des informations de dépannage sont fournies 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.

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.

Pour plus d'informations sur le dépannage de l'enregistrement de VDA, voir l'article CTX136668.

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 sélectionnez une image (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, la copie complète de l'instantané ou de l'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 (mentionnée ci-dessus), qui est en lecture seule et partagée entre les VM 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 reçoit un disque de différenciation. Le disque de différence conserve les modifications apportées au cours de sessions. Il est permanent pour les postes de travail dédiés. Pour les postes de travail regroupés, il est supprimé et un autre est créé après chaque redémarrage.

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 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)

La fonctionnalité d'optimisation du stockage Machine Creation Services (MCS) est également connue sous le nom d'E/S MCS. Cette fonctionnalité n'est disponible que sur Azure, GCP, XenServer, VMware et SCVMM.

- 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 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.

Activer les mises à jour de l'optimisation du stockage MCS Pour activer la fonctionnalité d'optimisation du stockage E/S MCS, mettez à niveau le Delivery Controller et le VDA avec la dernière version de Citrix DaaS.

> **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.

Pour plus d'informations sur l'attribution d'une lettre de lecteur au disque de cache en écriture différée, consultez Attribuer une lettre de lecteur spécifique au disque de cache en écriture différée des E/S de MCS.

Préparer une image principale sur l'hyperviseur ou le service de cloud

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 et les fournisseurs de service cloud peuvent utiliser des termes différents.
- Assurez-vous que l'hyperviseur ou le service cloud 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.
- Considérations liées à l'activation de Microsoft KMS lors de l'utilisation de MCS : si votre déploiement comprend un VDA 7.x avec XenServer 6.1 ou 6.2, vSphere ou hôte Microsoft System Center Virtual Machine Manager, vous n'avez pas à réarmer manuellement Microsoft Windows ou Microsoft Office.

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 du VDA 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 partir de **Gérer > Configuration complète**. 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 afin qu'il puisse être identifié. Si vous spécifiez une image principale plutôt qu'un instantané lors de la création d'un catalogue, l'interface de gestion crée un instantané, mais 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 versions 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.

Créez un catalogue de machines à l'aide de l'interface Configuration complète

Avant de créer un catalogue :

- 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 les machines. assurez-vous d'avoir installé un VDA sur cette image principale.

> **Remarque :**
>
> Lorsque vous utilisez un service cloud ou un hyperviseur pour héberger des machines virtuelles, l'assistant de création de catalogue peut contenir des pages supplémentaires spécifiques à cet hôte. Par exemple, lorsque vous utilisez une image principale Azure Resource Manager, l'assistant de création de catalogue contient une page **Types de stockage et de licence**. Pour obtenir des informations spécifiques à l'hôte, consultez les articles mentionnés dans la section Autres ressources.

Lancer l'assistant de création de catalogue

1. Connectez-vous à Citrix Cloud. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.
2. Sélectionnez **Gérer**.
3. 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.
4. Si vous avez déjà créé un catalogue et que vous souhaitez en créer un autre, procédez comme suit :
    a) Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
    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 pages décrites dans les sections suivantes. Les pages qui s'affichent peuvent être différentes selon les sélections que vous effectuez et la connexion (à un hôte) que vous utilisez. Hôtes et ressources de virtualisation répertorie les sources d'informations pour les types d'hôtes pris en charge.

Sélectionner un type de machine

Chaque catalogue doit contenir des machines d'un seul type de système d'exploitation. Sélectionnez l'une des options suivantes sur la page **Type de machine** :

- **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 types.
- **OS mono-session :** un catalogue de machines avec 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.

Sélectionner les options de gestion des machines

> **Remarque :**
>
> La page **Gestion des machines** ne s'affiche pas si vous sélectionnez **Remote PC Access** sur la page **Type de machine**.

La page **Gestion des machines** indique le mode de gestion des machines et l'outil utilisé pour les déployer.

Sélectionnez l'une des options pour indiquer le mode de gestion de l'alimentation des machines via l'interface Configuration complète :

- **Machines avec alimentation gérée (par exemple, des machines virtuelles ou des PC lames)**: cette option n'est disponible que si vous avez déjà configuré une connexion à un hyperviseur ou à un service cloud.
- **Machines avec alimentation non gérée (par exemple, des machines physiques)**

Si vous sélectionnez l'option **Machines avec alimentation gérée (par exemple, machines virtuelles ou PC lames)**, sélectionnez un outil pour créer des machines virtuelles :

- **Citrix Machine Creation Services (MCS) :** utilise une image principale pour créer et gérer les machines virtuelles. Les catalogues de machine dans les environnements de cloud utilisent MCS. MCS n'est pas disponible pour les machines physiques.
- **Autre service ou technologie :** outil qui gère les machines déjà présentes 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.

> **Remarque :**
>
> Pour les machines avec système d'exploitation Linux, consultez l'article Créer un VDA Linux à l'aide de Machine Creation Services (MCS).

Sélectionner une expérience de bureau

> **Remarque :**
>
> Les options de la page **Expérience de bureau** varient en fonction du type de machine que vous sélectionnez sur la page **Type de machine**.

- Pour les machines avec **OS multi-session**, les utilisateurs se voient attribuer un bureau aléatoire chaque fois qu'ils ouvrent une session. Les options suivantes sont disponibles sur la page **Expérience de bureau** :
  - Enregistrer les modifications sur le disque local de la machine hébergeant les bureaux virtuels : persistant
  - Ignorer toutes les modifications et effacer les bureaux virtuels lorsque l'utilisateur ferme sa session : non persistant

  > **Remarque :**
  >
  > Pour les machines multi-sessions persistantes, les modifications apportées par les utilisateurs aux bureaux seront enregistrées et accessibles à tous les utilisateurs autorisés.

- Pour les machines avec système d'exploitation mono-session, vous pouvez accéder aux options suivantes sur la page **Expérience de bureau** :
  - 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.

  Vous pouvez également décider si les modifications apportées par les utilisateurs seront enregistrées ou supprimées après la fermeture de leur session.

Sélectionner une image

> **Remarque :**
>
> - Cette page ne s'affiche que si vous sélectionnez **Citrix Machine Creation Services (MCS)** sur la page **Gestion des machines**.
> - Les options disponibles sur cette page varient en fonction de l'hyperviseur ou du service de cloud.

Pour définir les paramètres sur cette page, procédez comme suit :

1. Sélectionnez un type d'image pour le catalogue de machines, puis sélectionnez une image. Deux types d'images sont disponibles :

   - **Image principale** : instantané ou machine virtuelle créé(e) en tant qu'image principale. Elle est soumise à une préparation automatique des images au début de la création de catalogues. Si nécessaire, vous pouvez ajouter une note pour l'image sélectionnée.

     > **Remarque :**
     >
     > – Lorsque vous utilisez MCS, n'exécutez pas Sysprep sur les images principales.
     > – Si vous spécifiez une image principale plutôt qu'un instantané, l'interface de gestion crée un instantané, mais vous ne pouvez pas le renommer.
     > – 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.
     > – Pour mettre à jour les images d'un nœud d'image, sélectionnez-le dans l'arborescence, puis cliquez sur l'option **Actualiser** dans le coin supérieur droit. Si vous ne sélectionnez aucun nœud d'image, cliquez sur **Actualiser** pour mettre à jour toutes les images de l'arborescence. Pour effacer un nœud sélectionné dans l'arborescence, maintenez la touche **CTRL** enfoncée, puis cliquez sur le nœud.

   - **Image préparée** : image ayant fait l'objet d'une préparation d'image, prête à être utilisée directement lors de la création de machines virtuelles. Opter pour des images préparées plutôt que pour des images principales pour 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.

   Pour plus d'informations sur la préparation des images, consultez l'article de blog Machine Creation Service: Image Preparation Overview and Fault-Finding.

2. Pour hériter des paramètres de machine virtuelle à partir d'un profil de machine, sélectionnez **Utiliser un profil de machine**, puis sélectionnez une spécification de modèle de machine virtuelle ou ARM (propre à Azure) à utiliser comme profil de machine.

> **Remarque :**
>
> Actuellement, l'utilisation de profils de machine est limitée aux machines virtuelles Azure, AWS et GCP.

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.

Configurer des machines

> **Remarque :**
>
> - Le titre de cette page dépend de ce que vous avez sélectionné sur la page **Gestion des machines** : **Machines**, **Machines virtuelles** ou **Machines et utilisateurs**.
> - Cette page ne s'affiche pas si vous sélectionnez **Remote PC Access** sur la page **Type de machine**.
> - Vous pouvez créer un catalogue vide, ce qui signifie que le catalogue ne contient aucune machine.

- **Lorsque vous utilisez MCS pour créer des machines :**
  - Spécifiez le nombre de machines virtuelles à créer. Entrez **0** (zéro) si vous ne souhaitez pas en créer. Plus tard, pour créer des machines virtuelles pour un catalogue vide, vous pouvez effectuer l'opération **Ajouter des machines**.
  - Choisissez la quantité de mémoire (Mo) pour chaque machine virtuelle.

    > **Important :**
    >
    > 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 vous indiquez sur la page **Expérience de bureau** que les modifications apportées par l'utilisateur aux bureaux statiques doivent être enregistrées dans un fichier Personal vDisk distinct, spécifiez la taille du disque virtuel en Go et la lettre de lecteur.
  - Si votre déploiement utilise plusieurs zones, vous pouvez sélectionner une zone (emplacement de ressources) 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 aléatoires non persistantes, vous pouvez activer et configurer le cache en écriture différée pour les données temporaires sur les

machines afin d'améliorer les performances d'E/S. Pour plus d'informations, consultez Configurer un cache pour les données temporaires.

- **Lorsque vous utilisez d'autres outils pour fournir des machines virtuelles :**

  Ajoutez les noms des comptes de machines (ou importez une liste de noms). Vous pouvez modifier le nom du compte d'une machine virtuelle après l'avoir ajoutée ou importée. Si vous avez spécifié des machines statiques sur la page **Expérience de bureau**, vous pouvez également spécifier le nom de l'utilisateur pour chaque VM que vous ajoutez.

  > **Conseil :**
  >
  > Pour ajouter des utilisateurs, localisez-les ou entrez manuellement une liste de noms d'utilisateur séparés par des points-virgules. Si les utilisateurs se trouvent dans Active Directory, entrez directement les noms. Si ce n'est pas le cas, entrez les noms au format suivant : `<identity provider>:<user name>`. Exemple : `AzureAD:username`.

  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 de l'assistant.

- **Lors de l'utilisation d'autres outils (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 Cloud Connector.

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.

Configurer un cache pour les données temporaires Lorsque vous utilisez MCS pour gérer des machines aléatoires non persistantes dans un catalogue, vous pouvez activer le cache en écriture différée pour les machines afin d'améliorer les performances d'E/S.

Le cache en écriture différée est appelé MCSIO. Pour plus d'informations, consultez cet article de blog.

Logiciels requis Pour activer le cache en écriture différée, le catalogue doit répondre aux exigences suivantes :

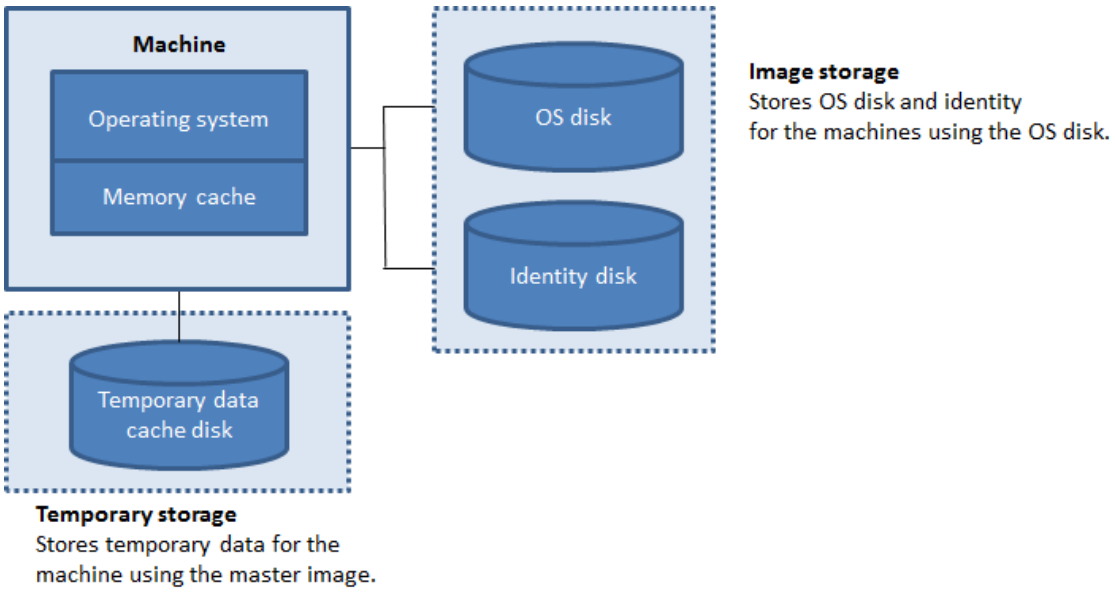
- Utilise une connexion qui spécifie le stockage des données temporaires. Pour de plus amples informations, consultez les articles Connexions et ressources.
- Les VDA doivent avoir au moins la version 7.9 et être installés avec un pilote MCSIO actuel.

  > **Remarque :**
  >
  > 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.

- Pour activer l'attribution de lettres de lecteur pour les caches de disque, les machines virtuelles doivent répondre aux exigences supplémentaires suivantes :
  - Système d'exploitation : Windows
  - Version VDA : 2305 ou ultérieure

Considérations

- Les caches à écriture différée sont disponibles comme cache *Mémoire* et cache *Disque*. Par défaut, leurs valeurs par défaut diffèrent selon le type de connexion. En général, les valeurs par défaut suffisent à la plupart des cas, cependant, tenez compte de l'espace nécessaire pour les :
  - 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.



- La configuration du cache en écriture différée avec uniquement un cache disque et aucun cache mémoire est obsolète. Pour activer la mise en cache des données temporaires, nous vous recommandons de sélectionner 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. Les données temporaires sont initialement écrites dans le cache mémoire. Lorsque le cache mémoire atteint sa limite configurée, les données les plus anciennes sont déplacées vers le cache disque de données temporaire.
- La mémoire cache est prise en compte dans le calcul de la quantité totale de mémoire sur chaque machine. Par conséquent, si vous cochez la case **Taille de la mémoire cache (Mo) (recommandé)**, envisagez d'augmenter la quantité totale de mémoire sur chaque machine.
- La modification de la **taille du cache disque (Go)** par défaut peut affecter les performances. La taille doit correspondre aux besoins des utilisateurs et à la charge de travail placée sur la machine.

  > **Important :**
  >
  > Si le cache disque vient à manquer d'espace, la session de l'utilisateur devient inutilisable.

- Si vous désactivez la case **Taille du cache disque**, aucun disque cache n'est créé. Dans ce cas, spécifiez une valeur de **Mémoire allouée au cache** suffisante pour stocker toutes les données temporaires. Cela est uniquement possible si d'importantes quantités de RAM sont disponibles pour allocation à chaque machine virtuelle.
- Si vous désélectionnez ces deux cases, les données temporaires ne seront 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 les versions antérieures à la version 7.9).

- N'activez pas la mise en cache si vous avez l'intention d'utiliser ce catalogue pour créer des AppDisks.
- Vous ne pouvez pas modifier les valeurs de cache dans un catalogue de machines après sa création.

Utilisation de fichiers CSV pour ajouter des machines en vrac Si vous utilisez l'interface de gestion **Configuration complète**, vous pouvez ajouter des machines en vrac à l'aide de fichiers CSV. Cette fonctionnalité est disponible pour tous les catalogues, à l'exception des catalogues créés via MCS.

Voici un workflow général qui utilise des fichiers CSV pour ajouter des machines en vrac :

1. Sur la page **Machines**, sélectionnez **Ajouter un fichier CSV**. La fenêtre **Ajouter des machines en vrac** s'affiche.
2. Sélectionnez **Télécharger le modèle CSV**.
3. Remplissez le fichier modèle.
4. Faites glisser le fichier ou naviguez jusqu'au fichier pour le télécharger.
5. Sélectionnez **Valider** pour contrôler la validité de votre importation.
6. Sélectionnez **Importer** pour terminer.

Pour plus d'informations sur les considérations relatives aux fichiers CSV, consultez Considérations lors de l'utilisation de fichiers CSV pour ajouter des machines.

Vous pouvez également exporter des machines à partir d'un catalogue sur la même page Machines. Le fichier CSV exporté des machines peut ensuite être utilisé comme modèle lors de l'ajout de machines en masse. Pour exporter des machines :

1. Sur la page **Machines**, sélectionnez **Exporter vers un fichier CSV**. Un fichier CSV contenant une liste des machines est téléchargé.
2. Ouvrez le fichier CSV pour ajouter ou modifier des machines selon vos besoins. Pour ajouter des machines en vrac à l'aide du fichier CSV enregistré, consultez la section précédente, Utilisation de fichiers CSV pour ajouter des machines en vrac.

> **Remarque :**
>
> - Cette fonctionnalité n'est pas disponible pour les catalogues Remote PC Access.
> - L'exportation et l'importation de machines dans des fichiers CSV ne sont prises en charge qu'entre des catalogues du même type.

Configurer les cartes d'interface réseau des machines

La page **NIC** ne s'affiche pas si vous sélectionnez **Remote PC Access** sur la page **Type de machine**.

Si vous prévoyez d'utiliser plusieurs cartes d'interface réseau, 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.

Ajouter des comptes de machines

> **Remarque :**
>
> La page **Comptes de machine** ne s'affiche que lorsque vous sélectionnez **Remote PC Access** sur la page **Type de machine**.

Ajoutez les comptes de machine Active Directory ou les unités organisationnelles (UO). N'utilisez pas de barre oblique (/) dans un nom d'unité d'organisation.

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.

Vous pouvez aussi ajouter des machines en bloc à l'aide de fichiers CSV. Voici un workflow général pour cette procédure :

1. Sur la page **Comptes de machine**, sélectionnez **Ajouter un fichier CSV**. La fenêtre **Ajouter des machines en vrac** s'affiche.
2. Sélectionnez **Télécharger le modèle CSV**.
3. Remplissez le fichier modèle.
4. Faites glisser le fichier ou naviguez jusqu'au fichier pour le télécharger.
5. Sélectionnez **Valider** pour contrôler la validité de votre importation.
6. Sélectionnez **Importer** pour terminer.

Pour plus d'informations sur les considérations relatives aux fichiers CSV, consultez Considérations lors de l'utilisation de fichiers CSV pour ajouter des machines.

Configurer des identités pour les machines du catalogue

> **Remarque :**
>
> - La page **Identités des machines** ne s'affiche que si vous ne sélectionnez pas **Remote PC Access** sur la page **Type de machine** et si vous sélectionnez **Citrix Machine Creation Services (MCS)** sur la page **Gestion des machines**.

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 :

- **Active Directory local** : machines appartenant à une organisation et connectées avec un compte Active Directory appartenant à cette organisation. Elles existent sur site.

  > **Remarque :**
  >
  > Par défaut, le domaine dans lequel réside la ressource (connexion) est sélectionné.

- **Joint à Azure AD** : machines appartenant à une organisation et connectées avec un compte Azure Active Directory appartenant à cette organisation. Elles n'existent que dans le cloud. Pour plus d'informations sur les exigences, les limites et les considérations, consultez la section Joint à Azure Active Directory.

  > **Remarque :**
  >
  > Cette option nécessite que l'image principale réponde aux exigences du système d'exploitation. Pour plus d'informations, consultez la documentation Microsoft sur les machines connectées à Microsoft Entra.

- **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. Consultez la page Configure Microsoft Entra hybrid join.
  > - Cette option nécessite que l'image principale réponde aux exigences du système d'exploitation. Pour plus d'informations, consultez la page Microsoft Entra hybrid joined devices.

- **Non joint au domaine**. Machines qui ne sont jointes à aucun domaine. Pour plus d'informations sur les exigences et les limitations, consultez la section Non joint au domaine.

> **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.
> - Le type d'identité **Non joint au domaine** nécessite la version 1811 ou ultérieure du VDA comme niveau fonctionnel minimum pour le catalogue. Pour le rendre disponible, mettez à jour le niveau fonctionnel minimum.
> - Les types d'identité **Joint à Azure Active Directory** et **Joint à Azure Active Directory Hybride** nécessitent la version 2203 ou ultérieure du VDA comme niveau fonctionnel minimum pour le catalogue. Pour les rendre disponibles, mettez à jour le niveau fonctionnel minimum.

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 des comptes ou cliquer sur **Importer** et spécifier un fichier `.csv` contenant les noms de compte. Le contenu du fichier importé doit utiliser le format suivant : `[ADComputerAccount] ADcomputeraccountname.domain`

Assurez-vous qu'il existe suffisamment de comptes pour toutes les machines que vous ajoutez. L'interface Configuration complète 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 de dénomination, tenez compte des points suivants :

- Le nombre maximum de caractères autorisés est de 15.

- Le schéma de dénomination 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 (-).
- Le nombre de caractères augmente avec l'augmentation du nombre de comptes de machine. Par exemple, si vous créez 1 000 comptes de machine avec le schéma « veryverylong# », le dernier nom de compte créé (veryverylong1000) contient 16 caractères et dépasse le nombre maximum de caractères autorisé.

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.

Ajouter des informations d'identification de 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`.

Sélectionner un jeu de configuration Workspace Environment Management (facultatif)

La page **WEM** ne s'affiche que lorsque vous utilisez l'édition Advanced ou Premium de Citrix DaaS.

Sélectionnez un jeu de configuration Gestion de l'environnement d'espace de travail (WEM) auquel vous souhaitez lier le catalogue. Un jeu de configuration est un conteneur logique utilisé pour organiser un ensemble de configurations WEM. La liaison d'un catalogue à un jeu de configuration vous permet d'utiliser WEM pour offrir la meilleure expérience d'espace de travail possible à vos utilisateurs.

> **Important :**
>
> - Avant de pouvoir lier un catalogue à un jeu de configuration, vous devez configurer le déploiement de votre service WEM. Connectez-vous à Citrix Cloud, puis lancez le service WEM. Pour plus d'informations, consultez la rubrique Découvrez Workspace Environment Management Service.
> - Si vous utilisez déjà WEM, les machines du catalogue que vous êtes sur le point de provisionner peuvent déjà être présentes dans un jeu de configuration. par exemple, via Active Directory. Dans ce cas, nous vous recommandons d'utiliser Active Directory de façon cohérente pour effectuer la configuration et ignorer cette configuration.

Si le jeu de configuration sélectionné ne contient pas de paramètres relatifs à la configuration de base de WEM, l'option suivante apparaît :

- **Appliquer les paramètres de base au jeu de configuration**. Cette option vous permet de commencer rapidement à utiliser WEM en appliquant des paramètres de base au jeu de configuration. Les paramètres de base incluent la protection contre les pics de processeur, la prévention

automatique des pics de processeur et l'optimisation intelligente du processeur. Pour afficher les paramètres de base, cliquez sur *ce lien*. Pour les modifier, utilisez la console WEM.

Mettre à niveau le VDA (facultatif)

> **Important :**
>
> - Pour garantir une mise à niveau fluide, assurez-vous de respecter les prérequis et d'examiner les problèmes connus avant de procéder à la mise à niveau des VDA vers les versions CR ou LTSR CU. Voir Mettre à niveau les VDA à l'aide de l'interface Configuration complète.
> - Lors de la mise à niveau de VDA LTSR vers des versions de mise à jour cumulative (CU) LTSR, assurez-vous que la version des agents de mise à niveau du VDA exécutés sur les VDA est 7.36.0.7 ou ultérieure. Pour plus d'informations, consultez Mettre à niveau les VDA à l'aide de l'interface Configuration complète.

Cette fonctionnalité s'applique aux types de machines suivants :

- Les machines persistantes provisionnées par MCS. Vous les déployez à l'aide de l'option **Citrix Machine Creation Services** sur la page **Gestion des machines** lors de la création du catalogue.
- Les machines qui ne sont pas créées à l'aide de MCS (par exemple, des machines physiques). Vous les déployez à l'aide de l'option **Autre service ou technologie** sur la page **Gestion des machines** lors de la création du catalogue.

Pour plus d'informations sur les deux options, consultez la section Gestion des machines.

Sur la page **Mise à niveau de VDA**, sélectionnez la version de VDA vers laquelle effectuer la mise à niveau. Si cela est spécifié, les VDA du catalogue sur lesquels l'agent de mise à niveau VDA est installé peuvent être mis à niveau vers la version sélectionnée, immédiatement ou à une heure planifiée.

> **Remarque :**
>
> - Cette fonctionnalité prend uniquement en charge la mise à niveau vers le dernier VDA. Le moment auquel vous créez un calendrier de mise à niveau de VDA ou mettez à niveau un VDA détermine la dernière version du VDA.
> - Après avoir configuré les paramètres de mise à niveau du VDA, le champ **Mise à niveau de VDA** peut prendre jusqu'à 15 minutes pour refléter le dernier état. Pour afficher la colonne **Mise à niveau de VDA**, cliquez sur l'icône Colonnes à afficher dans le coin supérieur droit, sélectionnez **Catalogue de machines > Mise à niveau de VDA**, puis cliquez sur **Enregistrer**.

Choisissez la version de VDA adaptée à votre déploiement :

> **Important :**
>
> Vous pouvez basculer entre le VDA CR et le VDA LTSR à condition de passer d'une version antérieure à une version ultérieure. Vous ne pouvez pas passer d'une version ultérieure à une version antérieure, car cela est considéré comme une rétrogradation. Par exemple, vous ne pouvez pas passer de 2212 CR à 2203 LTSR (n'importe quelle CU), mais vous pouvez mettre à niveau de 2112 CR à 2203 LTSR (n'importe quelle CU).

- **Version CR de VDA la plus récente**. Les versions actuelles (CR) offrent les fonctionnalités de virtualisation des applications, des bureaux et des serveurs les plus récentes et les plus innovantes.
- **Version LTSR de VDA la plus récente**. Les versions LTSR sont recommandées pour les environnements de production de grandes entreprises qui préfèrent conserver la même version de base pendant une longue période.

Après la création du catalogue, vous pouvez mettre à niveau les VDA selon vos besoins. Pour plus d'informations, consultez Mettre à niveau les VDA.

Si vous souhaitez activer la mise à niveau des VDA ultérieurement, vous pouvez revenir à cette page en modifiant le catalogue après sa création. Pour plus d'informations, consultez la section Configurer les paramètres de mise à niveau de VDA en modifiant un catalogue.

Vérifier les paramètres

Sur la page **Résumé**, vérifiez les paramètres que vous avez spécifiés. Entrez un nom et une description pour le catalogue. Ces informations apparaissent dans l'interface de gestion Configuration complète.

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

Créer un catalogue de machines MCS à l'aide de commandes PowerShell

Vous pouvez créer un catalogue de machines MCS à l'aide de commandes PowerShell. Pour plus d'informations, consultez :

- SDK et API
- Gérer Citrix DaaS à l'aide des SDK Remote PowerShell
- New-ProvScheme

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 procéder, vous pouvez utiliser des 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 à un disque de cache en écriture différée Pour attribuer une lettre de lecteur au 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. Pour plus d'informations, consultez la page Création d'un catalogue.
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.

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.

```
Invalid property found: <invalid property>. Ensure that the CustomProperties
 parameter supports the property.
```

Considérations importantes relatives à la définition des paramètres ProvScheme

Lorsque vous utilisez MCS pour créer un catalogue, un message d'erreur s'affiche si vous :

- Définissez les paramètres `New-ProvScheme` suivants dans des hyperviseurs non pris en charge lorsque vous créez un catalogue de machines :

Paramètre	Hyperviseur pris en charge
`UseWriteBackCache`	VMware
	Hyper-V
	XenServer
	Azure
	GCP
`DedicatedTenancy`	Azure
	GCP
	AWS
`TenancyType`	Azure
	GCP
	AWS
`UseFullDiskCloneProvisioning`	VMware
	Hyper-V
	XenServer

- Mettez à jour les paramètres `Set-ProvScheme` suivants après avoir créé le catalogue de machines :

- `CleanOnBoot`
- `UseWriteBackCache`
- `DedicatedTenancy`
- `TenancyType`
- `UseFullDiskCloneProvisioning`

Ajouter des SID lors de la création de machines virtuelles

Vous pouvez désormais ajouter le paramètre `ADAccountSid` pour identifier les machines de manière unique 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

Valider la configuration avant de créer un catalogue de machines MCS

Vous pouvez valider les paramètres de configuration avant de créer un catalogue de machines MCS à l'aide du paramètre `-validate` dans la commande `New-ProvScheme`. Après avoir exécuté cette commande PowerShell avec le paramètre, un message d'erreur approprié s'affiche si un paramètre incorrect est utilisé ou si un paramètre est en conflit avec un autre paramètre. Vous pouvez ensuite utiliser le message d'erreur pour résoudre le problème, puis créer le catalogue de machines MCS à l'aide de PowerShell. Actuellement, cette fonctionnalité est applicable aux environnements de virtualisation Azure, GCP et VMware.

> **Remarque :**
>
> Lors de la validation, vous ne devez pas créer de catalogue de machines MCS. Vous devez utiliser le résultat de la commande pour corriger les erreurs, puis créer le catalogue. Par conséquent, lors de l'exécution de la commande `New-ProvScheme`, utilisez un faux nom de pool d'identités.

Pour valider la configuration, procédez comme suit :

1. Ouvrez une fenêtre PowerShell depuis l'hôte Delivery Controller.

2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Exécutez la commande `New-ProvScheme` et utilisez le paramètre `-validate`. Fournissez un faux nom de pool d'identités pour que la commande fonctionne. Par exemple,

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg" -
    IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
    MasterImageVM "XDHyp:\HostingUnits\vSanRg\Windows19MasterImage.
    vm\Citrix_XD_NonMachineProfileWin19Machines.snapshot" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vSanRg\VM Network.network" }
  -ProvisioningSchemeName "MachineProfileW10Machines"  -Scope @()
-VMCpuCount 2  -VM
MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-
    Win11-tpm-BL-TEMPLATE.template" -TenancyType Shared  -
    FunctionalLevel "L7_20" -Validate
$result.TerminatingError | Format-List -Property *
<!--NeedCopy-->
```

Message d'erreur :

```
ErrorData    : {
 [[ValidationFailureCount, xxx], [InvalidMemoryValue, The memory
    size provided 6143 must be a multiple of 4 MB and must be
    greater than or equal to 4 MB.], [InconsistentGuestOsSetting,
    The GuestOs setting - windows9_64Guest of the selected machine
     profile does not match with the setting -
    windows2019srv_64Guest of master image. Please select a
    machine profile that matches the GuestOs setting of the master
     image.], [InconsistentVtpmSetting, The vTPM setting of the
    selected machine profile does not match with the selected
    master image. Please select a machine profile that matches the
     vTPM setting of the master image.], [
    InconsistentFirmwareSetting, The firmware setting - efi of the
     selected machine profile does not match with the setting -
    bios of master image. Please select a machine profile that
    matches the firmware setting of the master image ErrorId
    : ValidationFailure
ErrorMessage : ValidationFailure
Operation    : ValidatingInputs
<!--NeedCopy-->
```

4. Après avoir validé les paramètres de configuration, vous pouvez créer un catalogue de machines MCS avec un nom de pool d'identités réel et des paramètres corrects.

Autres ressources

Pour plus d'informations sur la création de catalogues d'hyperviseurs spécifiques, consultez :

- Créer un catalogue AWS
- 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
- Créer un catalogue XenServer

S'il s'agit du premier catalogue créé, vous êtes guidé dans la création d'un groupe de mise à disposition.

Pour passer en revue l'ensemble du processus de configuration, reportez-vous à la section Planifier et créer un déploiement.

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

- Gestion des images Citrix Virtual Apps and Desktops
- Créer et gérer des connexions et des ressources
- Créer des catalogues joints à des identités de machines
- Gérer des catalogues de machines

Créer un catalogue AWS

May 17, 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.

Location AWS

AWS propose les options de location suivantes : location partagée (type par défaut) et location dédiée. La location partagée signifie que plusieurs instances Amazon EC2 provenant de clients différents peuvent résider sur le même matériel physique. La location dédiée signifie que 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 dédiés AWS à l'aide de l'interface Configuration complète ou de PowerShell.

Configuration requise pour le provisioning des hôtes AWS

- 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.
- Activation du **placement automatique**.

Configurez la location d'hôte dédié AWS à l'aide de l'interface Configuration complète

Lorsque vous utilisez MCS pour créer un catalogue pour provisionner des machines dans AWS, la page **Création d'un catalogue de machines > Sécurité** présente les options suivantes :

- **Utiliser le matériel partagé**. Ce paramètre convient à la plupart des déploiements. Plusieurs clients partagent le matériel même s'ils n'interagissent pas les uns avec les autres. L'utilisation de matériel partagé est l'option la moins coûteuse pour exécuter vos instances Amazon EC2.

- **Utiliser un hôte dédié**. 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.
- **Utiliser une instance dédiée**. Ce paramètre est plus approprié aux déploiements nécessitant des exigences spécifiques en matière de sécurité et conformité. Avec une instance dédiée, vous bénéficiez toujours des avantages d'un hôte séparé des autres clients AWS, mais vous ne payez pas pour la totalité de l'hôte. Vous n'avez pas besoin de vous soucier de la capacité de l'hôte, mais vous êtes facturé à un taux plus élevé pour les instances.

  Ce paramètre convient aux déploiements avec des restrictions de licence ou exigences de sécurité qui nécessitent d'utiliser un hôte dédié. Avec un hôte dédié, vous possédez la totalité d'un hôte physique et vous êtes facturé sur une base horaire. Posséder cet hôte vous permet de faire tourner autant d'instances EC2 que cet hôte le permet, sans frais supplémentaires.

> **Remarque :**
>
> Vous pouvez supprimer les disques d'identité de préparation disponibles si aucune tâche de création de catalogue ou de mise à jour d'image n'est en cours.

Configurer les locataires d'hôtes dédiés AWS à l'aide de PowerShell

Vous pouvez également provisionner des hôtes dédiés AWS via PowerShell. Utilisez l'applet de commande `New-ProvScheme` en définissant le paramètre `TenancyType` sur `Host`.

Capturer les propriétés d'instance AWS

Lorsque vous créez un catalogue de machines à provisionner à l'aide de MCS (Machine Creation Services) dans AWS, vous sélectionnez une AMI (Amazon Machine Image) pour représenter l'image principale de ce catalogue. À partir de cette AMI, MCS utilise un instantané du disque.

> **Conseil :**
>
> Pour utiliser la capture de propriétés d'instance AWS, une machine virtuelle doit être associée à l'AMI.

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 d'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`. Pour appliquer correctement les balises et créer un catalogue AWS avec balisage des ressources opérationnelles, ne supprimez pas l'instance EC2 qui a été utilisée pour créer l'image AMI.

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 au New-ProvScheme.

> **Remarque :**
>
> `AwsCaptureInstanceProperties` est obsolète. Nous vous recommandons plutôt d'utiliser des profils de machine pour spécifier les propriétés des machines virtuelles.

Baliser une ressource opérationnelle

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 :**

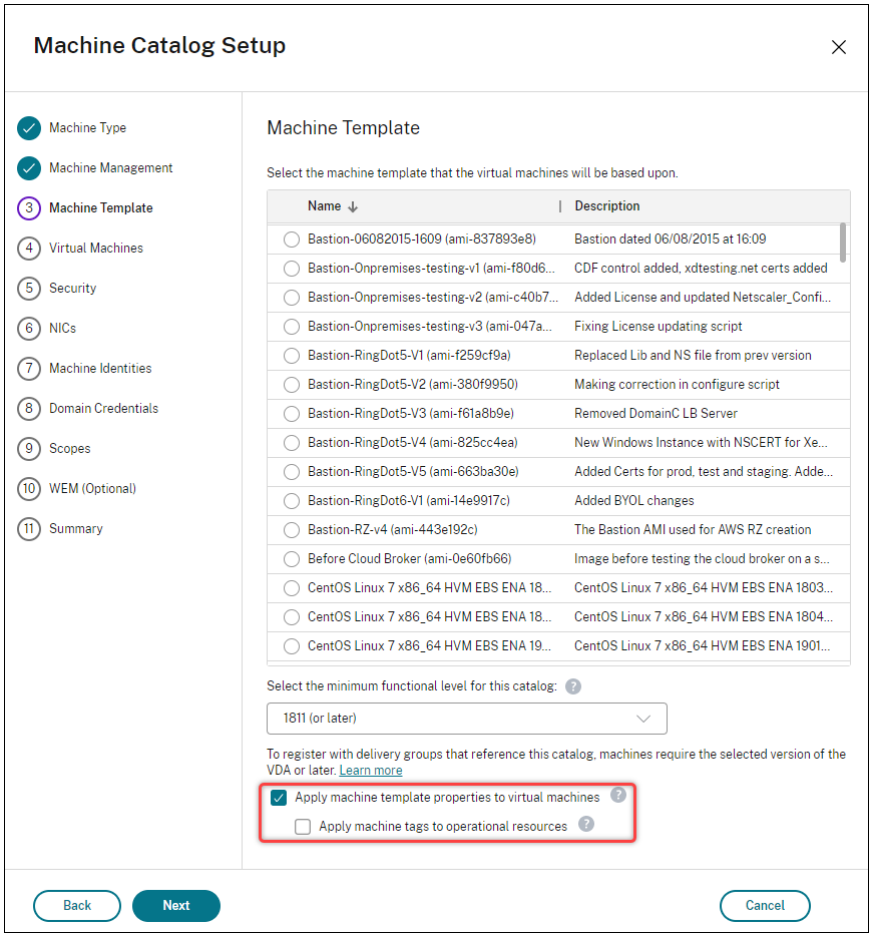
> La création de catalogues en capturant une propriété d'instance et un modèle de lancement est nécessaire pour utiliser le balisage des ressources opérationnelles.

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

Appliquer les propriétés d'instance AWS et baliser les ressources opérationnelles dans l'interface Configuration complète

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. Vous disposez des deux options suivantes :



- **Appliquer les propriétés du modèle de machine aux machines virtuelles**
  - Contrôle si le rôle IAM et les propriétés de balise associées au modèle de machine sélectionné doivent être appliqués aux machines virtuelles de ce catalogue.
- **Appliquer balises de machine aux ressources opérationnelles**
  - Contrôle si des balises de machine doivent être appliquées à chaque élément créé dans votre environnement AWS afin de faciliter le provisioning des machines. Les ressources opérationnelles sont créées en tant que sous-produits de la création de catalogue. Elles incluent des ressources temporaires et persistantes, telles que les instances de VM de préparation et les images de machine d'Amazon.

Appliquer une balise à une ressource opérationnelle à l'aide de PowerShell

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 appliquer une balise à une ressource de VM 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
>
```

Créer un catalogue de machines basé sur un profil de machine à l'aide de PowerShell

Vous pouvez utiliser un profil de machine pour capturer les propriétés matérielles d'une instance EC2 (VM) ou une version de Launch Template 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, les options d'UC, le type de locataire, la capacité de mise en veille prolongée et d'autres configurations AWS prises en charge.

Vous pouvez utiliser une instance AWS EC2 (VM) ou une version d'AWS Launch Template comme entrée de profil de machine.

> **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.

- Si aucun profil de machine n'est spécifié, vous devez indiquer explicitement les valeurs des propriétés suivantes :
  - Groupe de sécurité
  - Interface réseau élastique 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 :

- 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,

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain abcdf -NamingSchemeType Numeric
<!--NeedCopy-->
```

4. Exécutez la commande New-ProvScheme. Par exemple :

```
New-ProvScheme -ProvisioningSchemeName demet-test-1
-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
-CleanOnBoot
-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
    demet-ami.0 (ami-0ca813xxxxxx061ef).template'
-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east
    -1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).
    vm'
<!--NeedCopy-->
```

5. Terminez la création du catalogue.

Mettre à jour le profil de machine

Pour mettre à jour le profil de machine sur un catalogue initialement provisionné avec un profil de machine, procédez comme suit : Vous pouvez également modifier le type de location et la capacité de mise en veille prolongée de la source du profil de machine lors de la modification d'un catalogue de machines MCS.

1. Exécutez la commande `Set-ProvScheme`. Par exemple,

```
Set-ProvScheme `
-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 une version de modèle de lancement à l'aide de PowerShell

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 :

```
1 XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
      ls | Select FullPath
2 <!--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" `
-ZoneUid "xxxxxxxx" `
<!--NeedCopy-->
```

5. Créez un schéma de provisioning avec une version de modèle de lancement comme entrée de profil de machine. Par exemple :

```
New-ProvScheme `
-ProvisioningSchemeName "MPLT1" `
-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
   persistent-vda-win2022 (ami-0axxxxxxxxxx).template" `
-CleanOnBoot `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-01xxxxx).launchtemplate\lt-01xxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```

6. Enregistrez le schéma de provisioning en tant que catalogue de brokers. Par exemple :

```
New-BrokerCatalog -Name "MPLT1" `
-AllocationType Random `
-Description "Machine profile catalog" `
-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
-ProvisioningType Mcs `
-SessionSupport MultiSession `
-PersistUserChanges Discard
<!--NeedCopy-->
```

7. Terminez la création du catalogue.

Mettre à jour la source du 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. 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 :

```
 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-->
```

Crypter le système d'exploitation et les disques d'identité

Vous pouvez créer un catalogue persistant et non persistant de machines virtuelles avec des clés AWS KMS (clé gérée par le client et clé gérée par AWS) pouvant être utilisées pour crypter le disque du système d'exploitation et le disque d'identité (ID).

- Les clés gérées par AWS sont automatiquement renouvelées chaque année.
- Le renouvellement automatique des clés gérées par le client est facultatif et ces clés peuvent être gérées manuellement.

Pour en savoir plus sur les clés KMS, consultez les documents AWS suivants :

- Concepts d'AWS KMS
- Fonctionnement du renouvellement automatique des clés

Pour crypter le disque du système d'exploitation et le disque d'identité, configurez l'une des options suivantes :

- Utiliser une image principale cryptée (par exemple, une AMI créée à partir d'une instance ou d'un instantané contenant un volume racine EBS crypté avec une clé KMS)
- Utiliser une source de profil de machine (machine virtuelle ou modèle de lancement) contenant un volume racine EBS crypté.

Limitations

Tenez compte des limitations suivantes :

- Actuellement, MCS ne prend en charge qu'un seul disque sur l'AMI de l'image principale.

- Vous ne pouvez pas crypter directement des volumes EBS ou des instantanés non cryptés existants, ni modifier la clé KMS d'un volume crypté existant. Pour cela, vous devez procéder comme suit :

    1. Créez un instantané de ce volume.
    2. Créez un volume à partir de cet instantané
    3. Cryptez le nouveau volume.

Consultez les documents AWS suivants :

- Crypter des ressources non cryptées
- Limites du cryptage automatique ou par défaut des volumes EBS : Chiffrer automatiquement les volumes Amazon EBS existants et nouvellement créés.

Créer un catalogue avec cryptage de disque

Vous pouvez créer un catalogue de machines MCS avec cryptage de disque en utilisant :

- L'image principale
- Le profil de la machine

Points à prendre en compte lors de l'utilisation d'une entrée de profil de machine :

- La clé KMS de l'entrée de profil de machine a priorité sur la clé KMS de l'image principale.
- Si aucune entrée de profil de machine n'est spécifiée, la clé KMS de l'AMI principale est utilisée pour crypter les disques des machines virtuelles du catalogue.
- Si des mappages de périphériques en bloc sont présents dans le profil de machine, les périphériques en bloc présents dans le modèle d'image principale (AMI) et dans le profil de machine doivent correspondre. Par exemple, si l'AMI d'un périphérique est définie sur `/dev/sda1`, un périphérique doit également être défini sur le profil de machine `/dev/sda1`.
- S'il n'y a pas de clé dans la source du profil de machine et que l'image principale n'est pas cryptée, les disques des machines virtuelles du catalogue ne sont pas cryptés.
- Lorsque l'image principale est cryptée, une machine virtuelle source de profil de machine ou un modèle de lancement doit avoir un volume racine crypté pour être considéré comme une entrée valide.

Modifier un catalogue existant

Vous pouvez modifier un catalogue existant à l'aide de la commande PowerShell `Set-ProvScheme` de façon à obtenir :

- Une entrée de profil de machine dont le volume contient une nouvelle clé KMS.

- Un modèle d'image principale AMI crypté avec une nouvelle clé KMS.

Remarques importantes :

- Les volumes des nouvelles machines virtuelles ajoutées au catalogue sont cryptés avec la nouvelle clé KMS.
- Pour mettre à jour les paramètres de cryptage lorsqu'un profil de machine existe déjà, exécutez `Set-ProvScheme` avec un nouveau profil de machine.
- Vous ne pouvez pas modifier un catalogue existant pour transformer les volumes cryptés en volumes non cryptés.
  Vous ne pouvez pas mettre à jour une image pour remplacer une AMI principale cryptée en AMI principale non cryptée.

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.

Filtrer les instances de machines virtuelles à l'aide de PowerShell

Une instance de machine virtuelle AWS que vous utilisez comme machine virtuelle de profil de machine doit être compatible pour que le catalogue de machines soit créé et fonctionne correctement. Pour répertorier les instances de machines virtuelles AWS pouvant être utilisées comme machines virtuelles 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 :


```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ContinuationToken "ami-07xxxxxxxxx" -
    MaxRecords 10
<!--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 :

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -ContainName ' apollo '
     | select Name
<!--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
    -015xxxxxxxx" -Warn $true).AdditionalData
<!--NeedCopy-->
```

Autres ressources

- S'il s'agit du premier catalogue créé, vous êtes guidé dans la création d'un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, reportez-vous à la section Planifier et créer un déploiement.
- Pour gérer les catalogues, consultez Gérer les catalogues de machines et Gérer un catalogue AWS.

Informations supplémentaires

- Créer et gérer des connexions et des ressources
- Connexion à AWS
- Créer des catalogues de machines

Créer un catalogue Google Cloud Platform

May 22, 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).

Activer la sélection de zone

Citrix DaaS 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

Réserver 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.

Créer 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

> **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.

Vous pouvez créer un catalogue de machines de deux manières :

- Interface Configuration complète
- PowerShell. Reportez-vous à la section Gérer Citrix DaaS à l'aide des SDK Remote PowerShell. Pour plus d'informations sur la mise en œuvre de fonctionnalités spécifiques à l'aide de PowerShell, consulter Utiliser PowerShell

Créez un catalogue de machines à l'aide de l'interface Configuration complète

Suivez les instructions de la section Créer des catalogues de machines. Les informations suivantes sont uniques aux catalogues de Google Cloud.

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez **Créer un catalogue de machines** dans la barre d'actions.
3. Sur la page **Type de machine**, sélectionnez **OS multi-session**, puis sélectionnez **Suivant**. Citrix DaaS prend également en charge l'OS à session unique.
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.

6. Sur la page **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 en savoir plus sur les options de stockage Google Cloud, consultez Options de stockage.

7. Sur la page **Machines virtuelles**, spécifiez le nombre de machines virtuelles que vous souhaitez créer, affichez la spécification détaillée des machines virtuelles, sélectionnez le type de machine Google Cloud, 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 **Paramètres du disque**, vous pouvez configurer les paramètres suivants :
   - Choisissez d'activer ou non le cache en écriture différée. 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 :
       * Disque persistant standard
       * Disque persistant équilibré
       * Disque persistant SSD

       Pour en savoir plus sur les options de stockage Google Cloud, consultez Options de stockage.
     - 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 ne persiste pas pour les machines virtuelles provisionnées. Le disque est supprimé pendant les cycles d'alimentation et toutes les données redirigées vers le disque seront perdues.
       * **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.
   - Lorsque l'optimisation du stockage MCS (E/S MCS) est activée, vous pouvez choisir de conserver ou non les disques système pour les VDA pendant les cycles d'alimentation. Pour plus d'informations, consultez Activation des mises à jour de l'optimisation du stockage MCS.

- Choisissez d'utiliser ou non votre propre clé pour protéger le contenu du disque. Pour utiliser cette fonctionnalité, vous devez d'abord créer vos propres clés de chiffrement gérées par le client (CMEK). Pour plus d'informations, consultez la section Utilisation de clés de chiffrement gérées par le client (CMEK).

  > **Remarque :**
  >
  > Elle est disponible uniquement dans l'interface **Gérer > Configuration complète**.

  Après avoir créé les clés, vous pouvez sélectionner l'une de ces clés dans la liste. Vous ne pouvez pas modifier la clé après avoir créé le catalogue. Google Cloud ne prend pas en charge la rotation des clés sur des images ou des disques persistants existants. Par conséquent, une fois que vous avez provisionné un catalogue, le catalogue est lié à une version spécifique de la clé. Si cette clé est désactivée ou détruite, les instances et les disques chiffrés avec cette clé deviennent inutilisables jusqu'à ce qu'elle soit réactivée ou restaurée.

9. Sur la page **Identités des machines**, sélectionnez un compte Active Directory, puis **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.
10. 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.
11. Sur la page **Étendues**, sélectionnez les étendues pour le catalogue de machines, puis sélectionnez **Suivant**.
    - Vous pouvez sélectionner des étendues facultatives ou **Étendue personnalisée** pour personnaliser les étendues selon vos besoins.
12. Sur la page **Résumé**, vérifiez les informations, spécifiez un nom pour le catalogue, puis sélectionnez **Terminer**.

> **Remarque :**
>
> Le nom du catalogue peut contenir entre 1 et 39 caractères, et ne peut pas contenir uniquement des espaces ou les caractères `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

La création du catalogue de machines peut prendre du temps. Une fois terminé, le catalogue est répertorié. Vous pouvez vérifier que les machines sont créées sur les groupes de nœuds cibles dans la console Google Cloud.

Importer des machines Google Cloud créées manuellement

Grâce à cette fonctionnalité, vous pouvez :

- Importer des machines avec OS multi-session Google Cloud créées manuellement dans un catalogue Citrix DaaS.
- Supprimer des machines avec OS multi-session Google Cloud créées manuellement à partir d'un catalogue Citrix DaaS.
- Gérer l'alimentation des machines Google Cloud avec OS multi-session à l'aide des fonctionnalités de gestion de l'alimentation Citrix DaaS. Par exemple, définissez un programme de redémarrage pour ces machines.

Cette fonctionnalité ne nécessite aucune modification du workflow de provisioning Citrix DaaS existant, ni la suppression de toute fonctionnalité existante.

Nous vous recommandons d'utiliser MCS (Machine Creation Services) pour provisionner des machines dans l'interface Configuration complète de Citrix DaaS 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 :

- 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. Consultez la section Nouvelles autorisations requises.
- 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. Consultez la section Règles de pare-feu.

Pour plus d'informations sur la configuration d'un VPC partagé, consultez la section Configurer le VPC partagé.

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 DaaS. 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 :

- **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.
- **compute.networks.list** - Cette autorisation est obligatoire. Elle permet à MCS d'identifier les réseaux VPC partagés disponibles pour le compte de service.
- **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.
- **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 d'affecter les autorisations `compute.subnetworks.list` et `compute.subnetworks.use` au compte de service.

- Autorisation au niveau du sous-réseau :
  - Permet l'accès à des sous-réseaux spécifiques dans le VPC partagé.
  - Comme les autorisations `compute.subnetworks.list` et `compute.subnetworks.use` sont inhérentes à l'affectation au niveau du sous-réseau, vous n'avez pas besoin de les affecter 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 section Administrateurs de projets de service.

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."
```

Configurer le VPC partagé

Avant d'ajouter le VPC partagé en tant que connexion hôte dans l'interface Configuration complète de Citrix DaaS, 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 un compte de service au rôle IAM du projet hôte.
3. Ajoutez le compte de service Cloud Build au 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
- Un modèle plus restreint utilisant un *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'identification de votre projet en accédant à **Aperçu du Cloud > Tableau de bord** dans la console Google Cloud. L'identifiant et le numéro du projet sont affichés sur la carte d'information du projet du tableau de bord du projet :

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 (une pour l'entrée, une pour la sortie) 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 ces étapes pour créer une autre règle. Pour **Sens du trafic**, sélectionnez **Sortie**.

Utiliser des 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 DaaS doit disposer des autorisations correctes dans le projet où la clé est stockée. Consultez la section Attribuer des autorisations au compte Citrix DaaS. 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 DaaS

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 KMS au niveau du projet L'une des options consiste à fournir au compte Citrix DaaS 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 DaaS. Cela vous permet de parcourir les clés régionales du projet concerné dans l'inventaire.

Autorisations KMS 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 un compte Citrix DaaS à un trousseau de clés ou à une clé que vous utilisez pour le provisioning de catalogue.

> **Conseil :**
>
> Avec cette option, vous ne pouvez pas parcourir les clés régionales de votre projet dans l'inventaire car le compte Citrix DaaS 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 ID `cryptoKeyId` dans les propriétés `ProvScheme` personnalisées, décrites ci-dessous. Consultez la section Créer un catalogue avec CMEK à l'aide de propriétés personnalisées.

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 :

```
1 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).
2 We're aware that this can make things untidy, but we have no immediate
    plans to change this.
3 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 DaaS 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 DaaS 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.

Utiliser PowerShell

Cette section explique comment effectuer les tâches suivantes 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 avec CMEK à l'aide de propriétés personnalisées
- 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
- Créer un catalogue avec une 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, exécutez la commande PowerShell `New-ProvScheme CustomProperties`.

> **Conseil :**
>
> Utilisez le paramètre PowerShell `New-ProvScheme CustomProperties` 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 exem-

> ple, 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 écriture différée 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.

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-->
```

> **Remarque :**
>
> Cet exemple s'applique uniquement à Azure. Les propriétés sont différentes dans l'environnement GCP.

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 écriture différée n'est pas supprimé lorsque l'administrateur Citrix DaaS arrête la machine à l'aide de l'interface de gestion.

Lorsque la propriété `PersistWBC` est définie sur **false**, le disque de cache en écriture différée est supprimé lorsque l'administrateur Citrix DaaS 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 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" }
```



```
9
10 -ProvisioningSchemeName "BV-WBC1-CAT1"
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
      folder\Standard_D2s_v3.serviceoffering"
12 -UseWriteBackCache
13 -WriteBackCacheDiskSize 127
14 -WriteBackCacheMemorySize 256
15 <!--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 :

```
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="Resource<!--NeedCopy-->
5 ``````<!--NeedCopy-->
6 ````````Groups" Value="benvaldev5RG3" />
7 <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
     />
8 </CustomProperties>
9 <!--NeedCopy-->
```

Pour activer cette fonctionnalité, définissez la propriété personnalisée `PersistOSDisk` sur **true**. Par exemple :

```
1 New-ProvScheme
2 -CleanOnBoot
3 -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>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
     GoldImages.resourcegroup\W10MCSIO-01
     _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -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 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 :

```
'<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="<
       yourCryptoKeyId>" />
</CustomProperties>'
<!--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 :

```
'<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"/>.
```

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 `CryptoKeyId`, 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.

Mettre à jour un catalogue de machines avec un profil de machine comme modèle d'instance

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/.

Créer un catalogue avec une 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 protégée d'une instance de machine virtuelle. Vous pouvez ensuite utiliser cette instance de machine virtuelle comme entrée de profil de machine.

Créer un catalogue de machines MCS avec une machine virtuelle protégée

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.

Mettre à jour un 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 l'interface Configuration complète 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 l'interface Configuration complète, consultez Créer un catalogue de machines à l'aide de l'interface Configuration complète.

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, vous êtes guidé dans la création d'un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, reportez-vous à la section Planifier et créer un déploiement.
- 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

May 17, 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 :

- Interface Configuration complète
- Commandes PowerShell

Créez un catalogue de machines à l'aide de l'interface Configuration complète

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 :

```
1 New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False -
     MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
     BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
     Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
     -4578-bc07-bcf2a82d1463"
2 New-BrokerMachine -CatalogUid 3 -HostedMachineId "c10n1" -
     HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
     -1-5-21-2589939477-3963209805-1860259709-1121"
3 <!--NeedCopy-->
```

Autres ressources

- S'il s'agit du premier catalogue créé, vous êtes guidé dans la création d'un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, reportez-vous à la section Planifier et créer un déploiement.
- 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 13, 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 :

- Interface Configuration complète.
- PowerShell. Reportez-vous à la section Gérer Citrix DaaS à l'aide des SDK Remote PowerShell. Pour plus d'informations sur la mise en œuvre de fonctionnalités spécifiques à l'aide de PowerShell, consultez Utiliser PowerShell.

Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans l'interface Configuration complète

Ces informations étayent les instructions disponibles dans la section Créer des catalogues de machines.

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.

> **Remarque :**
>
> - L'utilisation d'un disque non géré pour provisionner une machine virtuelle est obsolète.
> - 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 :

1. 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.
2. Sur la page **Image**, sélectionnez l'image que vous souhaitez utiliser comme image principale pour toutes les machines du catalogue. L'assistant **Sélectionner une image** s'affiche. Pour sélectionner une image, procédez comme suit :

   a) (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.
   b) Sélectionnez un groupe de ressources.
   c) Accédez au disque géré Azure, à Azure Compute Gallery ou à la version d'image Azure.

   Lorsque vous sélectionnez une image, tenez compte des points suivants :

   - Vérifiez qu'un Citrix VDA est installé sur l'image.
   - Si vous sélectionnez un disque rattaché à une VM, vous devez arrêter la VM 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.
   > - 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.
> - 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.

Choisissez si vous souhaitez que les machines virtuelles du catalogue héritent des configurations d'un profil de machine. Par défaut, la case **Utiliser un profil de machine (obligatoire pour Azure Active Directory)** est 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.

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

> **Remarque :**
>
> - Lorsque vous sélectionnez une image principale pour les catalogues de machines dans Azure, le profil de machine est filtré en fonction de l'image principale que vous avez sélectionnée. Par exemple, le profil de la machine est filtré en fonction du système d'exploitation Windows, du type de sécurité, de la prise en charge de la mise en veille prolongée et de l'identifiant du jeu de chiffrement de disque de l'image principale.
> - 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. Pour plus d'informations sur le lancement fiable Azure, consultez https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.

Validez la spécification du modèle ARM pour vous assurer qu'elle peut être utilisée comme profil de machine pour créer un catalogue de machines. Pour plus d'informations sur la création d'une spécification de modèle Azure, voir Créer une spécification de modèle Azure.

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>`

  Par exemple :

```
1  Test-ProvInventoryItem -HostingUnitName "we-vdi0101-d-vnet" -
       InventoryPath machineprofile.folder/vdi01-d-rg.
       resourcegroup/VDD-templ-spec.templatespec/1.5.
       templatespecversion
2  <!--NeedCopy-->
```

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**, 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 Provisionner des machines virtuelles sur des 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.

3. 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, tenez compte des 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 :

   - Introduction to Azure Storage

- Stockage Premium Azure : Design for high performance
- Azure 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.
- 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.

Consultez les pages suivantes :

- Vérifier la licence Windows
- Configurer la licence Linux

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 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 Azure Compute Gallery lors de la création de catalogues de machines non persistants volumineux, car cela permet de réinitialiser plus rapide-

ment 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.

Pour plus d'informations sur Azure Compute Gallery, consultez la section Azure Compute Gallery.

4. Sur la page **Machines virtuelles**, indiquez le nombre de machines virtuelles à créer et leur taille. Après la création du catalogue, vous pouvez modifier la taille de machine en modifiant le catalogue.
5. 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.
6. 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.

- Choisissez si vous souhaitez crypter les données sur les machines de ce catalogue et quelle clé de cryptage utiliser. Le cryptage côté serveur à l'aide d'une clé gérée par le client (CMK)

vous permet de gérer le cryptage au niveau du disque géré et de protéger les données sur les machines du catalogue. Les paramètres par défaut sont hérités du profil de la machine ou de l'image principale, le profil étant prioritaire :

- Si vous utilisez un *profil de machine* avec une *CMK*, l'option **Utiliser la clé suivante pour chiffrer les données sur chaque machine** est sélectionnée automatiquement et utilise par défaut la clé du *profil de machine*.
- Si vous utilisez un *profil de machine* avec une clé gérée par la plate-forme (PMK) et que l'*image principale* est cryptée avec une *CMK*, l'option **Utiliser la clé suivante pour chiffrer les données sur chaque machine** est sélectionnée automatiquement et la valeur par défaut est la clé de l'image principale.
- Si vous n'utilisez *pas* de *profil de machine* et que l'*image principale* est cryptée avec une *CMK*, l'option **Utiliser la clé suivante pour chiffrer les données sur chaque machine** est sélectionnée automatiquement et utilise par défaut la clé de l'*image principale*.

Pour plus d'informations, consultez Chiffrement Azure côté serveur.

7. 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**.

   > **Remarque :**
   >
   > 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.

8. 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 :

   a) Dans le champ **Type d'identité**, sélectionnez **Joint à Azure Active Directory**. L'option **Groupe de sécurité Azure AD (facultatif)** s'affiche.
   b) Cliquez sur **Groupe de sécurité Azure AD : Créer un nouveau**.
   c) Entrez un nom de groupe, puis cliquez sur **Créer**.

d) 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.
e) Pour ajouter le groupe de sécurité à un groupe de sécurité attribué, sélectionnez **Rejoindre un groupe de sécurité attribué en tant que membre**, puis cliquez sur **Sélectionner un groupe** pour choisir un groupe à rejoindre.
f) Entrez le schéma de dénomination des comptes de machines virtuelles.

Après la création du catalogue, Citrix DaaS 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 DaaS 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.

> **Remarque :**
>
> Pour renommer le groupe de sécurité Azure AD après la création du catalogue, modifiez le catalogue et accédez à l'option **Groupe de sécurité Azure AD** dans le menu de navigation de gauche. Les noms des groupes de sécurité Azure AD ne doivent pas contenir les caractères suivants : `@ "\ / ; : # . * ? = < > | [ ] ( )'`.

- 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.

Créer une spécification de modèle Azure

Vous pouvez créer une spécification de modèle Azure dans le portail Azure et l'utiliser dans l'interface Configuration complète et les 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 l'interface Configuration complète ou les commandes PowerShell.

- Utilisation de l'interface **Configuration complète** : consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans l'interface Configuration complète.
- Pour PowerShell : consultez Utiliser une spécification de modèle lors de la création ou de la mise à jour d'un catalogue à l'aide de PowerShell

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 y parvenir à l'aide de l'interface Configuration complète ou de 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 dans l'interface Configuration complète

Lors de la création d'un catalogue de machines, vous pouvez spécifier des zones de disponibilité dans lesquelles vous souhaitez provisionner des machines. Sur la page **Machines virtuelles**, sélectionnez une ou plusieurs zones de disponibilité dans lesquelles vous souhaitez créer des machines.

Il existe deux raisons pour lesquelles aucune zone de disponibilité n'est proposée : la région n'a pas de zones de disponibilité ou la taille de machine sélectionnée n'est pas disponible.

Pour plus d'informations sur la configuration à l'aide d'une commande PowerShell, consultez la section Configurer des zones de disponibilité à l'aide de PowerShell.

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, consultez la section 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 Azure Compute Gallery. Pour plus d'informations, consultez la rubrique Galerie d'images partagées Azure.

Stocker 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 :

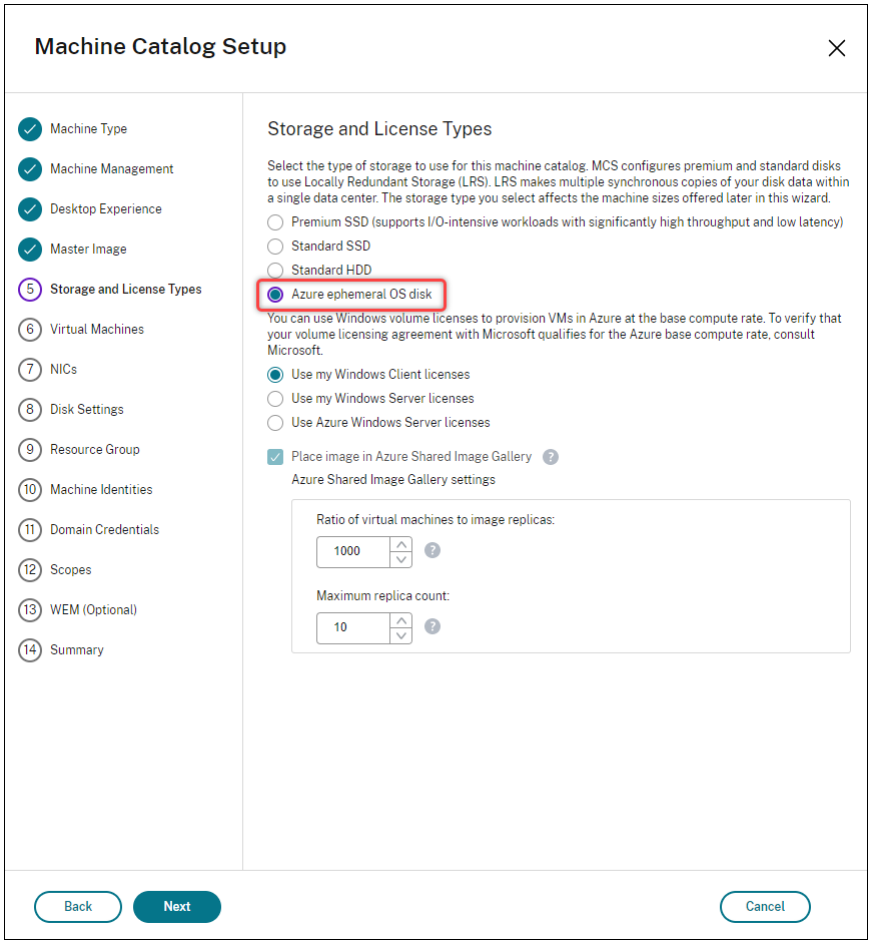
- Un disque éphémère est stocké soit sur le disque cache de la machine virtuelle, soit sur le disque temporaire (ressource) de la machine virtuelle. Le disque de cache est préféré au disque temporaire, sauf si le disque de cache n'est pas suffisamment grand pour le contenu du disque d'OS.
- Pour les 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.

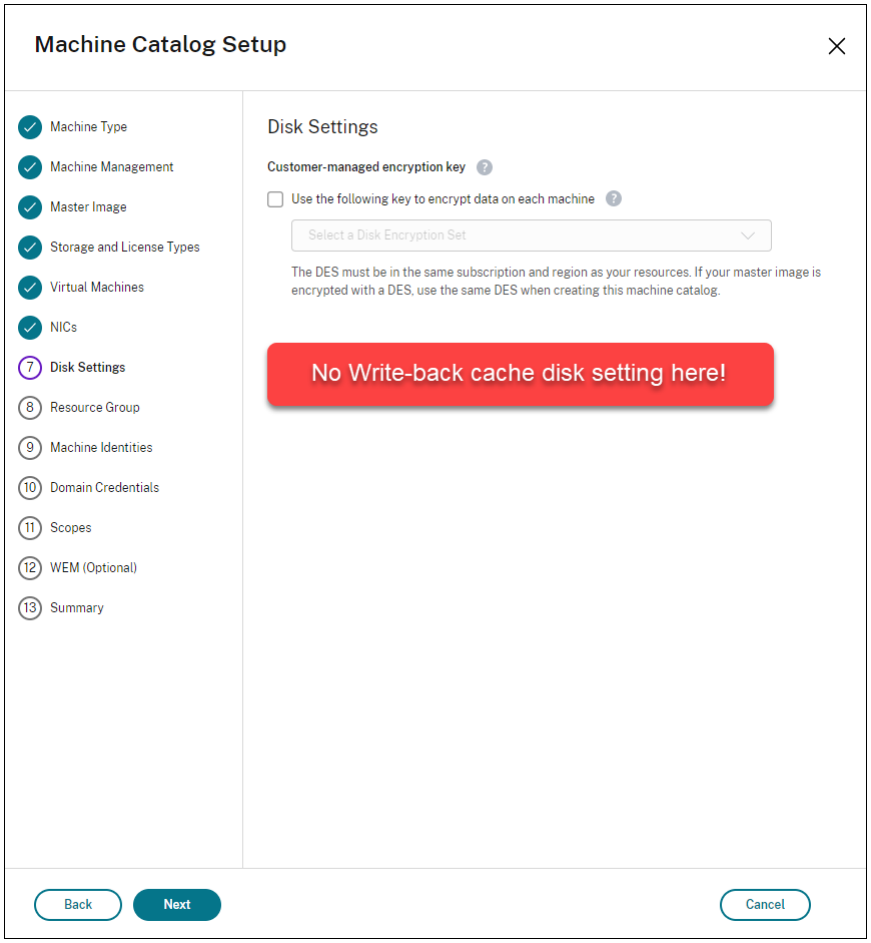
Optimisation du stockage MCS (Machine Creation Services) (E/S de MCS) et du disque d'OS éphémère

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.
- Dans l'assistant **Création d'un catalogue de machines**, si vous sélectionnez **Disque d'OS éphémère Azure** sur la page **Types de stockage et de licence**, vous ne voyez pas l'option pour les paramètres de disque de cache en écriture différée sur la page **Paramètres du disque**.





- Les paramètres PowerShell (`UseWriteBackCache` et `UseEphemeralOsDisk`) définis sur **true** dans `New-ProvScheme` ou `Set-ProvScheme` échouent avec un message d'erreur approprié.
- 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 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. Azure Compute 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 Image Gallery : chaque image d'une galerie Azure Compute Gallery peut avoir plusieurs versions et chacune peut avoir plusieurs réplicas dans différentes régions. Chaque réplica est une copie complète de l'image publiée. Citrix DaaS crée une version d'image Standard_LRS (version 1.0.0) pour chaque image avec le nombre approprié de réplicas dans la région du catalogue, en fonction du nombre de machines dans le catalogue, du ratio de réplica configuré et du maximum de réplicas configuré.

> **Remarque :**
>
> La fonctionnalité Azure Compute 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 des galeries d'images partagées.

Accédez aux images depuis 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. Ces images apparaissent dans la liste d'images de la page **Image** de l'assistant Création d'un catalogue de machines.

Pour que ces images apparaissent, vous devez :

1. Configurez Citrix DaaS.
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 Shared Image 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.

Pour plus d'informations sur la configuration d'Azure Compute Gallery, consultez la section Configurer Azure Compute Gallery.

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.
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.

Consultez les rubriques PowerShell suivantes :

- Créer un catalogue avec disque de cache en écriture différée non persistant
- Créer un catalogue avec disque de cache en écriture différée persistant

Chiffrement Azure côté serveur

Citrix DaaS prend en charge les clés de chiffrement 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.
- 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.
- 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 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 avec 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 plus d'informations, consultez :

- Créer un catalogue de machines avec une fonctionnalité de chiffrement sur l'hôte.
- Récupérer les informations de chiffrement sur l'hôte à partir d'un profil de machine

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 cryptage double à l'aide de l'interface Configuration complète et des 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 de jeu de chiffrement de disque 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.

Consultez les rubriques PowerShell suivantes :

- Créer un catalogue de machines avec cryptage double
- Convertir un catalogue non crypté en catalogue avec cryptage double
- Vérifier que le cryptage double est appliqué au catalogue

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.

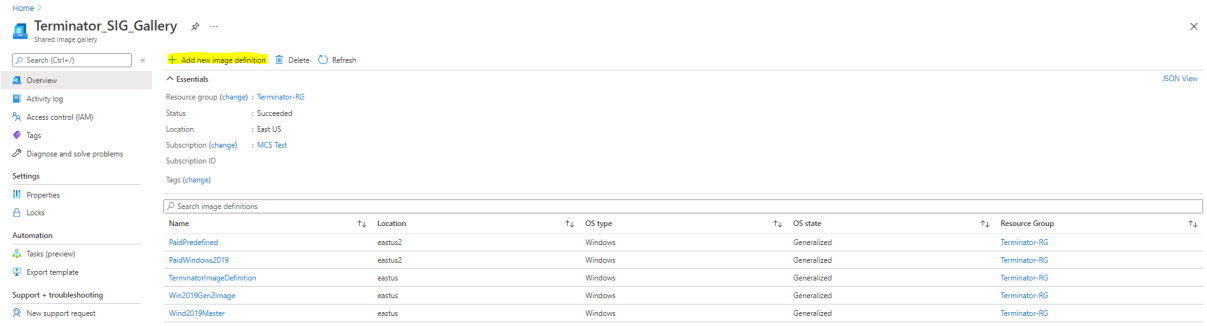
Azure Marketplace

Citrix DaaS 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 DaaS est destinée aux images payantes.

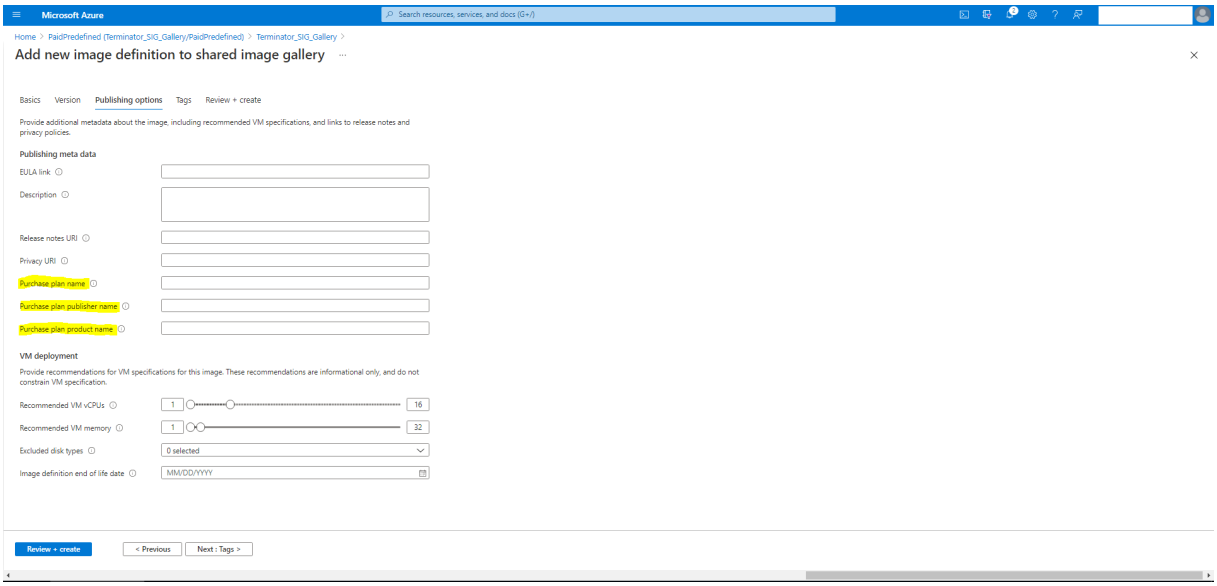
S'assurer que l'image créée dans Azure Compute Gallery contient des informations de plan Azure

Suivez la procédure décrite dans cette section pour afficher les images Azure Compute Gallery dans l'interface de configuration complète. Ces images peuvent éventuellement être utilisées pour une image principale. Pour placer l'image dans Azure Compute Gallery, créez une définition d'image dans une galerie.

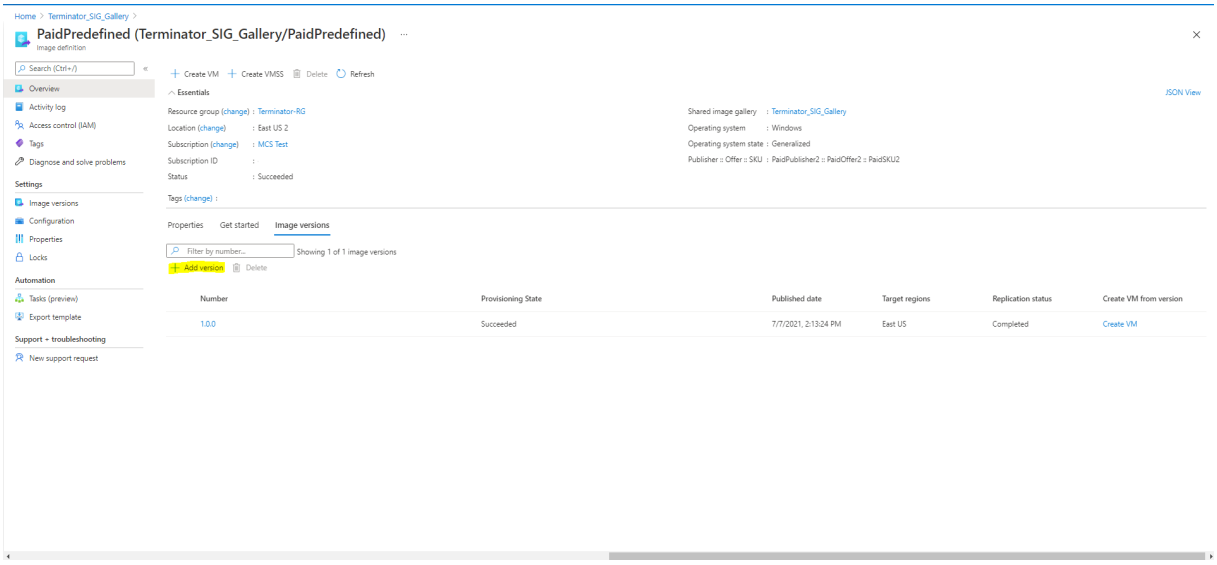


Sur la page **Options de publication**, vérifiez les informations du plan d'achat.

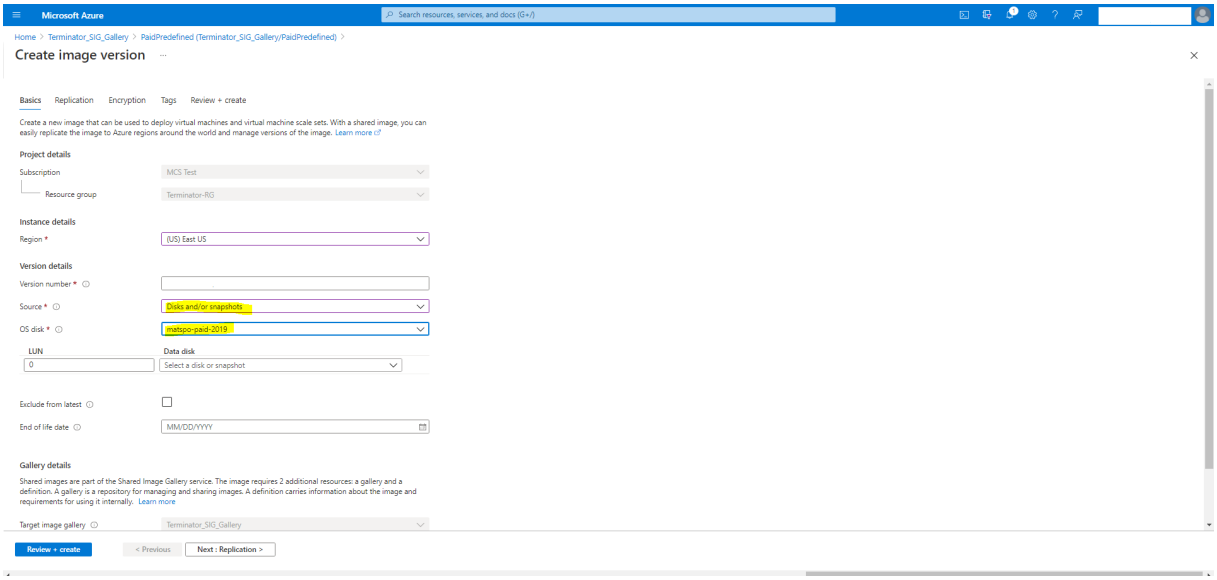
Les champs d'informations sur le plan d'achat sont initialement vides. Renseignez ces champs avec les informations de plan d'achat utilisées pour l'image. Ne pas renseigner les informations du plan d'achat peut entraîner l'échec du processus de catalogue de machines.



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 :



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 mesures 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 À propos des autorisations Azure 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 PowerShell, `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 plus d'informations sur la création d'un catalogue avec AMA activé à l'aide de PowerShell, consultez Provisionner des machines virtuelles de catalogue avec AMA activé.

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 avec des machines virtuelles confidentielles Azure à l'aide de l'interface Configuration complète et des commandes 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 de l'interface Configuration complète ou des commandes 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 l'interface Configuration complète, suivez les étapes décrites dans 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.

Utiliser PowerShell

Cette section explique comment effectuer les tâches suivantes à l'aide de PowerShell :

- Utiliser une spécification de modèle lors de la création ou de la mise à jour d'un catalogue à l'aide de PowerShell
- Activer les extensions de VM Azure
- Catalogues de machines avec lancement fiable
- Utiliser les valeurs des propriétés du profil machine
- Configurer des zones de disponibilité à l'aide de PowerShell
- Provisionner des machines virtuelles sur des hôtes dédiés Azure
- Configurer des types de stockage
- Activer le stockage redondant interzone
- Capturez les paramètres de diagnostic sur les machine virtuelle et les cartes d'interface réseau à partir d'un profil de machine
- Vérifier la licence Windows
- Configurer la licence Linux
- Créer un catalogue avec un disque éphémère Azure
- Configurer Azure Compute Gallery
- Créer ou mettre à jour un catalogue avec plusieurs cartes réseau par machine virtuelle
- Créer un catalogue avec disque de cache en écriture différée non persistant
- Créer un catalogue avec disque de cache en écriture différée persistant
- Améliorer les performances de démarrage avec MCSIO
- Créer un catalogue de machines avec une clé de chiffrement gérée par le client
- Créer un catalogue de machines avec une fonctionnalité de chiffrement sur l'hôte
- Créer un catalogue de machines avec cryptage double
- Détermination de l'emplacement du fichier de page
- Scénarios de configuration du fichier de page
- Spécifier le paramètre du fichier de page
- Modifier les paramètres du fichier de page
- Provisionner des machines virtuelles de catalogue avec l'agent AMA activé
- Créer un catalogue à l'aide des machines virtuelles Azure Spot
- Copier les balises sur toutes les ressources

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 l'interface Configuration complète ou les commandes PowerShell.

Pour l'interface Configuration complète, consultez la section Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans l'interface Configuration complète.

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>]
[<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]
[<CommonParameters>]
<!--NeedCopy-->
```

Activer les extensions de VM Azure

Après avoir sélectionné la spécification de modèle ARM, exécutez les commandes PowerShell suivantes pour utiliser les extensions de VM Azure :

- Pour afficher la liste des extensions de VM Azure prises en charge : `Get-ProvMetadataConfiguration`

- Pour ajouter d'autres extensions de VM : `Add-ProvMetadataConfiguration`. Par exemple, `Add-ProvMetadataConfiguration -PluginType "AzureRM"-ConfigurationName "Extension"-ConfigurationValue "CustomScriptExtension"`

  Si vous essayez d'ajouter l'un des éléments suivants, la commande échoue avec un message d'erreur :

  - Extension définie par Citrix.
  - Extension existante définie par l'utilisateur.
  - Clés de configuration non prises en charge. Actuellement, la clé de configuration prise en charge est `Extension`.

- Pour supprimer des extensions de la liste : `Remove-ProvMetadataConfiguration`. Vous pouvez supprimer les extensions que vous avez ajoutées.

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 DaaS 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 l'interface Configuration complète ou des commandes PowerShell.

   - Si vous souhaitez utiliser l'interface Configuration complète, consultez la section Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans l'interface Configuration complète.
   - 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`
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 propriétés 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
    ```



```
<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="<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>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA
   -value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
   value>"/>
</CustomProperties>
<!--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

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
   \machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\
   serviceoffering.folder<explicit-machine-size>.
   serviceoffering"
<!--NeedCopy-->
```

Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<explicit-machine-size>.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="explicit-storage-type"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "value-from-machineprofile"/>
</CustomProperties>
<!--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.

```
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="
      Linux"/>
4  </CustomProperties>
5  <!--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 :

```
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="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesB-value>"/>
6       </CustomProperties>
7  <!--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 :

```
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="<CustomPropertiesB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
       CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mp-A-value>"/>
6  </CustomProperties>
7  <!--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 :

```
1  Get-ProvScheme | select ServiceOffering
2  serviceoffering.folder<value-from-machineprofile>.
       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="<mpB-value>"/>
```



```
<Property xsi:type="StringProperty" Name="OSType" Value="<
    prior-CustomProperties-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<mpB-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

Configurer des zones de disponibilité à l'aide de PowerShell

À l'aide de PowerShell, vous pouvez afficher les éléments d'inventaire de l'offre Citrix DaaS 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.

Résultat de l'utilisation simultanée de groupes d'hôtes et de zones de disponibilité Azure

Une vérification préliminaire permet de déterminer si la création d'un catalogue de machines sera réussie en fonction de la zone de disponibilité spécifiée dans la propriété personnalisée et de la zone

du groupe d'hôtes. La création du catalogue échoue si la propriété personnalisée de la zone de disponibilité ne correspond pas à la zone du groupe d'hôtes.

Pour plus d'informations sur la configuration des zones de disponibilité via PowerShell, consultez Configuration des zones de disponibilité via PowerShell.

Pour plus d'informations sur les hôtes dédiés Azure, consultez la section Hôtes dédiés Azure.

Le tableau suivant décrit les différentes combinaisons de zone de disponibilité et de zone de groupe d'hôtes, et celles qui entraînent la réussite ou l'échec de la création d'un catalogue de machines.

Zone du groupe d'hôtes	Zone de disponibilité dans la propriété personnalisée	Résultat de création du catalogue de machines
Spécifié. Par exemple, le groupe d'hôtes se trouve dans la zone 1.	Aucun spécifié.	Succès. Les machines sont créées dans la zone du groupe d'hôtes.
Spécifié. Par exemple, le groupe d'hôtes se trouve dans la zone 1.	Même zone que la zone du groupe d'hôtes. Par exemple, la zone de la propriété personnalisée est définie sur 1.	Succès. Les machines sont créées dans la zone 1.
Spécifié. Par exemple, le groupe d'hôtes se trouve dans la zone 1.	Différente de la zone du groupe d'hôtes. Par exemple, la zone de la propriété personnalisée est définie sur 2.	La zone de disponibilité spécifiée et la zone du groupe d'hôtes ne correspondant pas, la création du catalogue échoue avec une erreur lors des vérifications préliminaires.
Spécifié. Par exemple, le groupe d'hôtes se trouve dans la zone 1.	Plusieurs zones sont spécifiées. Par exemple, les zones des propriétés personnalisées sont définies sur 1,2 ou 2,3.	La zone de disponibilité spécifiée et la zone du groupe d'hôtes ne correspondant pas, la création du catalogue échoue avec une erreur lors des vérifications préliminaires.
Non spécifié. Par exemple, la zone du groupe d'hôtes est None.	Aucun spécifié.	Comme la zone de disponibilité spécifiée et la zone du groupe d'hôtes correspondent (c'est-à-dire, aucune zone), la création du catalogue est réussie. Les machines ne sont créées dans aucune zone.

Zone du groupe d'hôtes	Zone de disponibilité dans la propriété personnalisée	Résultat de création du catalogue de machines
Non spécifié. Par exemple, la zone du groupe d'hôtes est `None`.	Spécifié. Par exemple, les zones de la propriété personnalisée sont définies sur une ou plusieurs zones.	La zone de disponibilité spécifiée et la zone du groupe d'hôtes ne correspondant pas, la création du catalogue échoue avec une erreur lors des vérifications préliminaires

Provisionner des machines virtuelles sur des 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 :

```
1 New-ProvScheme <otherParameters> -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="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
5 <!--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.

Configurer des 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 les types de stockage des machines virtuelles

Pour configurer les types de stockage de machines virtuelles, définissez le paramètre `StorageType` dans `New-ProvScheme`. Pour mettre à jour la valeur du paramètre `StorageType` dans un catalogue existant avec l'un des types de stockage pris en charge, utilisez la commande `Set-ProvScheme`.

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 remplacer le stockage localement redondant d'une machine virtuelle existante par un stockage redondant dans une zone.

> **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.

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 nouveau catalogue dans Azure à l'aide de la commande Powershell `New-ProvScheme`, utilisez `Standard_ZRS` comme valeur dans `StorageAccountType`.
Par exemple :

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
<!--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 tentez d'utiliser un stockage ZRS dans une région Azure qui ne prend pas en charge ce type de stockage.
- **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 :

- Interface Configuration complète.
- PowerShell. Reportez-vous à la section Gérer Citrix DaaS à l'aide des SDK Remote PowerShell. Pour plus d'informations sur la mise en œuvre de fonctionnalités spécifiques à l'aide de PowerShell, consultez Utiliser PowerShell.

Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans l'interface Configuration complète

Ces informations étayent les instructions disponibles dans la section Créer des catalogues de machines.

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.

> **Remarque :**
>
> - L'utilisation d'un disque non géré pour provisionner une machine virtuelle est obsolète.
> - 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@5180@0> où le GUID est généré de manière aléatoire. Par exemple, <!JEKYLL@5180@1>.

Dans l'assistant de création de catalogue de machines :

1. 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.
2. Sur la page **Image**, sélectionnez l'image que vous souhaitez utiliser comme image principale pour toutes les machines du catalogue. L'assistant **Sélectionner une image** s'affiche. Pour sélectionner une image, procédez comme suit :

a) (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.
b) Sélectionnez un groupe de ressources.
c) Accédez au disque géré Azure, à Azure Compute Gallery ou à la version d'image Azure.

Lorsque vous sélectionnez une image, tenez compte des points suivants :

- Vérifiez qu'un Citrix VDA est installé sur l'image.
- Si vous sélectionnez un disque rattaché à une VM, vous devez arrêter la VM 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.
> - 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.
> - 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.

Choisissez si vous souhaitez que les machines virtuelles du catalogue héritent des configurations d'un profil de machine. Par défaut, la case **Utiliser un profil de machine (obligatoire**

pour Azure Active Directory) est 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.

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

> **Remarque :**
>
> - Lorsque vous sélectionnez une image principale pour les catalogues de machines dans Azure, le profil de machine est filtré en fonction de l'image principale que vous avez sélectionnée. Par exemple, le profil de la machine est filtré en fonction du système d'exploitation Windows, du type de sécurité, de la prise en charge de la mise en veille prolongée et de l'identifiant du jeu de chiffrement de disque de l'image principale.
> - 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. Pour plus d'informations sur le lancement fiable Azure, consultez https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.

Validez la spécification du modèle ARM pour vous assurer qu'elle peut être utilisée comme profil de machine pour créer un catalogue de machines. Pour plus d'informations sur la création d'une spécification de modèle Azure, voir Créer une spécification de modèle Azure.

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@5180@2>
  - <!JEKYLL@5180@3>

  Par exemple :

  <!JEKYLL@5180@4>

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**, 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 Provisionner des machines virtuelles sur des 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.

3. 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, tenez compte des 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 :

- Introduction to Azure Storage
- Stockage Premium Azure : Design for high performance
- Azure 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.
- 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.

Consultez les pages suivantes :

- Vérifier la licence Windows
- Configurer la licence Linux

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 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 Azure Compute Gallery 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.

Pour plus d'informations sur Azure Compute Gallery, consultez la section Azure Compute Gallery.

4. Sur la page **Machines virtuelles**, indiquez le nombre de machines virtuelles à créer et leur taille. Après la création du catalogue, vous pouvez modifier la taille de machine en modifiant le catalogue.
5. 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.
6. 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.

- Choisissez si vous souhaitez crypter les données sur les machines de ce catalogue et quelle clé de cryptage utiliser. Le cryptage côté serveur à l'aide d'une clé gérée par le client (CMK) vous permet de gérer le cryptage au niveau du disque géré et de protéger les données sur les machines du catalogue. Les paramètres par défaut sont hérités du profil de la machine ou de l'image principale, le profil étant prioritaire :

  - Si vous utilisez un *profil de machine* avec une *CMK*, l'option **Utiliser la clé suivante pour chiffrer les données sur chaque machine** est sélectionnée automatiquement et utilise par défaut la clé du *profil de machine*.
  - Si vous utilisez un *profil de machine* avec une clé gérée par la plate-forme (PMK) et que l'*image principale* est cryptée avec une *CMK*, l'option **Utiliser la clé suivante pour chiffrer les données sur chaque machine** est sélectionnée automatiquement et la valeur par défaut est la clé de l'image principale.
  - Si vous n'utilisez *pas* de *profil de machine* et que l'*image principale* est cryptée avec une *CMK*, l'option **Utiliser la clé suivante pour chiffrer les données sur chaque machine** est sélectionnée automatiquement et utilise par défaut la clé de l'*image principale*.

Pour plus d'informations, consultez Chiffrement Azure côté serveur.

7. 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**.

> **Remarque :**
>
> 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.

8. 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 :

   a) Dans le champ **Type d'identité**, sélectionnez **Joint à Azure Active Directory**. L'option **Groupe de sécurité Azure AD (facultatif)** s'affiche.
   b) Cliquez sur **Groupe de sécurité Azure AD : Créer un nouveau**.
   c) Entrez un nom de groupe, puis cliquez sur **Créer**.
   d) 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.
   e) Pour ajouter le groupe de sécurité à un groupe de sécurité attribué, sélectionnez **Rejoindre un groupe de sécurité attribué en tant que membre**, puis cliquez sur **Sélectionner un groupe** pour choisir un groupe à rejoindre.
   f) Entrez le schéma de dénomination des comptes de machines virtuelles.

   Après la création du catalogue, Citrix DaaS 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 DaaS 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.

   > **Remarque :**
   >
   > Pour renommer le groupe de sécurité Azure AD après la création du catalogue, modifiez le catalogue et accédez à l'option **Groupe de sécurité Azure AD** dans le menu de navigation de gauche. Les noms des groupes de sécurité Azure AD ne doivent pas contenir les

> caractères suivants : <!JEKYLL@5180@5>.

- 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.

Créer une spécification de modèle Azure

Vous pouvez créer une spécification de modèle Azure dans le portail Azure et l'utiliser dans l'interface Configuration complète et les 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@5180@6> spécifié dans la spécification de modèle. Par exemple :

   <!JEKYLL@5180@7>
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@5180@8>

- Pour obtenir des informations sur la version de la spécification de modèle, exécutez :

  <!JEKYLL@5180@9>

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 l'interface Configuration complète ou les commandes PowerShell.

- Utilisation de l'interface **Configuration complète** : consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans l'interface Configuration complète.
- Pour PowerShell : consultez Utiliser une spécification de modèle lors de la création ou de la mise à jour d'un catalogue à l'aide de PowerShell

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 y parvenir à l'aide de l'interface Configuration complète ou de 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 dans l'interface Configuration complète

Lors de la création d'un catalogue de machines, vous pouvez spécifier des zones de disponibilité dans lesquelles vous souhaitez provisionner des machines. Sur la page **Machines virtuelles**, sélectionnez une ou plusieurs zones de disponibilité dans lesquelles vous souhaitez créer des machines.

Il existe deux raisons pour lesquelles aucune zone de disponibilité n'est proposée : la région n'a pas de zones de disponibilité ou la taille de machine sélectionnée n'est pas disponible.

Pour plus d'informations sur la configuration à l'aide d'une commande PowerShell, consultez la section Configurer des zones de disponibilité à l'aide de PowerShell.

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, consultez la section 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 Azure Compute Gallery. Pour plus d'informations, consultez la rubrique Galerie d'images partagées Azure.

Stocker 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@5180@10>.

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.

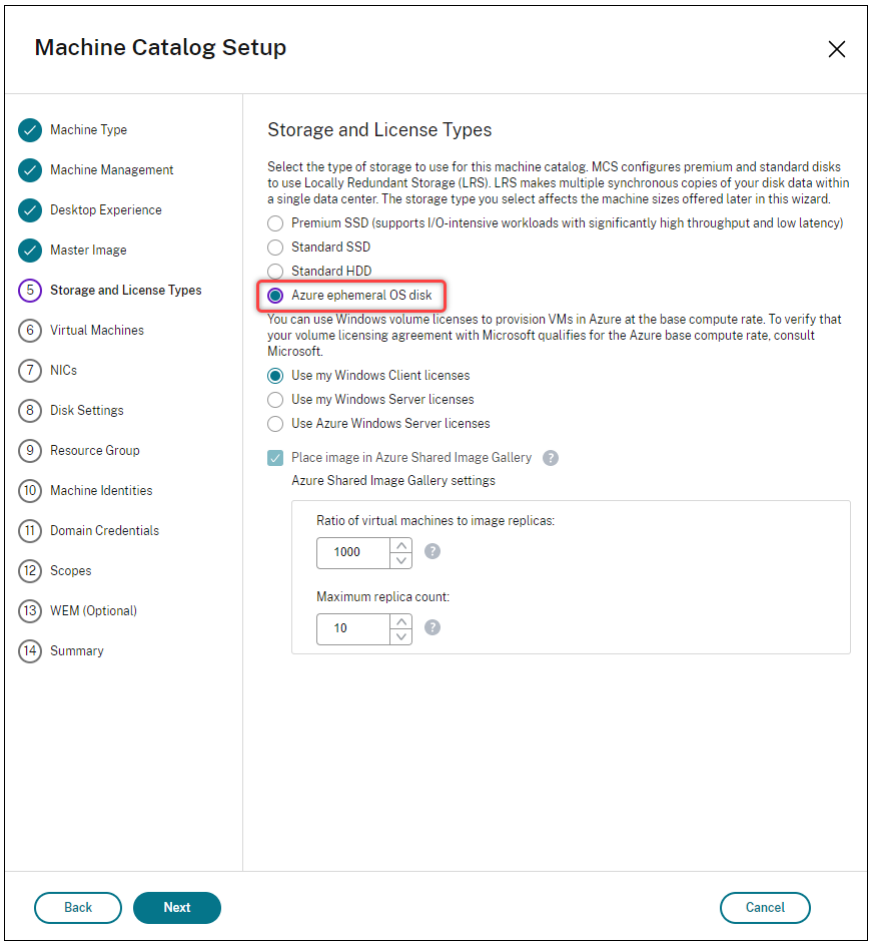
Optimisation du stockage MCS (Machine Creation Services) (E/S de MCS) et du disque d'OS éphémère

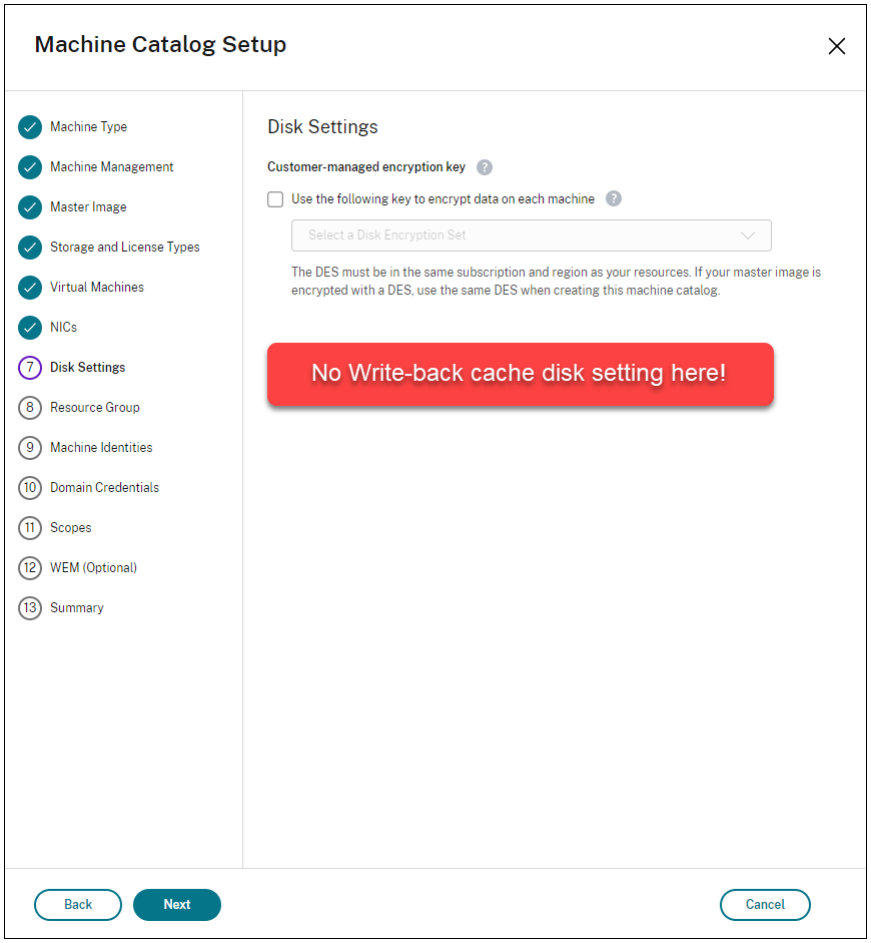
Le disque d'OS éphémère Azure et les E/S de MCS ne peuvent pas être activés en même temps.

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.

- Dans l'assistant **Création d'un catalogue de machines**, si vous sélectionnez **Disque d'OS éphémère Azure** sur la page **Types de stockage et de licence**, vous ne voyez pas l'option pour les paramètres de disque de cache en écriture différée sur la page **Paramètres du disque**.





- Les paramètres PowerShell (<!JEKYLL@5180@11> et <!JEKYLL@5180@12>) définis sur **true** dans <!JEKYLL@5180@13> ou <!JEKYLL@5180@14> échouent avec un message d'erreur approprié.
- 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 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. Azure Compute 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 Image Gallery : chaque image d'une galerie Azure Compute Gallery peut avoir plusieurs versions et chacune peut avoir plusieurs réplicas dans différentes régions. Chaque réplica est une copie complète de l'image publiée. Citrix DaaS crée une version d'image Standard_LRS (version 1.0.0) pour chaque image avec le nombre approprié de réplicas dans la région du catalogue, en fonction du nombre de machines dans le catalogue, du ratio de réplica configuré et du maximum de réplicas configuré.

> **Remarque :**
>
> La fonctionnalité Azure Compute 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 des galeries d'images partagées.

Accédez aux images depuis 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. Ces images apparaissent dans la liste d'images de la page **Image** de l'assistant Création d'un catalogue de machines.

Pour que ces images apparaissent, vous devez :

1. Configurez Citrix DaaS.
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 Shared Image 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.

Pour plus d'informations sur la configuration d'Azure Compute Gallery, consultez la section Configurer Azure Compute Gallery.

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@5180@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 « MCSWCDisk » est créé et un fichier WBC <!JEKYLL@5180@16> est placé sur ce disque.
Le disque temporaire dispose de suffisamment d'espace pour l'utilisation du cache en écriture différée, mais <!JEKYLL@5180@17> est défini sur false.	Un disque VHD « MCSWCDisk » est créé et un fichier WBC <!JEKYLL@5180@18> est placé sur ce disque.

Consultez les rubriques PowerShell suivantes :

- Créer un catalogue avec disque de cache en écriture différée non persistant
- Créer un catalogue avec disque de cache en écriture différée persistant

Chiffrement Azure côté serveur

Citrix DaaS prend en charge les clés de chiffrement 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@5180@19>. Toutes les ressources associées à la modification de <!JEKYLL@5180@20> 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.
- 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.
- 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@5180@21>

Sélectionnez un DES dans la liste. Le DES sélectionné doit se trouver dans le même abonnement et la même région que vos ressources.

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 avec 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 plus d'informations, consultez :

- Créer un catalogue de machines avec une fonctionnalité de chiffrement sur l'hôte.
- Récupérer les informations de chiffrement sur l'hôte à partir d'un profil de machine

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 cryptage double à l'aide de l'interface Configuration complète et des 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@5180@22> 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 de jeu de chiffrement de disque 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.

Consultez les rubriques PowerShell suivantes :

- Créer un catalogue de machines avec cryptage double
- Convertir un catalogue non crypté en catalogue avec cryptage double
- Vérifier que le cryptage double est appliqué au catalogue

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.

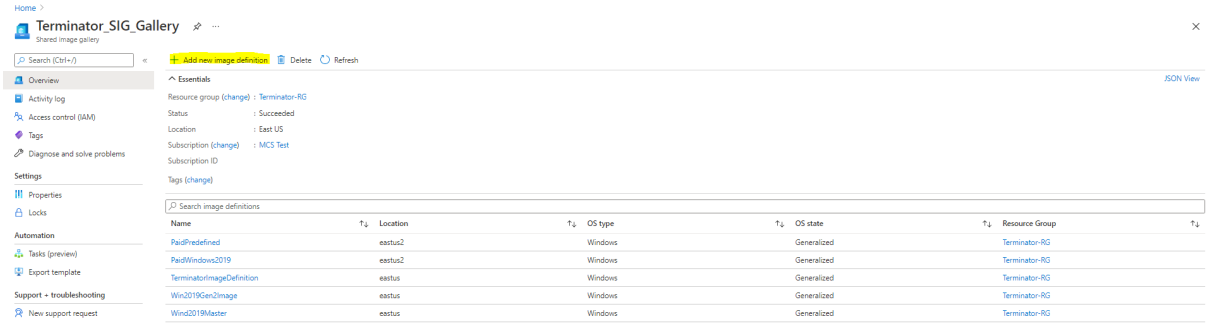
Azure Marketplace

Citrix DaaS 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 DaaS est destinée aux images payantes.

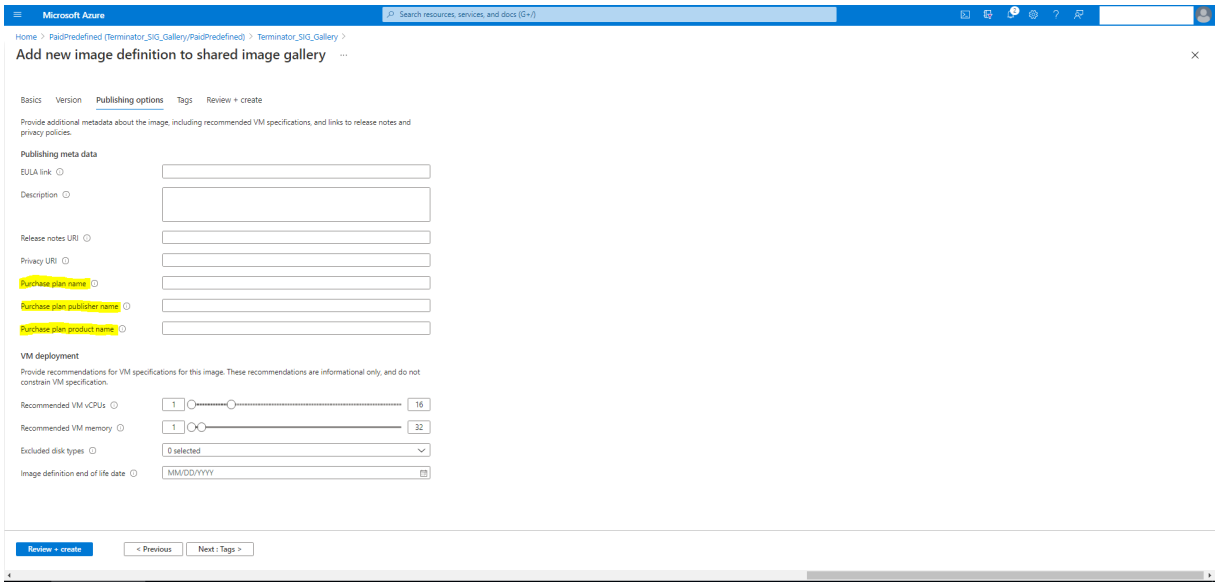
S'assurer que l'image créée dans Azure Compute Gallery contient des informations de plan Azure

Suivez la procédure décrite dans cette section pour afficher les images Azure Compute Gallery dans l'interface de configuration complète. Ces images peuvent éventuellement être utilisées pour une image principale. Pour placer l'image dans Azure Compute Gallery, créez une définition d'image dans une galerie.

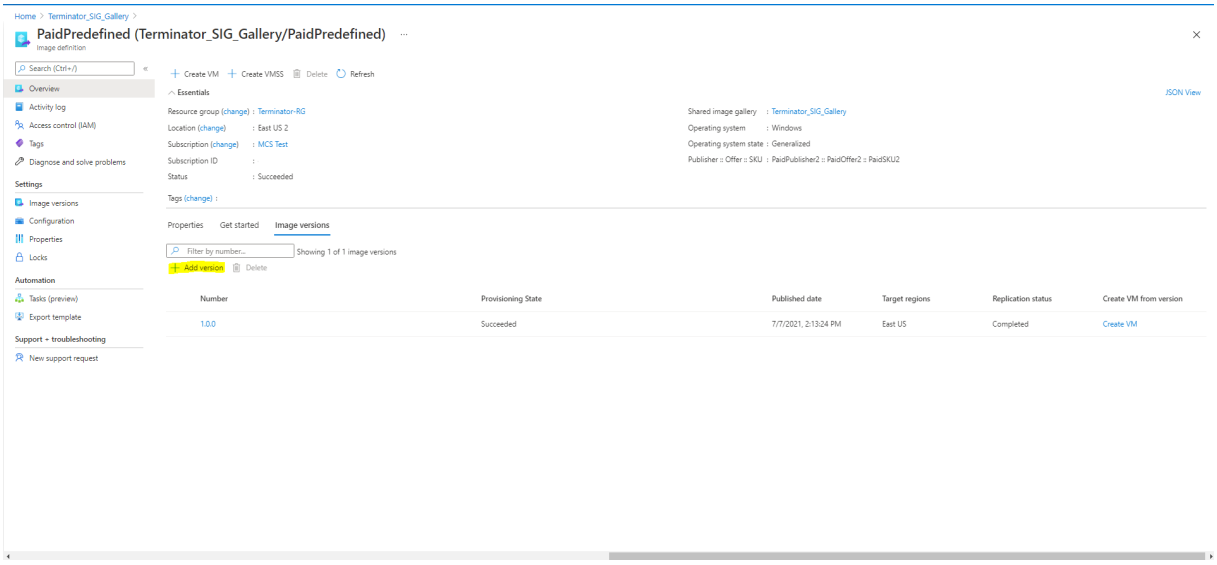


Sur la page **Options de publication**, vérifiez les informations du plan d'achat.

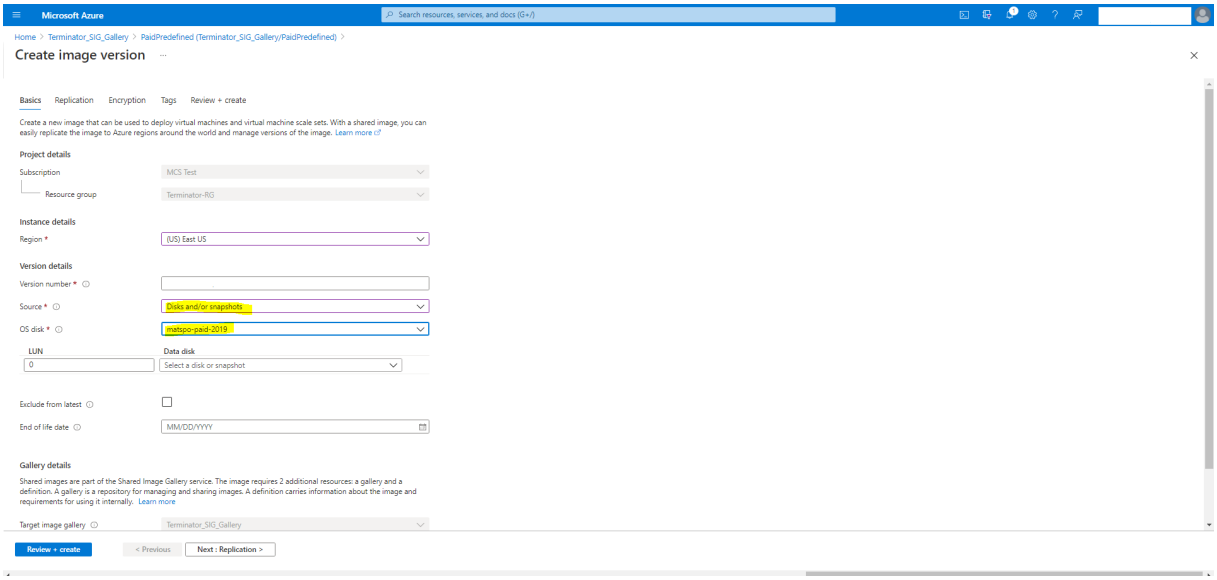
Les champs d'informations sur le plan d'achat sont initialement vides. Renseignez ces champs avec les informations de plan d'achat utilisées pour l'image. Ne pas renseigner les informations du plan d'achat peut entraîner l'échec du processus de catalogue de machines.



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 :



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 mesures 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 À propos des autorisations Azure et des autorisations suivantes pour utiliser Azure Monitor :
  - <!JEKYLL@5180@23>
  - <!JEKYLL@5180@24>
  - <!JEKYLL@5180@25>
  - <!JEKYLL@5180@26>
  - <!JEKYLL@5180@27>
- 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@5180@28> et <!JEKYLL@5180@29> sont des extensions sur liste blanche définies par Citrix. Pour afficher la liste des extensions figurant sur la liste blanche, utilisez la commande PowerShell, <!JEKYLL@5180@30>.
- 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 plus d'informations sur la création d'un catalogue avec AMA activé à l'aide de PowerShell, consultez Provisionner des machines virtuelles de catalogue avec AMA activé.

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 avec des machines virtuelles confidentielles Azure à l'aide de l'interface Configuration complète et des commandes 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@5180@31>

  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@5180@32>

  Le champ de données supplémentaire est <!JEKYLL@5180@33>.
- 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 de l'interface Configuration complète ou des commandes 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 l'interface Configuration complète, suivez les étapes décrites dans 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.

Utiliser PowerShell

Cette section explique comment effectuer les tâches suivantes à l'aide de PowerShell :

- Utiliser une spécification de modèle lors de la création ou de la mise à jour d'un catalogue à l'aide de PowerShell
- Activer les extensions de VM Azure
- Catalogues de machines avec lancement fiable
- Utiliser les valeurs des propriétés du profil machine
- Configurer des zones de disponibilité à l'aide de PowerShell
- Provisionner des machines virtuelles sur des hôtes dédiés Azure
- Configurer des types de stockage
- Activer le stockage redondant interzone
- Capturez les paramètres de diagnostic sur les machine virtuelle et les cartes d'interface réseau à partir d'un profil de machine
- Vérifier la licence Windows
- Configurer la licence Linux
- Créer un catalogue avec un disque éphémère Azure
- Configurer Azure Compute Gallery
- Créer ou mettre à jour un catalogue avec plusieurs cartes réseau par machine virtuelle
- Créer un catalogue avec disque de cache en écriture différée non persistant
- Créer un catalogue avec disque de cache en écriture différée persistant
- Améliorer les performances de démarrage avec MCSIO
- Créer un catalogue de machines avec une clé de chiffrement gérée par le client
- Créer un catalogue de machines avec une fonctionnalité de chiffrement sur l'hôte
- Créer un catalogue de machines avec cryptage double
- Détermination de l'emplacement du fichier de page
- Scénarios de configuration du fichier de page
- Spécifier le paramètre du fichier de page
- Modifier les paramètres du fichier de page
- Provisionner des machines virtuelles de catalogue avec l'agent AMA activé
- Créer un catalogue à l'aide des machines virtuelles Azure Spot
- Copier les balises sur toutes les ressources

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 l'interface Configuration complète ou les commandes PowerShell.

Pour l'interface Configuration complète, consultez la section Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans l'interface Configuration complète.

Utilisation des commandes PowerShell :

1. Ouvrez la fenêtre **PowerShell**.
2. Exécutez <!JEKYLL@5180@34>.
3. Créez ou mettez à jour un catalogue.

    - Pour créer un catalogue :
        a) Utilisez la commande <!JEKYLL@5180@35> avec une spécification de modèle comme entrée de profil de machine. Par exemple :

        <!JEKYLL@5180@36>

        b) Terminez la création du catalogue.
    - Pour mettre à jour un catalogue, utilisez la commande <!JEKYLL@5180@37> avec une spécification de modèle comme entrée de profil de machine. Par exemple :

    <!JEKYLL@5180@38>

Activer les extensions de VM Azure

Après avoir sélectionné la spécification de modèle ARM, exécutez les commandes PowerShell suivantes pour utiliser les extensions de VM Azure :

- Pour afficher la liste des extensions de VM Azure prises en charge : <!JEKYLL@5180@39>
- Pour ajouter d'autres extensions de VM : <!JEKYLL@5180@40>. Par exemple, <!JEKYLL@5180@41>

  Si vous essayez d'ajouter l'un des éléments suivants, la commande échoue avec un message d'erreur :

  - Extension définie par Citrix.
  - Extension existante définie par l'utilisateur.
  - Clés de configuration non prises en charge. Actuellement, la clé de configuration prise en charge est <!JEKYLL@5180@42>.
- Pour supprimer des extensions de la liste : <!JEKYLL@5180@43>. Vous pouvez supprimer les extensions que vous avez ajoutées.

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 DaaS 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@5180@44>
4. Exécutez <!JEKYLL@5180@45>.
5. Vérifiez la valeur de l'attribut <!JEKYLL@5180@46>.
   - Si la valeur de <!JEKYLL@5180@47> est **True**, la taille de machine virtuelle prend en charge le lancement fiable.
   - Si la valeur de <!JEKYLL@5180@48> 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@5180@49>

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@5180@50> 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@5180@51> 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@5180@52> 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 l'interface Configuration complète ou des commandes PowerShell.

   - Si vous souhaitez utiliser l'interface Configuration complète, consultez la section Créer un catalogue de machines à l'aide d'une image Azure Resource Manager dans l'interface Configuration complète.
   - Si vous souhaitez utiliser des commandes PowerShell, utilisez la commande <!JEKYLL@5180@53> 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@5180@54> avec une machine virtuelle comme entrée de profil de machine :

     <!JEKYLL@5180@55>

     Exemple de commande <!JEKYLL@5180@56> avec une spécification de modèle comme entrée de profil de machine :

     <!JEKYLL@5180@57>

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@5180@58>
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@5180@59>
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@5180@60>
Si vous sélectionnez un profil de machine avec un type de sécurité différent du type de sécurité de l'image principale	<!JEKYLL@5180@61>
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@5180@62>

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@5180@63> 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@5180@64> et <!JEKYLL@5180@65> lorsque toutes les propriétés sont définies pour <!JEKYLL@5180@66> 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@5180@67>

    Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    <!JEKYLL@5180@68>
  - MachineProfile a certaines propriétés et les propriétés CustomProperties ne sont pas définies. Exemple : MachineProfile a uniquement LicenseType et OSType.

    <!JEKYLL@5180@69>

    Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    <!JEKYLL@5180@70>
  - MachineProfile et CustomProperties définissent toutes les propriétés. Exemple :

    <!JEKYLL@5180@71>

    Les propriétés personnalisées sont prioritaires. Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    <!JEKYLL@5180@72>
  - 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@5180@73>

    Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    <!JEKYLL@5180@74>

  - 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@5180@75>

    Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    <!JEKYLL@5180@76>

  - 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@5180@77>

    La valeur de l'image principale est écrite dans les propriétés personnalisées, dans ce cas Linux.

    <!JEKYLL@5180@78>

- Scénarios Set-ProvScheme

  - Un catalogue existant avec :

    * CustomProperties pour <!JEKYLL@5180@79> et OSType
    * MachineProfile <!JEKYLL@5180@80> 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@5180@81>

    Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

    <!JEKYLL@5180@82>

  - Un catalogue existant avec :

    * CustomProperties pour <!JEKYLL@5180@83> et OSType
    * MachineProfile <!JEKYLL@5180@84> qui définit StorageAccountType et LicenseType

  - Mises à jour :

    * Un nouveau jeu de propriétés personnalisées $CustomPropertiesB qui définit StorageAccountType et OSType

  <!JEKYLL@5180@85>

  Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

  <!JEKYLL@5180@86>

- Un catalogue existant avec :
    * CustomProperties pour <!JEKYLL@5180@87> et OSType
    * MachineProfile <!JEKYLL@5180@88> qui définit les zones
- Mises à jour :
    * MachineProfile mpB.machine virtuelle qui définit StorageAccountType et LicenseType
    * <!JEKYLL@5180@89> n'est pas spécifié

  <!JEKYLL@5180@90>

  Les valeurs suivantes sont définies en tant que propriétés personnalisées pour le catalogue :

  <!JEKYLL@5180@91>

Configurer des zones de disponibilité à l'aide de PowerShell

À l'aide de PowerShell, vous pouvez afficher les éléments d'inventaire de l'offre Citrix DaaS en utilisant <!JEKYLL@5180@92>. Par exemple, pour consulter l'offre de services de la *région États-Unis de l'Est* <!JEKYLL@5180@93> :

<!JEKYLL@5180@94>

Pour afficher les zones, utilisez le paramètre <!JEKYLL@5180@95> de l'élément :

<!JEKYLL@5180@96>

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@5180@97>. 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@5180@98> pour les zones 1 et 3.

Utilisez la commande <!JEKYLL@5180@99> 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.

Résultat de l'utilisation simultanée de groupes d'hôtes et de zones de disponibilité Azure

Une vérification préliminaire permet de déterminer si la création d'un catalogue de machines sera réussie en fonction de la zone de disponibilité spécifiée dans la propriété personnalisée et de la zone du groupe d'hôtes. La création du catalogue échoue si la propriété personnalisée de la zone de disponibilité ne correspond pas à la zone du groupe d'hôtes.

Pour plus d'informations sur la configuration des zones de disponibilité via PowerShell, consultez Configuration des zones de disponibilité via PowerShell.

Pour plus d'informations sur les hôtes dédiés Azure, consultez la section Hôtes dédiés Azure.

Le tableau suivant décrit les différentes combinaisons de zone de disponibilité et de zone de groupe d'hôtes, et celles qui entraînent la réussite ou l'échec de la création d'un catalogue de machines.

Zone du groupe d'hôtes	Zone de disponibilité dans la propriété personnalisée	Résultat de création du catalogue de machines
Spécifié. Par exemple, le groupe d'hôtes se trouve dans la zone 1.	Aucun spécifié.	Succès. Les machines sont créées dans la zone du groupe d'hôtes.
Spécifié. Par exemple, le groupe d'hôtes se trouve dans la zone 1.	Même zone que la zone du groupe d'hôtes. Par exemple, la zone de la propriété personnalisée est définie sur 1.	Succès. Les machines sont créées dans la zone 1.
Spécifié. Par exemple, le groupe d'hôtes se trouve dans la zone 1.	Différente de la zone du groupe d'hôtes. Par exemple, la zone de la propriété personnalisée est définie sur 2.	La zone de disponibilité spécifiée et la zone du groupe d'hôtes ne correspondant pas, la création du catalogue échoue avec une erreur lors des vérifications préliminaires.

Zone du groupe d'hôtes	Zone de disponibilité dans la propriété personnalisée	Résultat de création du catalogue de machines
Spécifié. Par exemple, le groupe d'hôtes se trouve dans la zone 1.	Plusieurs zones sont spécifiées. Par exemple, les zones des propriétés personnalisées sont définies sur 1,2 ou 2,3.	La zone de disponibilité spécifiée et la zone du groupe d'hôtes ne correspondant pas, la création du catalogue échoue avec une erreur lors des vérifications préliminaires.
Non spécifié. Par exemple, la zone du groupe d'hôtes est <!JEKYLL@5180@100>.	Aucun spécifié.	Comme la zone de disponibilité spécifiée et la zone du groupe d'hôtes correspondent (c'est-à-dire, aucune zone), la création du catalogue est réussie. Les machines ne sont créées dans aucune zone.
Non spécifié. Par exemple, la zone du groupe d'hôtes est <!JEKYLL@5180@101>.	Spécifié. Par exemple, les zones de la propriété personnalisée sont définies sur une ou plusieurs zones.	La zone de disponibilité spécifiée et la zone du groupe d'hôtes ne correspondant pas, la création du catalogue échoue avec une erreur lors des vérifications préliminaires

Provisionner des machines virtuelles sur des 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@5180@102>

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@5180@103>.
- 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.

Configurer des 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@5180@104> est configuré pour un type d'OS et un compte de stockage. <!JEKYLL@5180@105> est configuré pour le type de stockage Cache en écriture différée. Pour un catalogue normal, <!JEKYLL@5180@106> est requis. Si <!JEKYLL@5180@107> n'est pas configuré, <!JEKYLL@5180@108> est utilisé par défaut pour <!JEKYLL@5180@109>.

Si WBCDiskStorageType n'est pas configuré, StorageType est utilisé par défaut pour WBCDiskStorageType.

Configurer les types de stockage des machines virtuelles

Pour configurer les types de stockage de machines virtuelles, définissez le paramètre <!JEKYLL@5180@110> dans <!JEKYLL@5180@111>. Pour mettre à jour la valeur du paramètre <!JEKYLL@5180@112> dans un catalogue existant avec l'un des types de stockage pris en charge, utilisez la commande <!JEKYLL@5180@113>.

Voici un exemple du paramètre <!JEKYLL@5180@114> dans un schéma de provisioning :

<!JEKYLL@5180@115>

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@5180@116> et les paramètres <!JEKYLL@5180@117> et <!JEKYLL@5180@118>. Vous pouvez remplacer le stockage localement redondant d'une machine virtuelle existante par un stockage redondant dans une zone.

> **Remarque :**
>
> - <!JEKYLL@5180@119> indique que l'heure de démarrage planifiée est l'heure actuelle.
> - <!JEKYLL@5180@120> avec un nombre négatif (par exemple, —1) indique qu'il n'y a pas de limite supérieure dans le créneau planifié.

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@5180@121>
- 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 nouveau catalogue dans Azure à l'aide de la commande Powershell <!JEKYLL@5180@122>, utilisez <!JEKYLL@5180@123> comme valeur dans <!JEKYLL@5180@124>. Par exemple :

<!JEKYLL@5180@125>

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 tentez d'utiliser un stockage ZRS dans une région Azure qui ne prend pas en charge ce type de stockage.
- **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@5180@126>
- <!JEKYLL@5180@127>
- <!JEKYLL@5180@128>

> **Remarque :**
>
> Lors de la création du catalogue, le disque d'OS du profil de machine <!JEKYLL@5180@129> 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@5180@130> 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@5180@131>.

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`.

Vérifier la licence Windows

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/.

Configurer la licence Linux

Grâce aux 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>'
2 <!--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 :

```
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" /></
    CustomProperties>'
2 <!--NeedCopy-->
```

Créer un catalogue avec un disque éphémère Azure

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.

Vous devez également tenir compte de ces contraintes lors des opérations suivantes :

- Création du schéma de provisioning
- Modification du schéma de provisioning
- Mise à jour de l'image

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 existant

Pour configurer un disque d'OS éphémère Azure pour un catalogue, définissez 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-->
```


Configurer Azure Compute Gallery

Utilisez la commande `New-ProvScheme` pour créer un schéma de provisioning avec la prise en charge de Azure Compute 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 Azure Compute Gallery :

`UseSharedImageGallery`

- Indique si vous souhaitez utiliser Azure Compute Gallery pour stocker les images publiées. Si cette propriété est définie sur **True**, l'image est stockée en tant qu'image Azure Compute 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 Azure Compute 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 Azure Compute Gallery et du maximum de réplicas

Le catalogue de machines existant utilise Azure Compute 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 :

```
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="True"/> <Property xsi:type="
     IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
     Property xsi:type="IntProperty" Name="
     SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
2 <!--NeedCopy-->
```

Cas d'utilisation : conversion d'un catalogue d'instantanés en catalogue Azure Compute 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 :

```
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="True"/> <Property xsi:type="
     IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
     Property xsi:type="IntProperty" Name="
     SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
2 <!--NeedCopy-->
```


> **Conseil :**
>
> Les paramètres `SharedImageGalleryReplicaRatio` et `SharedImageGalleryReplicaMaximum` ne sont pas obligatoires. Une fois la commande `Set-ProvScheme` terminée, l'image Azure Compute 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 Azure Compute 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 Azure Compute 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 Azure Compute 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 voir les propriétés personnalisées Azure Compute 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'instan-

> tané. 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 Azure Compute Gallery (galerie, image et version) sont automatiquement nettoyées en quelques heures.

Créer ou mettre à jour un catalogue avec plusieurs cartes réseau par machine virtuelle

MCS prend en charge plusieurs cartes réseau par machine virtuelle. Vous pouvez associer plusieurs cartes réseau sur une machine virtuelle à plusieurs sous-réseaux, mais ces sous-réseaux doivent se trouver dans le même réseau virtuel (vNet). Vous pouvez utiliser la commande PowerShell pour :

- Créer un catalogue avec plusieurs cartes réseau sur une machine virtuelle
- Mettre à jour la configuration d'un catalogue existant pour disposer de plusieurs cartes réseau sur une machine virtuelle afin que les machines virtuelles nouvellement créées disposent de plusieurs cartes réseau
- Mettre à jour une machine virtuelle existante pour disposer de plusieurs cartes réseau

Vous pouvez créer ou mettre à jour un catalogue de machines non basé sur un profil de machine et un catalogue de machines basé sur un profil de machine pour disposer de plusieurs cartes réseau sur une machine virtuelle. Actuellement, pour un catalogue de machines basé sur un profil de machine, vous ne pouvez disposer que du même nombre de cartes réseau que celui spécifié dans la source du profil de machine.

Les propriétés telles que la mise en réseau accélérée et le groupe de sécurité réseau sont dérivées de la source du profil de la machine.

> **Remarque :**
>
> La taille de la machine virtuelle doit prendre en charge le même nombre de cartes réseau et la mise en réseau accélérée correspondante, sinon vous obtiendrez une erreur.

Vous pouvez récupérer le nombre maximum de cartes réseau associées à une taille de machine virtuelle sélectionnée. Une propriété PowerShell appelée `MaxNetworkInterfaces` affiche le nombre maximal de cartes réseau lorsque vous exécutez la commande PowerShell `get-item` avec le paramètre `AdditionalData`.

Récupérer le nombre maximal de cartes réseau

Pour récupérer le nombre maximal de cartes réseau :

1. Ouvrez une fenêtre **PowerShell** depuis l'hôte Delivery Controller.

2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Exécutez `Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"` pour répertorier toutes les tailles de machines virtuelles disponibles.
4. Exécutez `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData`.
5. Vérifiez `MaxNetworkInterfaces` pour connaître le nombre maximum de cartes réseau.

Créer un catalogue avec plusieurs cartes réseau sur une machine virtuelle

Pour créer un catalogue avec plusieurs cartes réseau sur une machine virtuelle, procédez comme suit :

1. Ouvrez une fenêtre PowerShell depuis l'hôte Delivery Controller.
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. Créez le schéma de provisioning :
   - Si vous créez un catalogue de machines non basé sur un profil de machine, exécutez la commande `New-ProvScheme` avec le paramètre `NetworkMappings`. Vous pouvez ajouter plusieurs sous-réseaux au paramètre `NetworkMappings`. Par exemple :

     ```
     New-Provscheme -NetworkMappings @{
     "0"="subnetpath1";"1"="subnetpath1" }

     <!--NeedCopy-->
     ```

   - Si vous créez un catalogue de machines basé sur un profil de machine :
     a) Créez une machine virtuelle dans Azure pour disposer de plusieurs cartes réseau. Pour plus d'informations, voir Créer et gérer une machine virtuelle Windows dotée de plusieurs cartes réseau. Vous pouvez également créer une nouvelle machine virtuelle, puis associer une interface réseau sur la page Réseau du portail Azure.
     b) Exécutez la commande `New-ProvScheme` avec la machine virtuelle comme entrée de profil de machine.

     > **Remarque :**
     > Lors de la création d'un catalogue de machines basé sur un profil de machine, le nombre de `NetworkMappings` doit être identique à celui de `NetworkInterfaceCount` pour le profil de machine. Le nombre `NetworkInterfaceCount` peut être récupéré à partir de `AdditionalData` dans `Get-item -Path "machine profile path"`.

5. Terminez la création du catalogue.

Mettre à jour un catalogue pour disposer de plusieurs cartes réseau sur une machine virtuelle

Pour mettre à jour un catalogue afin d'avoir plusieurs cartes réseau sur une machine virtuelle, procédez comme suit :

1. Ouvrez une fenêtre **PowerShell** depuis l'hôte Delivery Controller.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell propres à Citrix.
3. Mettez à jour le schéma de provisioning :
    - Si vous créez un catalogue de machines non basé sur un profil de machine, exécutez la commande `Set-ProvScheme` avec le paramètre `NetworkMappings`. Vous pouvez ajouter plusieurs sous-réseaux au paramètre `NetworkMappings`. Par exemple :

      ```
      Set-Provscheme -NetworkMappings @{
      "0"="subnetpath1";"1"="subnetpath1" }

      <!--NeedCopy-->
      ```

    - Si vous créez un catalogue de machines basé sur un profil de machine :
        a) Créez une machine virtuelle dans Azure pour disposer de plusieurs cartes réseau. Pour plus d'informations, voir Créer et gérer une machine virtuelle Windows dotée de plusieurs cartes réseau.
        b) Exécutez la commande `Set-ProvScheme` avec la machine virtuelle comme entrée de profil de machine.

Mettre à jour une machine virtuelle existante pour disposer de plusieurs cartes réseau sur une machine virtuelle

Vous pouvez également mettre à jour une machine virtuelle existante en utilisant `Set-ProvVMUpdateTimeWin` et également effectuer un cycle d'alimentation sur une machine virtuelle existante pendant la fenêtre de mise à jour. Pour plus d'informations sur la mise à jour d'une machine virtuelle existante, consultez Mettre à jour les machines provisionnées vers l'état du schéma de provisioning actuel.

Créer un catalogue avec disque de cache en écriture différée non persistant

Pour configurer un catalogue avec un disque de cache en écriture différée non persistant, utilisez le paramètre PowerShell `New-ProvScheme CustomProperties`. Les propriétés personnalisées sont les suivantes :

- `UseTempDiskForWBC`. Cette propriété 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.

Par exemple, utilisation du paramètre `CustomProperties` pour définir la valeur `UseTempDiskForWBC` sur true :

```
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="PersistWBC" Value="false
          "/> `
3      <Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
          false"/> `
4      <Property xsi:type="StringProperty" Name="PersistVm" Value="false
          "/> `
5      <Property xsi:type="StringProperty" Name="StorageAccountType" Value
          ="Premium_LRS"/> `
6      <Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value
          ="Premium_LRS"/> `
7      <Property xsi:type="StringProperty" Name="LicenseType" Value="
          Windows_Client"/> `
8      <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
          ="true"/> `
9      </CustomProperties>'
10 <!--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 différée 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 `New-ProvScheme CustomProperties` 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.

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-->
```

> **Remarque :**
>
> Cet exemple s'applique uniquement à Azure. Les propriétés sont différentes dans l'environnement GCP.

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 écriture différée n'est pas supprimé lorsque l'administrateur Citrix DaaS arrête la machine à l'aide de l'interface de gestion.

Lorsque la propriété `PersistWBC` est définie sur **false**, le disque de cache en écriture différée est supprimé lorsque l'administrateur Citrix DaaS 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 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="ResourceGroups" 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 avec une clé de chiffrement gérée par le client

Si vous souhaitez créer un catalogue de machines à l'aide de commandes PowerShell, où la clé de chiffrement est une clé gérée par le client, procédez comme suit :

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=`"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 une fonctionnalité de chiffrement sur l'hôte

Pour créer un catalogue de machines avec une 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 :

```
PS XDHyp:\Connections<your connection>\east us.region\
    serviceoffering.folder>
<!--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 l'interface Configuration complète 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-->
```

Créer un catalogue de machines avec cryptage double

Vous pouvez créer et mettre à jour un catalogue de machines utilisant un cryptage double à l'aide de l'interface Configuration complète et des 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 (ex. 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 l'interface Configuration complète, effectuez l'une des opérations suivantes en plus des étapes décrites dans 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 jeu de 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 (ou une image préparée) 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"
         }
8
9   -ProvisioningSchemeName aio-test
10  -MachineProfile XDHyp:\HostingUnits\azure-east\
       machineprofile.folder\abc.resourcegroup\abx-mp.
       templatespec\1.0.0.templatespecversion
11  <!--NeedCopy-->
```

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 cryptage d'un catalogue de machines (à l'aide de propriétés personnalisées ou d'un profil de machine).

- 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 :

```
1  Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
2  -CustomProperties '<CustomProperties xmlns="http://schemas.citrix
      .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
      /2001/XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
      Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
      resourceGroups/Sample-RG/providers/Microsoft.Compute/
      diskEncryptionSets/SampleEncryptionSet" />
4  </CustomProperties>'
5  <!--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 :

```
1  Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
       XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
      resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
2  <!--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 l'interface Configuration complète, procédez comme suit :

  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.

Détermination de l'emplacement du fichier de page

L'emplacement du fichier de page est déterminé selon le scénario suivant :

> **Remarque :**
>
> L'emplacement par défaut du fichier de page est un disque du système d'exploitation.

Scénario	Emplacement
Le paramètre du fichier de page est spécifié dans les propriétés personnalisées	Comme indiqué dans les propriétés personnalisées
Le disque d'OS éphémère ou la mise en veille prolongée est activée	Disque OS
La machine virtuelle possède un disque temporaire	Disque temporaire
E/S MCS est activé	Disque WBC

Scénarios de configuration du fichier de page

Le tableau suivant 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	Vous définissez le fichier d'échange de l'image source sur le disque temporaire, tandis que la taille de machine virtuelle que vous spécifiez dans le schéma de provisioning n'a pas de disque temporaire.	Le fichier d'échange est placé sur le système d'exploitation.
Préparation de l'image	Vous définissez le fichier d'échange de l'image source sur le disque d'OS, tandis que la taille de machine virtuelle que vous spécifiez dans le schéma de provisioning a un disque temporaire.	Le fichier d'échange est placé sur le disque temporaire.
Préparation de l'image	Vous définissez le fichier d'échange de l'image source sur le disque temporaire et activez le disque d'OS éphémère 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 tentez de mettre à jour le schéma de provisioning lorsque la version du VDA est antérieure à la version 2311	Modifie le paramètre du fichier de page et envoie un avertissement
Mise à jour du schéma de provisioning	Vous tentez de mettre à jour le schéma de provisioning lorsque la version du VDA est 2311 ou ultérieure	Détermine l'emplacement du fichier de page selon l'emplacement du fichier de page déterminé

Spécifier le paramètre du fichier de page

À l'aide des commandes PowerShell, vous pouvez spécifier les paramètres du fichier de page, y compris l'emplacement et la taille. Cette action remplace les paramètres du fichier de page déterminés par MCS selon l'emplacement du fichier de page déterminé. Pour ce faire, exécutez la commande `New-ProvScheme` suivante lors de la création du catalogue de machines.

Remarques importantes

Avant de procéder à la création du catalogue, tenez compte des points suivants :

- Vous devez fournir toutes les propriétés personnalisées (PageFileDiskDriveLetterOverride, InitialPageFileSizeInMB et MaxPageFileSizeInMB) dans la commande `New-ProvScheme` ou aucune d'entre elles.
- Cette fonctionnalité n'est pas prise en charge dans Citrix Studio.
- 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.
- Vous pouvez définir à la fois la taille initiale du fichier d'échange et la taille maximale du fichier d'échange sur zéro en même temps.

> **Remarque :**
>
> Vous pouvez modifier les paramètres du fichier de page des machines virtuelles récemment ajoutées à un catalogue, sans mettre à jour l'image principale. Pour modifier les paramètres du fichier de page, vous avez besoin de la version 2311 ou ultérieure du VDA. Vous pouvez modifier les paramètres du fichier de page à l'aide des commandes PowerShell. Pour plus d'informations, consultez Modifier les paramètres du fichier de page.


```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "zijinnet" `
-IdentityPoolName "PageFileSettingExample" `
-ProvisioningSchemeName "PageFileSettingExample" `
-InitialBatchSizeHint 1 `
-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-zijincloud-resources.resourcegroup\CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3efeea88f.manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\zijinnet\virtualprivatecloud.folder\East US. region\virtualprivatecloud.folder\neal-zijincloud-resources. resourcegroup\neal-zijincloud-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\zijinnet\serviceoffering.folder\Standard_B2ms.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="PersistOsDisk" Value="false"/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="PageFileDiskDriveLetterOverride" Value="d"/> `
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB" Value="2048"/> `
<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-->
```

Modifier les paramètres du fichier de page

Vous pouvez modifier les paramètres du fichier de page des machines virtuelles récemment ajoutées à un catalogue sans mettre à jour l'image principale. Actuellement, cette fonctionnalité ne s'applique qu'aux environnements Azure.

Pour modifier les paramètres du fichier de page, vous avez besoin de la version 2311 ou ultérieure du VDA. Vous pouvez modifier les paramètres du fichier de page à l'aide des commandes PowerShell.

Voici les différents paramètres de fichier de page que vous pouvez modifier dans l'environnement Azure :

- `PageFileDiskDriveLetterOverride`

- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

Modifier les paramètres de fichier de page d'un catalogue existant

Pour modifier les paramètres de fichier de page d'un catalogue de machines existant, exécutez la commande `Set-ProvScheme`. Dans ce cas, les mises à jour ne sont appliquées qu'aux machines virtuelles nouvellement ajoutées au catalogue. Par exemple :

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -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="
    StandardSSD_LRS" />
<Property xsi:type="StringProperty" Name="
    PageFileDiskDriveLetterOverride" Value="D" />
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
    Value="2048" />
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
    ="8196" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property  xsi:type="StringProperty" Name="Zones" Value="1" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
    test-group1" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
</CustomProperties>'
<!--NeedCopy-->
```

> **Remarque :**
>
> Si vous activez le cache de réécriture et que vous essayez de définir `PageFileDiskDriveLetterOverride` sur `C:` à l'aide de la commande PowerShell, le pilote E/S MCS redirige automatiquement le fichier de page vers un lecteur de disque approprié mais pas vers `C:`.

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
 }

 }
 ,
 {

    "type": "Microsoft.Insights/
       dataCollectionRuleAssociations",
    "apiVersion": "2021-11-01",
    "name": "<associatio-name>",
    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
    "dependsOn": [
     "Microsoft.Compute/virtualMachines/<vm-name>",
    "Microsoft.Compute/virtualMachines/<vm-name>/extensions
       /AzureMonitorWindowsAgent"
    ],
    "properties": {

       "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-->
```

> **Remarque :**
>
> Si vous avez configuré une règle de collecte de données avec un connecteur de données Microsoft Sentinel, vous pouvez simplement ajouter `dataCollectionRuleAssociation` dans la spécification de modèle de la même manière que vous le feriez pour une association DCR classique. Les machines virtuelles du catalogue peuvent ensuite apparaître dans la DCR Sentinel et l'agent AMA sera installé sur ces machines virtuelles. Pour plus d'informations sur les meilleures pratiques pour la création de règles de collecte de données, consultez Meilleures pratiques pour la création et la gestion de règles de collecte de données dans Azure Monitor.

2. Créez ou mettez à jour un catalogue de machines MCS existant.

   - Pour créer un nouveau catalogue MCS :

     a) Sélectionnez cette machine virtuelle ou spécification de modèle en tant que profil de machine dans l'interface Configuration complète.
     b) Procédez aux étapes suivantes pour créer le catalogue.

   - Pour mettre à jour un catalogue MCS existant, utilisez les commandes PowerShell suivantes : Dans ce cas, seules les nouvelles machines virtuelles obtiennent le modèle de profil de machine mis à jour.

     ```
     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, exécutez `Set-ProvScheme`, puis `Set-ProvVMUpdateTimeWindow` :

     ```
     1  Set-ProvScheme -ProvisioningSchemeName "name" -MachineProfile
            "XDHyp:\HostingUnits\Unit1\machineprofile.folder\abc.
           resourcegroup\ab-machine-profile.vm"
     2  Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
            -StartsNow -DurationInMinutes -1
     3  <!--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 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**.

  ```
  1  (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.
        folder\Standard_D2ds_v4.serviceoffering"). AdditionalData
  2  <!--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.

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.

Logiciels 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 :

```
1 Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
     MachineProfile <PathToYourMachineProfile>
2 <!--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, vous êtes guidé dans la création d'un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, reportez-vous à la section Planifier et créer un déploiement.
- 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

February 21, 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 connex-

> ion à machine virtuelleM. Voir Connexion à Microsoft System Center Virtual Machine Manager.

Créer une machine virtuelle principale

- Installez un VDA sur la VM principale et sélectionnez l'option d'optimisation du bureau. Cela améliore les performances.
- Réalisez un instantané de la machine virtuelle principale à utiliser comme sauvegarde.
- Créez des bureaux virtuels.

MCS sur des partages de fichiers SMB 3

Pour les catalogues de machines créés avec MCS sur des partages de fichiers SMB 3 pour le stockage de VM, les informations d'identification doivent satisfaire aux exigences suivantes pour que les appels provenant de la bibiothèque XenServer Communications Library (HCL) se connectent avec succès 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 VM sont effectuées par le biais du serveur Hyper-V à l'aide des informations d'identification de l'utilisateur VMM.

Pour plus d'informations sur SMB 3, consultez l'article Overview of file sharing using the SMB 3 protocol in Windows Server.

Lors de l'utilisation de VMM 2012 SP1 avec Hyper-V sur Windows Server 2012 : lorsque vous utilisez SMB comme méthode de stockage, activez Authentication Credential Security Support Provider (CredSSP) depuis le Cloud Connector sur différentes machines Hyper-V individuelles. Pour plus d'informations, veuillez consulter l'article CTX137465.

À l'aide d'une session à distance PowerShell V3 standard, le HCL dans le Cloud Connector utilise CredSSP pour ouvrir une connexion à la machine Hyper-V. Cette fonctionnalité transmet des informations d'identification de l'utilisateur cryptées avec Kerberos à la machine Hyper-V, et les commandes PowerShell dans la session sur la machine Hyper-V distante exécutée avec les informations d'identification fournies (dans ce cas, celles de l'utilisateur VMM), de façon à ce que les commandes de communication vers le stockage fonctionnent correctement.

Les tâches suivantes utilisent des scripts PowerShell qui proviennent du HCL. Les scripts sont alors envoyés à la machine Hyper-V pour agir sur le stockage SMB 3.0.

Consolider l'image principale : une image crée un nouveau schéma de provisioning MCS (catalogue de machines). Il clone et écrase la VM principale en préparation pour la création de nouvelles VM à partir du nouveau disque créé (et supprime une dépendance sur la VM 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 différenciation : crée un disque de différenciation à partir de l'image générée par la consolidation de l'image. Le disque de différenciation est alors rattaché à une nouvelle VM.

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 Cloud Connector, 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 le 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 puis le supprime 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 VMM 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 à l'aide d'un script PowerShell en cours d'exécution dans la session à distance 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, vous êtes guidé dans la création d'un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, reportez-vous à la section Planifier et créer un déploiement.
- 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

February 13, 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 en utilisant Nutanix AHV XI comme ressources, sur la page **Conteneur**, 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. 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 d'interface réseau**, sélectionnez le type de carte réseau pour filtrer les réseaux associés. Cette option n'est disponible que pour les connexions PC Nutanix AHV. 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, les plug-ins Nutanix AHV 2.7.1 et Nutanix AHV 2.5.1), la taille du disque dur des machines virtuelles provisionnées s'affiche de manière incorrecte sur l'interface "Configuration complète".

- Plug-in Nutanix AHV 2.7.1 : la taille affichée est beaucoup plus petite (1 Go) que la taille de stockage réelle.
- Plug-in Nutanix AHV 2.5.1 : la taille affichée est beaucoup plus petite (32 Go) que la taille de stockage réelle.

Cependant, l'opération fonctionne comme prévu si la machine virtuelle de l'image principale est un instantané de la machine virtuelle.

Autres ressources

- S'il s'agit du premier catalogue créé, vous êtes guidé dans la création d'un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, reportez-vous à la section Planifier et créer un déploiement.
- 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

May 17, 2024

La section Créer des catalogues de machines décrit les assistants qui permettent de créer un catalogue de machines.

> **Remarque :**
>
> Avant de créer un catalogue VMware, vous devez terminer la création d'une connexion à VMware. Voir Connexion à VMware.

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*` pour charger des modules PowerShell propres à 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, vous êtes guidé dans la création d'un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, reportez-vous à la section Planifier et créer un déploiement.

- 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
- Connexion aux solutions partenaires et cloud VMware
- Créer des catalogues de machines

Créer un catalogue XenServer

March 7, 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 (anciennement Citrix Hypervisor).

> **Remarque :**
>
> Avant de créer un catalogue XenServer, vous devez terminer la création d'une connexion à XenServer. Consultez Connexion à XenServer.

Créer un catalogue de machines à l'aide d'un XenServer compatible GPU

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 VM.
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.

Créer un catalogue de machines basé sur un profil de machine à l'aide de PowerShell

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'un instantané 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`

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.

```
1 $password = "password123" | ConvertTo-SecureString -AsPlainText -
     Force
2 New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
     10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
3 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\ExampleSnapshot.snapshot"
<!--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.

Mettre à jour un catalogue avec un nouveau profil de machine

> **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.

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.

Autres ressources

- S'il s'agit du premier catalogue créé, vous êtes guidé dans la création d'un groupe de mise à disposition.
- Pour passer en revue l'ensemble du processus de configuration, reportez-vous à la section Planifier et créer un déploiement.
- 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 des catalogues de différents types de jointure

July 5, 2023

À l'aide de MCS, vous pouvez provisionner des machines en tant que machines non jointes au domaine, jointes à AD sur site, jointes à Azure AD ou jointes à Azure AD hybride.

Pour plus d'informations sur la configuration des identités de machines dans l'interface Configuration complète, voir 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
- Créer des catalogues compatibles Microsoft Intune
- Créer des catalogues joints à Azure Active Directory hybride
- Créer des catalogues non joints à un domaine

Créer des catalogues joints à Azure Active Directory

February 13, 2024

Cet article explique comment créer des catalogues joints à Azure Active Directory (AD) à l'aide de Citrix DaaS.

Pour plus d'informations sur les exigences, les limites et les considérations, consultez la section Joint à Azure Active Directory.

Avant de créer le catalogue de machines, vous devez disposer des éléments suivants :

1. Nouvel emplacement de ressources
    - Accédez à l'interface utilisateur d'administration Citrix Cloud > menu hamburger en haut à gauche > **Emplacements des ressources**.
    - Cliquez sur **+ Emplacement des ressources**.
    - Entrez un nom pour le nouvel emplacement de ressources, puis cliquez sur **Enregistrer**.
2. Créer une connexion hôte. Voir la section Créer et gérer des connexions pour plus de détails. Lorsque vous déployez des machines sur Azure, consultez la section Connexion à Azure Resource Manager.
3. Pour supprimer systématiquement les machines Azure AD obsolètes et autoriser de nouvelles machines à rejoindre Azure AD, vous pouvez attribuer le rôle d'administrateur de machine cloud au principal du service de provisioning. Si vous ne supprimez pas les machines Azure AD obsolètes, la machine virtuelle non persistante correspondante reste dans l'état d'initialisation jusqu'à ce que vous la supprimiez manuellement du portail Azure AD. Pour cela, activez la gestion des connexions hôtes des appareils joints à Azure AD à l'aide de l'interface Configuration complète ou effectuez les étapes suivantes :
    a) Connectez-vous au portail Azure et accédez à **Azure Active Directory > Rôles et administrateurs**.
    b) Recherchez le rôle intégré **Administrateur de machine cloud** et cliquez sur **Ajouter des attributions** pour attribuer le rôle au principal de service de l'application utilisée par la connexion d'hébergement.
    c) Utilisez le Citrix Remote PowerShell SDK pour exécuter les commandes suivantes afin d'obtenir les paramètres `CustomProperties` existants de la connexion d'hébergement. `${ HostingConnectionName }` fait référence au nom de la connexion d'hébergement.
        i. Ouvrez une fenêtre **PowerShell**.
        ii. Exécutez `asnp citrix*` pour charger des modules **PowerShell** propres à Citrix.

iii. Exécutez la commande suivante pour obtenir les propriétés personnalisées existantes de la connexion d'hébergement.

```
(Get-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
 ).CustomProperties
<!--NeedCopy-->
```

iv. Copiez les CustomProperties depuis la connexion vers un bloc-notes et ajoutez le paramètre de propriété <Property xsi:type="StringProperty"Name="AzureAdDeviceManagement"Value="true"/>.

v. Dans la fenêtre **PowerShell**, attribuez une variable aux propriétés personnalisées modifiées. Par exemple, $UpdatedCustomProperties='<CustomProperties ...</CustomProperties>'.

vi. Redéfinissez la propriété personnalisée sur la connexion d'hébergement :

```
Set-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
  -CustomProperties ${
 UpdatedCustomProperties }
  -ZoneUid ${
 ZoneUid }

<!--NeedCopy-->
```

vii. Exécutez la commande (Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName }).CustomProperties pour vérifier les paramètres de propriétés personnalisées mis à jour.

Vous pouvez créer des catalogues joints à Azure AD à l'aide de l'interface Configuration complète ou de **PowerShell**.

Utiliser l'interface Configuration complète

Les informations suivantes étayent les instructions disponibles dans la section Créer des catalogues de machines. Pour créer des catalogues joints à Azure AD, suivez les instructions générales de cet article, en tenant compte des détails spécifiques aux catalogues joints à Azure AD.

Dans l'assistant de création de catalogues :

1. Sur la page **Image** :
   - Sélectionnez 2106 (ou version ultérieure) comme niveau fonctionnel.
   - Sélectionnez **Utiliser un profil de machine** et sélectionnez la machine appropriée dans la liste.

2. Sur la page **Identités des machines**, sélectionnez **Joint à Azure Active Directory**. Les machines créées appartiennent à une organisation et sont connectées avec un compte Azure AD qui appartient à cette organisation. Elles n'existent que dans le cloud.

   > **Remarque :**
   >
   > - Le type d'identité **Joint à Azure Active Directory** nécessite la version 2106 ou ultérieure comme niveau fonctionnel minimum pour le catalogue.
   > - Les machines sont jointes au domaine Azure AD associé au locataire auquel la connexion d'hébergement est liée.

3. Les utilisateurs doivent disposer d'un accès explicite dans Azure pour se connecter aux machines à l'aide de leurs informations d'identification AAD. Consultez la section Joint à Azure Active Directory pour plus de détails.

Utiliser PowerShell

Les étapes **PowerShell** suivantes sont équivalentes aux opérations dans Configuration complète. 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 réside dans la création du pool d'identités et du schéma de provisioning.

Pour créer un pool d'identités pour les catalogues joints à Azure AD, procédez comme suit :

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType="AzureAD" -
     WorkgroupMachine -IdentityPoolName "AzureADJoinedCatalog" -
     NamingScheme "AzureAD-VM-##" -NamingSchemeType "Numeric" -Scope @()
     -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

Pour créer un schéma de provisioning pour les catalogues joints à Azure AD, le paramètre **MachineProfile** est requis dans New-ProvScheme :

```
1 New-ProvScheme -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=`"StandardSSD_LRS`" /><
     Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"
     Windows_Server`" /></CustomProperties>" -HostingUnitName "
     AzureResource" -IdentityPoolName "AzureADJoinedCatalog" -
     InitialBatchSizeHint 1 -MachineProfile "XDHyp:\HostingUnits\
     AzureResource\image.folder\azuread-rg.resourcegroup\MasterVDA.vm" -
     MasterImageVM "XDHyp:\HostingUnits\AzureResource\image.folder\
```



```
    azuread-rg.resourcegroup\azuread-
    small_OsDisk_1_5fb42fadf7ff460bb301ee0d56ea30da.manageddisk" -
    NetworkMapping @{
"0"="XDHyp:\HostingUnits\AzureResource\virtualprivatecloud.folder\East
    US.region\virtualprivatecloud.folder\azuread-rg.resourcegroup\
    azuread-vnet.virtualprivatecloud\Test_VNET.network" }
 -ProvisioningSchemeName "AzureADJoinedCatalog" -RunAsynchronously -
    Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits
    \AzureResource\serviceoffering.folder\Standard_DS1_v2.
    serviceoffering"
<!--NeedCopy-->
```

Toutes les autres commandes utilisées pour créer des catalogues joints à Azure AD sont les mêmes que pour les catalogues joints à AD sur site traditionnels.

Afficher l'état Azure AD

Dans l'interface Configuration complète, l'état Azure AD est visible lorsque les machines jointes à Azure AD 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
- Pas encore joint à Azure AD

> **Remarque :**
>
> Si les machines ne sont pas jointes à Azure AD, elles ne s'enregistrent pas auprès du Delivery Controller. L'état de leur enregistrement apparaît comme **Initialisation.**

En outre, à l'aide de l'interface Configuration complète, 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.

Groupe de mise à disposition

Consultez la section Créer des groupes de mise à disposition pour plus d'informations.

Activer Rendezvous

Une fois le groupe de mise à disposition créé, vous pouvez activer Rendezvous. Consultez Rendezvous V2 pour plus d'informations.

Dépannage

Si des machines ne peuvent pas être jointes à Azure AD, procédez comme suit :

- Vérifiez si l'identité gérée attribuée par le système est activée pour les machines. Elle doit être activée automatiquement sur les machines provisionnées par MCS. Le processus d'association à Azure AD échoue sans identité gérée attribuée par le système. Si l'identité gérée attribuée par le système n'est pas activée pour les machines provisionnées par MCS, la raison peut être la suivante :
  - Le paramètre `IdentityType` du pool d'identités associé au schéma de provisioning n'est pas défini sur `AzureAD`. Vous pouvez le vérifier en exécutant `Get-AcctIdentityPool`.
- Pour les catalogues qui utilisent des images principales avec VDA version 2206 ou antérieure, vérifiez l'état de provisionning de l'extension **AADLoginForWindows** pour les machines. Si l'extension **AADLoginForWindows** n'existe pas, les raisons possibles sont les suivantes :
  - Le paramètre `IdentityType` du pool d'identités associé au schéma de provisioning n'est pas défini sur `AzureAD`. Vous pouvez le vérifier en exécutant `Get-AcctIdentityPool`.
  - L'installation de l'extension **AADLoginForWindows** est bloquée par la stratégie Azure.
- Pour résoudre les problèmes de provisioning de l'extension **AADLoginForWindows**, vous pouvez consulter les journaux sous `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` sur la machine provisionnée par MCS.

  > **Remarque :**
  >
  > MCS ne base pas sur l'extension `AADLoginForWindows` pour joindre une machine virtuelle à Azure AD lorsqu'une image principale est utilisée avec VDA version 2209 ou ultérieure. Dans ce cas, l'extension `AADLoginForWindows` ne sera pas installée sur la machine provisionnée par MCS. Par conséquent, il n'est pas possible de collecter les journaux de provisionning de l'extension `AADLoginForWindows`.

- Vérifiez l'état de l'association avec Azure AD et les journaux de débogage en exécutant la commande `dsregcmd /status` sur la machine provisionnée par MCS.
- Consultez les journaux d'événements Windows sous **Journaux des applications et des services > Microsoft > Windows > User Device Registration** (Enregistrement de l'appareil utilisateur).
- Vérifiez si la gestion des appareils Azure AD est correctement configurée en exécutant `Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName }`.

Assurez-vous que la valeur de :

- la propriété `AzureAdDeviceManagement` dans `CustomProperties` est **true**
- la propriété `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` dans les métadonnées est **true**

Si `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` est défini sur **false**, cela indique que le `ServicePrincipal` de l'application utilisée par la connexion d'hébergement ne dispose pas des autorisations suffisantes pour effectuer la gestion des appareils Azure AD. Pour résoudre ce problème, attribuez à `ServicePrincipal` le rôle **Administrateur de machine cloud**.

Groupe de sécurité dynamique Azure Active Directory

Les règles de groupe dynamique placent les machines virtuelles du catalogue dans un groupe de sécurité dynamique en fonction du schéma de dénomination du catalogue de machines.

Si le schéma de dénomination du catalogue de machines est Test### (où # signifie numéro), Citrix crée la règle d'appartenance dynamique ^*Test[0-9]{3}$* dans le groupe de sécurité dynamique. Désormais, si le nom de la machine virtuelle créée par Citrix est compris entre Test001 et Test999, la machine virtuelle est incluse dans le groupe de sécurité dynamique.

> **Remarque :**
>
> Si le nom de la machine virtuelle que vous avez créée manuellement est compris entre Test001 et Test999, la machine virtuelle est également incluse dans le groupe de sécurité dynamique. C'est l'une des limites du groupe de sécurité dynamique.

La fonctionnalité de groupe de sécurité dynamique est utile lorsque vous souhaitez gérer les machines virtuelles avec Azure Active Directory (Azure AD). Elle est également utile lorsque vous souhaitez appliquer des stratégies d'accès conditionnel ou distribuer des applications depuis Intune en filtrant les machines virtuelles avec le groupe de sécurité dynamique Azure AD.

Vous pouvez utiliser des commandes **PowerShell** pour :

- Créer un catalogue de machines avec groupe de sécurité dynamique Azure AD
- Activer la fonctionnalité de groupe de sécurité pour un catalogue Azure AD
- Supprimer un catalogue de machines avec groupe de sécurité de machines jointes à Azure AD

> **Important :**
>
> - Pour créer un catalogue de machines avec groupe de sécurité dynamique Azure AD, ajouter des machines au catalogue et supprimer le catalogue de machines, vous devez disposer d'un jeton d'accès Azure AD. Pour savoir comment obtenir le jeton d'accès Azure AD, con-

> sultez https://docs.microsoft.com/en-us/graph/graph-explorer/graph-explorer-features#consent-to-permissions/.
> - Pour demander un jeton d'accès dans Azure AD, Citrix demande l'autorisation **Group.ReadWrite.All** pour l'API Microsoft Graph. Un utilisateur Azure AD disposant d'un consentement de l'administrateur locataire peut accorder l'autorisation **Group.ReadWrite.All** pour l'API Microsoft Graph. Pour savoir comment accorder le consentement de l'administrateur locataire à une application dans Azure Active Directory (Azure AD), consultez le document Microsoft https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent/.

Créer un catalogue de machines avec groupe de sécurité dynamique Azure AD

1. Dans l'interface utilisateur de configuration de catalogue de machines de la console Web, sur la page **Identités des machines**, sélectionnez **Joint à Azure Active Directory**.
2. Connectez-vous à Azure AD.
3. Obtenez le jeton d'accès à l'API MS Graph. Utilisez ce jeton d'accès comme valeur de paramètre `$AzureADAccessToken` lorsque vous exécutez les commandes **PowerShell**.
4. Exécutez la commande suivante pour vérifier si le nom du groupe de sécurité dynamique existe dans le locataire.

```
Get-AcctAzureADSecurityGroup
 –AccessToken  $AzureADAccessToken
 –Name "SecurityGroupName"
<!--NeedCopy-->
```

5. Créez un catalogue de machines à l'aide de l'ID du locataire, du jeton d'accès et du groupe de sécurité dynamique. Exécutez la commande suivante pour créer un IdentityPool avec `IdentityType=AzureAD` et créer un groupe de sécurité dynamique dans Azure.

```
New-AcctIdentityPool
-AllowUnicode
-IdentityPoolName "SecurityGroupCatalog"
-NamingScheme "SG-VM-###"
-NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
-WorkgroupMachine
-IdentityType "AzureAD"
-DeviceManagementType "None"
-AzureADTenantId  620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupName "SecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```


Activer la fonctionnalité de groupe de sécurité pour un catalogue Azure AD

Vous pouvez activer la fonctionnalité de sécurité dynamique pour un catalogue Azure AD qui a été créé sans que la fonctionnalité de groupe de sécurité dynamique soit activée. Pour ce faire :

1. Créez manuellement un nouveau groupe de sécurité dynamique. Vous pouvez également réutiliser un groupe de sécurité dynamique existant.
2. Connectez-vous à Azure AD et obtenez le jeton d'accès à l'API MS Graph. Utilisez ce jeton d'accès comme valeur de paramètre `$AzureADAccessToken` lorsque vous exécutez les commandes **PowerShell**.

   > **Remarque :**
   >
   > Pour plus d'informations sur les autorisations requises par l'utilisateur Azure AD, consultez https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent#prerequisites/.

3. Exécutez la commande suivante pour connecter le pool d'identités au groupe de sécurité dynamique Azure AD créé.

```
Set-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupNam "ExistingSecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Si vous mettez à jour le schéma de dénomination, Citrix le met à jour en tant que nouvelle règle d'appartenance. Si vous supprimez le catalogue, c'est la règle d'appartenance qui est supprimée, et non le groupe de sécurité.

Supprimer un catalogue de machines avec groupe de sécurité de machines jointes à Azure AD

Lorsque vous supprimez un catalogue de machines, le groupe de sécurité de machines jointes à Azure AD est également supprimé.

Pour supprimer le groupe de sécurité dynamique Azure AD, procédez comme suit :

1. Connectez-vous à Azure AD.
2. Obtenez le jeton d'accès à l'API MS Graph. Utilisez ce jeton d'accès comme valeur de paramètre `$AzureADAccessToken` lorsque vous exécutez les commandes **PowerShell**.
3. Exécutez la commande suivante :


```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Créer un groupe de sécurité dynamique Azure AD sous un groupe de sécurité attribué à Azure AD existant

Vous pouvez créer un groupe de sécurité dynamique Azure AD dans un groupe de sécurité attribué à Azure AD existant. Vous pouvez effectuer les opérations suivantes :

- Obtenir des informations sur les groupes de sécurité.
- Obtenir tous les groupes de sécurité attribués à Azure AD qui sont synchronisés à partir du serveur AD local ou aux groupes de sécurité attribués auxquels des rôles Azure AD peuvent être attribués.
- Obtenir tous les groupes de sécurité dynamiques Azure AD.
- Ajouter un groupe de sécurité dynamique Azure AD en tant que membre de groupe attribué à Azure AD.
- Supprimer l'appartenance entre le groupe de sécurité dynamique Azure AD et le groupe de sécurité attribué à Azure AD lorsque le groupe de sécurité dynamique Azure AD est supprimé en même temps que le catalogue de machines.

Vous pouvez également voir des messages d'erreur explicites lorsque l'une des opérations échoue.

Exigence :

Vous devez disposer du jeton d'accès à l'API MS Graph lorsque vous exécutez les commandes **PowerShell**.

Pour obtenir le jeton d'accès :

1. Ouvrez l'afficheur Graph de Microsoft et connectez-vous à Azure AD.
2. Assurez-vous de disposer des autorisations **Group.ReadWrite.All** et **GroupMember.ReadWrite.All**.
3. Obtenez un jeton d'accès depuis l'afficheur Graph de Microsoft. Utilisez ce jeton d'accès lorsque vous exécutez les commandes **PowerShell**.

Pour obtenir des informations sur les groupes de sécurité par identifiant de groupe :

1. Obtenez le jeton d'accès.
2. Trouvez l'identifiant d'un objet de groupe sur le portail Azure.
3. Exécutez la commande **PowerShell** suivante dans la console **PowerShell** :

```
Get-AcctAzureADSecurityGroup
-AccessToken <token> -GroupId <GroupUid>
```



```
<!--NeedCopy-->
```

Pour obtenir des groupes de sécurité par nom d'affichage :

1. Obtenez le jeton d'accès.
2. Exécutez la commande **PowerShell** suivante dans la console **PowerShell** :

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Name <TargetGroupDisplayName>
<!--NeedCopy-->
```

Pour obtenir des groupes de sécurité dont le nom d'affichage contient une sous-chaîne :

1. Obtenez le jeton d'accès.
2. Exécutez la commande **PowerShell** suivante dans la console **PowerShell** :

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-SearchString <displayNameSubString>
<!--NeedCopy-->
```

Pour obtenir tous les groupes de sécurité attribués à Azure AD qui sont synchronisés à partir du serveur AD local ou les groupes de sécurité attribués auxquels des rôles Azure AD peuvent être attribués :

1. Obtenez le jeton d'accès.
2. Exécutez la commande **PowerShell** suivante dans la console **PowerShell** :

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
<!--NeedCopy-->
```

Pour obtenir tous les groupes de sécurité dynamiques Azure AD :

1. Obtenez le jeton d'accès.
2. Exécutez la commande **PowerShell** suivante dans la console **PowerShell** :

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Dynamic true
<!--NeedCopy-->
```

Pour obtenir des groupes de sécurité attribués à Azure AD avec un nombre maximal d'enregistrements :

1. Obtenez le jeton d'accès.

2. Exécutez la commande **PowerShell** suivante dans la console **PowerShell** :

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
-MaxRecordCount 10
<!--NeedCopy-->
```

Pour ajouter un groupe de sécurité dynamique Azure AD en tant que membre de groupe de sécurité attribué à Azure AD :

1. Obtenez le jeton d'accès.
2. Exécutez la commande **PowerShell** suivante dans la console **PowerShell** :

```
Add-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
-RefGroupId <DSG-Id>
<!--NeedCopy-->
```

Pour obtenir les membres d'un groupe de sécurité attribué à Azure AD :

1. Obtenez le jeton d'accès.
2. Exécutez la commande **PowerShell** suivante dans la console **PowerShell** :

```
Get-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
<!--NeedCopy-->
```

> **Remarque :**
>
> `Get-AcctAzureADSecurityGroupMember` vous fournit uniquement les membres directs du type de groupe de sécurité dans le groupe de sécurité attribué à Azure AD.

Pour supprimer l'appartenance entre le groupe de sécurité dynamique Azure AD et le groupe de sécurité attribué à Azure AD lorsque le groupe de sécurité dynamique Azure AD est supprimé avec le catalogue de machines :

1. Obtenez le jeton d'accès.
2. Exécutez la commande **PowerShell** suivante dans la console **PowerShell** :

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```


Modifier le nom du groupe de sécurité dynamique Azure AD

Vous pouvez modifier le nom du groupe de sécurité dynamique Azure AD associé à un catalogue de machines. Cette modification fait en sorte que les informations du groupe de sécurité stockées dans l'objet du pool d'identités Azure AD correspondent aux informations stockées dans le portail Azure.

> **Remarque :**
>
> Les groupes de sécurité dynamiques d'Azure AD n'incluent pas les groupes de sécurité synchronisés à partir d'une instance AD locale et d'autres types de groupes tels que le groupe Office 365.

Vous pouvez modifier le nom du groupe de sécurité dynamique Azure AD à l'aide de l'interface Configuration complète et de commandes **PowerShell**.

Pour modifier le nom du groupe de sécurité dynamique Azure AD à l'aide de **PowerShell** :

1. Ouvrez la fenêtre **PowerShell**.
2. Exécutez `asnp citrix*` pour charger des modules **PowerShell** propres à Citrix.
3. Exécutez la commande `Set-AcctIdentityPool -AzureAdSeurityGroupName [DSG-Name]`.

Les messages d'erreur appropriés s'affichent si le nom du groupe de sécurité dynamique Azure AD ne peut pas être modifié.

Créer des catalogues compatibles Microsoft Intune

May 17, 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 compatibles Microsoft Intune à l'aide de Citrix DaaS. Vous pouvez activer Microsoft Intune à l'aide de l'interface Configuration complète ou de PowerShell.

Pour plus d'informations sur les exigences, les limites et les considérations, consultez Microsoft Intune.

Utiliser l'interface Configuration complète

Les informations suivantes étayent les instructions disponibles dans la section Créer des catalogues de machines. Cette fonctionnalité nécessite la sélection de **Joint à Azure Active Directory** dans **Identités des machines** lors de la création du catalogue. Suivez les instructions générales de cet article, en tenant compte des détails spécifiques à cette fonctionnalité.

Dans l'assistant de création de catalogues :

- Sur la page **Identités des machines**, sélectionnez **Joint à Azure Active Directory**, puis **Inscrire les machines dans Microsoft Intune**. Si cette option est activée, inscrivez les machines dans Microsoft Intune pour la gestion.

Utiliser PowerShell

Les étapes PowerShell suivantes sont équivalentes aux opérations dans Configuration complète.

Pour inscrire des machines dans Microsoft Intune à l'aide du SDK Remote PowerShell, utilisez le paramètre `DeviceManagementType` dans `New-AcctIdentityPool`. Cette fonctionnalité nécessite que le catalogue soit joint à Azure AD et qu'Azure AD possède la licence Microsoft Intune correcte. Par exemple :

```
1 New-AcctIdentityPool -AllowUnicode -DeviceManagementType "Intune"
     IdentityType="AzureAD" -WorkgroupMachine -IdentityPoolName "
     AzureADJoinedCatalog" -NamingScheme "AzureAD-VM-##" -
     NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-d2f2-49d2-
     ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

Dépannage

Si l'inscription des machines à Microsoft Intune échoue, procédez comme suit :

- Vérifiez si les machines provisionnées par MCS sont jointes à Azure AD. L'inscription des machines à Microsoft Intune échoue si elles ne sont pas jointes à Azure AD. Consultez https://docs.citrix.com/en-us/citrix-daas/install-configure/create-machine-identities-joined-catalogs/create-azure-ad-joined-catalogs.html pour résoudre les problèmes d'association à Azure AD.
- Vérifiez si la licence Intune appropriée est attribuée à votre locataire Azure AD. Consultez la page https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses pour connaître les licences requises pour Microsoft Intune.

- Pour les catalogues qui utilisent des images principales avec VDA version 2206 ou antérieure, vérifiez l'état de provisioning de l'extension **AADLoginForWindows** pour les machines. Si l'extension **AADLoginForWindows** n'existe pas, les raisons possibles sont les suivantes :
  - Le paramètre `IdentityType` du pool d'identités associé au schéma de provisioning n'est pas défini sur `AzureAD` ou `DeviceManagementType` n'est pas défini sur `Intune`. Vous pouvez le vérifier en exécutant `Get-AcctIdentityPool`.
  - L'installation de l'extension **AADLoginForWindows** est bloquée par la stratégie Azure.
- Pour résoudre les problèmes de provisionnement de l'extension **AADLoginForWindows**, vous pouvez consulter les journaux `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` ci-dessous sur la machine provisionnée par MCS.

  > **Remarque :**
  >
  > MCS ne se base pas sur l'extension `AADLoginForWindows` pour joindre une machine virtuelle à Azure AD et s'inscrire à Microsoft Intune lorsqu'une image principale est utilisée avec VDA version 2209 ou ultérieure. Dans ce cas, l'extension `AADLoginForWindows` ne sera pas installée sur la machine provisionnée par MCS. Par conséquent, il n'est pas possible de collecter les journaux de provisioning de l'extension `AADLoginForWindows` .

- Consultez les journaux d'événements Windows sous **Journaux des applications et des services > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider**.

Créer des catalogues joints à Azure Active Directory hybride

May 17, 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 à l'aide de Citrix DaaS.

Vous pouvez créer des catalogues joints à Azure AD à l'aide de l'interface Configuration complète 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 l'interface Configuration complète

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

Les étapes PowerShell suivantes sont équivalentes aux opérations dans Configuration complète. 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 :

```
1 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"
2 New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
    -ADUserName "corp\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
4 <!--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 Configuration complète, 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 l'interface Configuration complète, 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 :

    ```
    1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
          UserCertificate
    2  <!--NeedCopy-->
    ```

Pour plus d'informations sur le problème du certificat utilisateur, consultez CTX566696.

Créer des catalogues non joints à un domaine

November 9, 2022

Cet article explique comment créer des catalogues non joints à un domaine à l'aide de Citrix DaaS.

Pour plus d'informations sur les exigences, les limites et les considérations, consultez Non joint au domaine.

Avant de créer le catalogue de machines, vous devez disposer des éléments suivants :

1. Nouvel emplacement de ressources
    - Accédez à l'interface utilisateur d'administration Citrix Cloud > menu hamburger en haut à gauche > **Emplacements des ressources**.
    - Cliquez sur **+ Emplacement des ressources**.
    - Entrez un nom pour le nouvel emplacement de ressources, puis cliquez sur **Enregistrer**.
2. Créer une connexion hôte. Voir la section Créer et gérer des connexions pour plus de détails.

À l'aide de Citrix DaaS, vous pouvez créer des catalogues basés sur un groupe de travail ou des machines n'appartenant pas au domaine. La création de machines n'appartenant pas au domaine dépend de la façon dont le pool d'identités de compte est créé. Le pool d'identités de compte est le mécanisme utilisé par MCS pour créer et suivre les noms de machines pendant le provisioning du catalogue.

Vous pouvez créer des catalogues n'appartenant pas à un domaine à l'aide de l'interface Configuration complète ou de PowerShell.

Utiliser l'interface Configuration complète

Les informations suivantes étayent les instructions disponibles dans la section Créer des catalogues de machines. Pour créer des catalogues n'appartenant pas à un domaine, suivez les instructions générales de cet article, en tenant compte des détails spécifiques aux catalogues n'appartenant pas à un domaine.

Dans l'assistant de création de catalogues :

- Sur la page **Identités des machines**, sélectionnez **Non joint au domaine**. Les machines créées ne sont jointes à aucun domaine.

> **Remarque :**
>
> Le type d'identité **Non joint au domaine** nécessite la version 1811 ou ultérieure du VDA comme niveau fonctionnel minimum pour le catalogue. Pour le rendre disponible, mettez à jour le

> niveau fonctionnel minimum, si nécessaire.

Utiliser PowerShell

Les étapes PowerShell suivantes sont équivalentes aux opérations dans Configuration complète.

Vous pouvez créer un pool d'identités pour les catalogues n'appartenant pas à un domaine à l'aide du SDK Remote PowerShell.

Par exemple, dans les versions précédentes, tous les champs Active Directory étaient fournis dans une seule instance :

```
1 New-AcctIdentityPool -AllowUnicode -Domain "corp.local" -
      IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme "NDJ-VM-##"
      -NamingSchemeType "Numeric" -OU "CN=Computers,DC=corp,DC=local"* -
      Scope @() -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

MCS utilise désormais les nouveaux paramètres PowerShell, **WorkgroupMachine** et **IdentityType**, pour créer un pool d'identités pour les catalogues n'appartenant pas à un domaine. En utilisant le même exemple que ci-dessus, les paramètres éliminent le besoin de spécifier tous les paramètres spécifiques à AD, y compris les informations d'identification de l'administrateur de domaine :

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup" -
      WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -
      NamingScheme "NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -
      ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

Toutes les autres commandes utilisées pour créer des catalogues non joints à un domaine sont les mêmes que pour les catalogues joints à Active Directory sur site traditionnel.

Gérer des catalogues de machines

June 13, 2024

> **Remarque :**
>
> Cet article explique comment gérer des catalogues à l'aide de l'interface Configuration complète et des commandes PowerShell. Si vous avez créé le catalogue à l'aide de l'interface Déploiement rapide et que vous continuez à utiliser cette interface pour gérer le catalogue, suivez les instructions dans Gérer les catalogues dans Déploiement rapide.

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.

La gestion des catalogues peut également consister à s'assurer que chaque machine dispose des mises à jour de système d'exploitation, des mises à jour des logiciels antivirus, des mises à niveau de système d'exploitation ou des modifications apportées à la configuration les plus récentes.

- 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 utilisée dans le catalogue, puis en mettant à jour les machines. Cette méthode vous permet de mettre à jour efficacement un grand nombre de machines utilisateur.
- Pour les catalogues contenant des machines statiques affectées en permanence, vous pouvez gérer l'image ou le modèle actuellement utilisé par ces catalogues, mais seules les machines que vous ajoutez ultérieurement aux catalogues sont créées à l'aide de la nouvelle image ou du nouveau modèle.
- Pour les catalogues Remote PC Access, vous gérez les mises à jour des machines des utilisateurs en dehors de l'interface de gestion Configuration complète. 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 des connexions à des hyperviseurs hôtes et à des services cloud, consultez l'article Créer et gérer des connexions et des 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 de l'image principale d'un catalogue MCS contenant des machines persistantes, toutes les nouvelles machines ajoutées au catalogue utilisent l'image mise à jour. Les machines préexistantes continuent d'utiliser l'image principale 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 uniquement si la machine est redémarrée dans Studio ou PowerShell. Si la machine est redémarrée à partir de l'hyperviseur en dehors de Studio, le disque n'est pas réinitialisé.

- 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 l'interface Configuration complète
- Utilisation de PowerShell

Utiliser l'interface Configuration complète

Cette section explique comment gérer des catalogues à l'aide de l'interface Configuration complète :

- Afficher les détails du catalogue
- Ajouter des machines à un catalogue
- Supprimer des machines d'un catalogue
- Modifier un catalogue
- Renommer un catalogue
- Supprimer un catalogue
- Gérer les comptes d'ordinateurs Active Directory dans un catalogue
- Modifier l'image principale d'un catalogue
- Modifier le niveau fonctionnel ou annuler la modification
- Cloner un catalogue
- Organiser les catalogues sous forme de dossiers
- Configurer la mise à niveau automatique pour les VDA
- Gérer le jeu de configuration d'un catalogue
- Réessayer de créer un catalogue
- (VDA non provisionnés par Citrix uniquement) Générer et gérer des jetons d'inscription

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 Aléatoire : les machines du catalogue sont attribuées à un utilisateur de manière aléatoire. 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 Type d'OS : OS multi-session (virtuel). Données utilisateur : Abandonner. Type d'OS : OS multi-session (virtuel). Données utilisateur : Sur le disque local Type d'OS : OS mono-session (Remote PC Access) Type d'OS : OS mono-session (virtuel). Données utilisateur : Abandonner. Type d'OS : OS mono-session (virtuel). Données utilisateur : Sur le disque local
Nombre de machines	Nombre de machines du catalogue et méthode de provisioning utilisée. Les méthodes de provisioning possibles incluent : Machine Creation Services (MCS), Manuel et Citrix Provisioning Services.
Nombre alloué	Nombre de machines du catalogue attribuées à un groupe de mise à disposition.
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 (hyperviseur ou fournisseur de service cloud) 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 l'interface de gestion Configuration complète pour créer des comptes d'ordinateur Active Directory pour les machines supplémentaires, vous devez disposer des autorisations d'administrateur de domaine appropriées.

> **Conseil :**
>
> Si le compte Citrix DaaS utilisé pour ajouter des machines au catalogue possède des autorisations AD restreintes, ajoutez tous les connecteurs cloud souhaités dans l'écran **Ouvrir une session sur**.

Pour ajouter des machines à un catalogue :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez un catalogue de machines, puis sélectionnez **Ajouter des machines** dans la barre d'actions.
3. Sur la page **Machines virtuelles**, sélectionnez le nombre de machines virtuelles à ajouter.
4. Sur la page **Identités des machines**, configurez les paramètres comme suit :

    - Sélectionnez une identité dans la liste.
    - Le cas échéant, indiquez s'il faut créer des comptes ou utiliser des comptes existants, ainsi que l'emplacement (domaine) de ces comptes.

      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.

      Si vous utilisez des comptes Active Directory existants, accédez aux comptes ou sélectionnez **Importer** et spécifiez un fichier `.csv` contenant les noms de compte. Assurez-vous qu'il existe suffisamment de comptes pour toutes les machines que vous ajoutez. L'interface Configuration complète gère ces comptes. 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).
    - Si ce pool d'identités est utilisé par d'autres catalogues, vous ne pouvez pas le remplacer par un autre pool à l'aide de Configuration complète. Utilisez plutôt l'applet de com-

mande PowerShell **Set-ProvScheme**. Pour de plus amples informations, consultez la documentation de SDK Citrix Virtual Apps and Desktops.

- 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. 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.

  Lorsque vous spécifiez par quoi commencent les noms de compte, tenez compte du scénario suivant : Si les chiffres ou les lettres de départ sont déjà utilisés, le premier compte créé est nommé à l'aide des chiffres ou des lettres non utilisés les plus proches par la suite.

  Consultez Gérer le numéro de séquence du nom de la machine pour personnaliser le numéro de séquence des machines déployées à l'aide de MCS, via les commandes PowerShell.

5. Sur la page **Informations d'identification du domaine**, sélectionnez **Entrer informations d'identification** et entrez les informations d'identification de l'utilisateur avec des autorisations suffisantes pour créer des comptes de machine.

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 machines se poursuit même si vous fermez l'interface de gestion Configuration complète.

Utiliser des fichiers CSV pour ajouter des machines en vrac à un catalogue

Vous pouvez ajouter des machines en bloc à l'aide de fichiers CSV. La fonctionnalité est disponible pour tous les catalogues à l'exception des catalogues provisionnés via MCS.

Pour ajouter des machines en vrac à un catalogue, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez un catalogue de machines, puis sélectionnez **Ajouter des machines** dans le volet d'action. La fenêtre **Ajouter des machines** s'affiche.
3. Sélectionnez **Ajouter un fichier CSV**. La fenêtre **Ajouter des machines en vrac** s'affiche.
4. Sélectionnez **Télécharger le modèle CSV**.
5. Remplissez le fichier modèle.
6. Faites glisser le fichier ou naviguez jusqu'au fichier pour le télécharger.
7. Sélectionnez **Valider** pour contrôler la validité de votre importation.
8. Sélectionnez **Importer** pour terminer le processus.

Considérations lors de l'utilisation de fichiers CSV pour ajouter des machines

> **Remarque :**
>
> - Pour les utilisateurs non Active Directory, vous devez saisir leur nom au format suivant : `<identity provider>:<user name>`. Exemple : `AzureAD:username`.
> - Les noms de VM sont sensibles à la casse. Lors de la saisie des chemins d'accès aux machines virtuelles, assurez-vous de saisir correctement les noms des machines virtuelles.

Lorsque vous modifiez le fichier de modèle CSV, gardez à l'esprit les points suivants :

- La fonctionnalité vous donne plus de flexibilité avec l'ajout de machines en vrac via un fichier CSV. Dans le fichier, vous pouvez ajouter uniquement des machines (à utiliser avec des attributions utilisateur automatiques) ou ajouter des machines avec attributions utilisateur. Tapez vos données dans le format suivant :
  - Pour les paires compte de machine/nom d'utilisateur (samName) :
    - Domain\ComputerName1, Domain\Username1
    - Domain\ComputerName2, Domain\Username1;Domain\Username2
    - Domain\ComputerName3, AzureAD:username
  - Pour les comptes de machine uniquement :
    - Domain\ComputerName1
    - Domain\ComputerName2
  - Pour les paires VM et noms d'utilisateur :
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Computer
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Computer
  - Pour les VM uniquement :
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName1.vm,Domain\Computer
    - XDHyp:\Connections\ConnectionName\RegionName\vm.folder\VMName2.vm,Domain\Computer

    Par exemple :
    `XDHyp:\Connections\xpace-scale\East US.region\vm.folder\wsvdaV3-2.vm`

    où

    - `xpace-scale` correspond à la valeur ConnectionName : le nom de la connexion que vous avez saisi dans **Configuration complète > Hébergement > Ajouter des connexions et des ressources**. Pour de plus amples informations, consultez Créer une connexion et des ressources.

    * `East US.region` correspond à la valeur RegionName : le nom de la région avec l'extension `.region`.
    * `wsvdaV3-2.vm` correspond à la valeur VMName : le nom de la machine virtuelle avec l'extension `.vm`.

- Le nombre maximal de machines qu'un fichier peut contenir est de 1 000. Pour importer plus de 1 000 machines, répartissez-les sur différents fichiers, puis importez ces fichiers un par un. Nous vous recommandons de ne pas importer plus de 1 000 machines. Sinon, la création d'un catalogue peut prendre beaucoup de temps.

Vous pouvez également exporter des machines à partir d'un catalogue sur la même page **Ajouter des machines**. Le fichier CSV exporté des machines peut ensuite être utilisé comme modèle lors de l'ajout de machines en masse. Pour exporter des machines :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez un catalogue de machines, puis sélectionnez **Ajouter des machines** dans le volet d'action. La fenêtre **Ajouter des machines** s'affiche.
3. Sélectionnez **Exporter au format CSV**. Un fichier CSV contenant une liste des machines est téléchargé.
4. Ouvrez le fichier CSV pour ajouter ou modifier des machines selon vos besoins. Pour ajouter des machines en vrac à l'aide du fichier CSV enregistré, consultez la section précédente, Utiliser des fichiers CSV pour ajouter des machines en vrac à un catalogue.

> **Remarque :**
>
> - Cette fonctionnalité n'est pas disponible pour Remote PC Access et les catalogues provisionnés par MCS.
> - L'exportation et l'importation de machines dans des fichiers CSV ne sont prises en charge qu'entre des catalogues du même type.

Inscrire des machines à des catalogues à l'aide de l'outil d'inscription de VDA WebSocket

L'outil d'inscription de VDA WebSocket facilite l'inscription basée sur des jetons pour les machines VDA. Cet outil vous permet de convertir une connexion en connexion WebSocket en ajoutant le VDA au catalogue de machines à l'aide du jeton d'inscription.

> **Remarque :**
>
> Cet outil est conçu pour inscrire des machines VDA qui n'ont été inscrites dans aucun catalogue de machines.

Pour exécuter l'outil d'inscription, procédez comme suit :

1. Connectez-vous au VDA.
2. Localisez l'outil `EnrollMachine.exe` dans `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool`.
3. Exécutez l'outil avec les paramètres d'entrée appropriés. Par exemple, `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

Le tableau suivant décrit les paramètres d'entrée de l'outil d'inscription :

Nom du paramètre	Obligatoire	Description	Exemple
`-websocket_token_stdin`	Oui	Lit le jeton d'inscription.	`.\EnrollMachine.exe -websocket_token_stdin`
`-websocket_token_string`		Lit le jeton d'inscription directement à partir du paramètre de ligne de commandes.	`.\EnrollMachine.exe -websocket_token_string:<token>`
`-websocket_token_file:[token-file-path]`		Lit le jeton d'inscription à partir du chemin fourni.	`.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt`
`log:[log-file-path]`	Non	Affiche les journaux de l'outil d'inscription.	`.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]`
`-help`	Non	Affiche un bref texte d'aide.	`.\EnrollMachine.exe -help`

Une fois l'inscription réussie, vous recevrez un message de réussite sur l'outil et dans les journaux. Assurez-vous de vous connecter à la configuration complète pour vérifier que la machine VDA est ajoutée au catalogue et que son état est enregistré.

Dépannage Par défaut, vous pouvez trouver les journaux de l'outil d'inscription à l'adresse suivante :

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

Si vous avez spécifié un chemin différent pour les journaux, vous pouvez utiliser `log: [log-file-path]` pour récupérer vos journaux.

Le tableau suivant répertorie les codes renvoyés par l'outil d'inscription :

Code	Chaîne	Description
0	Réussite	Le VDA a été ajouté au catalogue de machines.
-1	InvalidArgument	Le paramètre d'entrée du jeton d'inscription n'est pas valide.
-2	BrokerAgentNotFound	Le service d'agent broker est introuvable.
-3	TokenInvalid	Le jeton saisi n'est pas valide.
-4	TokenMissingRequiredClaims	Les revendications requises pour le jeton sont manquantes, par exemple, l'ID client ou les URI d'inscription.
-5	InternalError	Une erreur générale s'est produite.
-6	TimedOut	Le délai de la tâche a expiré.
-7	FailedToDetermineMachineADJoinedStatus	Le service qui renvoie l'état de la jointure AD de la machine a échoué.
-8	ADMachineFailedToFindSid	Le service qui renvoie le SID de la machine AD a échoué.
-9	EnrollRequestFailed	La demande a échoué en raison d'une erreur HTTP.
-10	EnrollResponseMissingRequiredFields	Le paramètre `VirtualSiteId` est absent de la réponse de l'outil d'inscription.
-11	InsufficientPermission	Vous n'avez pas l'autorisation requise pour exécuter la tâche.

Code	Chaîne	Description
-12	FailedToDetermineMachineAadJoinedStatus	Le test qui vérifie l'état de jointure AD de la machine génère une erreur.
-13	AadMachineFailedToFindDeviceId	Le paramètre supplémentaire `AAD device id` ajouté par le système est vide.
-14	AadDeviceIdNotValid	Le paramètre supplémentaire `AAD device id` ajouté par le système n'est pas un GUID valide.
-15	NoValidMacAddress	Adresse MAC non valide.
-16	FailedToGetComputerHostNameForVdaInstanceName	Impossible d'obtenir le nom d'hôte de l'ordinateur pour définir le paramètre supplémentaire `VdaInstanceName`.
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	Impossible d'ouvrir la clé de registre VDA pour écrire la liste des Delivery Controller.
-18	Failed Token reached the max count	Le nombre maximal de jetons ayant échoué a été atteint.

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. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionner un catalogue, puis sélectionnez **Afficher les machines** dans la barre d'actions.
3. Sélectionnez une ou plusieurs machines, puis sélectionnez **Supprimer** dans la barre d'actions.

4. Si vous supprimez des machines persistantes du catalogue, indiquez si vous souhaitez les supprimer également de l'hyperviseur ou du service cloud. Si vous choisissez de les supprimer, indiquez s'il faut conserver, désactiver ou supprimer leurs comptes Active Directory.

Lorsque vous supprimez des machines persistantes d'un catalogue Azure Resource Manager, les machines et les groupes de ressources associés sont supprimés d'Azure, même si vous choisissez de les conserver.

Lorsque vous supprimez des machines non persistantes d'un catalogue, elles sont automatiquement supprimées de l'hyperviseur ou du service cloud.

Modifier un catalogue

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez un catalogue, puis sélectionnez **Modifier le catalogue de machines** dans la barre d'actions.
3. Sur la page **Étendues**, modifiez les étendues.
4. Sur la page **Carte d'interface réseau**, effectuez les actions suivantes :

   - Pour modifier le mappage de sous-réseau d'une carte d'interface réseau, sélectionnez un réseau dans le champ **Réseau associé**.
   - Pour ajouter un mappage de sous-réseau, sélectionnez **Ajouter une carte réseau**, sélectionnez un réseau dans le champ **Réseau associé**, puis sélectionnez **Enregistrer**.

   Seuls les sous-réseaux présents sur l'hôte associé au catalogue s'affichent dans le champ **Réseau associé**.

   Vous pouvez uniquement ajouter une carte d'interface réseau aux catalogues de machines Azure sans profil de machine.

   > **Remarque :**
   >
   > - Pour les catalogues de machines AWS, vous ne pouvez pas mapper le même sous-réseau à plusieurs cartes d'interface réseau.
   > - Pour les catalogues de machines avec des profils de machine, le nombre de cartes d'interface réseau du catalogue doit être égal au nombre de cartes d'interface réseau du profil de machine.
   > - Cette fonctionnalité n'est pas prise en charge pour les hyperviseurs IBM Cloud.
   > - Cette fonctionnalité n'est prise en charge que pour Nutanix Prism Element dans le cas des hyperviseurs Nutanix.

5. Sur la page **Mise à niveau de VDA**, modifiez ou sélectionnez la version de VDA vers laquelle effectuer la mise à niveau. Pour de plus amples informations, consultez Mise à niveau de VDA.
6. Des pages supplémentaires 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 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 réinitialisera 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.

   Pour plus d'informations sur les paramètres disponibles sur les pages, consultez Créer un catalogue de machines à l'aide d'une image Azure Resource Manager.

   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.

7. Sur la page **Description**, modifiez la description du catalogue.
8. Cliquez sur **Appliquer** pour appliquer les modifications que vous avez apportées et cliquez sur **Enregistrer** pour quitter la page.

Renommer un catalogue

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez un catalogue, puis sélectionnez **Renommer le catalogue de machines** dans la barre d'actions.
3. Entrez le nouveau nom.

Supprimer un catalogue

Avant de supprimer un catalogue, vérifiez ce qui suit :

- Tous les utilisateurs ont fermé leur session et qu'aucune session déconnectée n'est en cours d'exécution.
- 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. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez un catalogue, puis sélectionnez **Supprimer le catalogue de machines** dans la barre d'actions.
3. Si le catalogue contient des machines persistantes, indiquez si vous souhaitez également supprimer ces machines de l'hyperviseur ou du service cloud. Si vous choisissez de le faire, indiquez si vous souhaitez conserver, désactiver ou supprimer leurs comptes d'ordinateur Active Directory.
4. Si nécessaire, sélectionnez **Masquer la progression** pour exécuter la suppression en arrière-plan.

> **Remarque :**
>
> - Lorsque vous supprimez un catalogue Azure Resource Manager, les machines et les groupes de ressources associés sont supprimés d'Azure, même si vous choisissez de les conserver.

> - Lorsque vous supprimez un catalogue contenant des machines non persistantes, ces machines sont supprimées de l'hyperviseur ou du service cloud.
> - Lorsque l'hyperviseur ou le service cloud est inaccessible au cours de la suppression du catalogue, la suppression du catalogue et des machines virtuelles échoue. Si nécessaire, vous pouvez choisir de supprimer les enregistrements de machine virtuelle uniquement de la base de données de votre site Citrix. Pour ce faire, sélectionnez le catalogue de machines dans le nœud **Catalogues de machines**, puis effectuez la suppression indiquée dans l'onglet **Dépannage**. N'oubliez pas que cette action laisse les machines virtuelles intactes sur l'hôte.

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 mono-session et 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. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez un catalogue, puis sélectionnez **Gérer les comptes AD** dans la barre d'actions.
3. 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. Si vous entrez un mot de passe, le mot de passe est modifié sur les comptes lors de leur importation. Si vous supprimez un compte, indiquez si le compte dans Active Directory doit être conservé, désactivé ou supprimé.

Vous pouvez également indiquer si les comptes Active Directory doivent être conservés, désactivés ou supprimés lorsque vous supprimez les machines d'un catalogue ou supprimez un catalogue.

Modifier l'image principale d'un catalogue

Nous vous recommandons de sauvegarder des copies ou des instantanés d'images avant de modifier l'image principale d'un catalogue. La base de données conserve un enregistrement historique des images utilisées avec chaque catalogue de machines. Si les utilisateurs rencontrent des problèmes avec la nouvelle image que vous avez déployée sur leur bureau, vous pouvez revenir à la version précédente afin de minimiser les temps d'inactivité des utilisateurs. Ne supprimez, déplacez ou renommez pas les images. Sinon, vous ne pourrez pas restaurer l'image principale.

> **Important :**
>
> Lorsque vous modifiez l'image principale d'un catalogue persistant, tenez compte des points suivants : Seules les machines que vous ajoutez au catalogue ultérieurement sont créées à l'aide de la nouvelle image. Nous ne déployons pas la nouvelle image sur les machines existantes du catalogue.

Après qu'une machine a été mise à jour, elle redémarre automatiquement.

Mettre à jour ou créer une image

Avant de modifier l'image principale d'un catalogue, préparez une nouvelle image sur votre hyperviseur hôte en mettant à jour une image existante ou en en créant une.

1. Sur votre hyperviseur ou fournisseur de services de cloud, prenez un instantané de la VM et donnez à l'instantané un nom significatif. Cet instantané peut être utilisé pour restaurer l'image principale.
2. Si nécessaire, démarrez l'image et ouvrez une session.
3. Installez les mises à jour ou apportez les modifications requises à l'image.
4. Si l'image utilise un Personal vDisk, mettez à jour l'inventaire.
5. Arrêtez la machine virtuelle.
6. Prenez un instantané de la VM et attribuez-lui un nom significatif qui sera reconnu lorsque vous modifiez l'image principale.

> **Remarque :**
>
> Bien que vous puissiez créer un instantané à l'aide de l'interface de gestion, nous vous recommandons de créer un instantané à l'aide de la console de gestion de l'hyperviseur, puis de sélectionner cet instantané dans l'interface de gestion Configuration complète. Cette méthode vous permet de choisir un nom et une description significatifs plutôt qu'un nom généré automatiquement. Pour les images GPU, vous pouvez modifier l'image uniquement par le biais de la console XenCenter de XenServer.

Modifier l'image principale

Pour déployer une nouvelle image principale sur toutes les machines d'un catalogue :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez un catalogue, puis sélectionnez **Modifier image principale** dans la barre d'actions.
3. 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**.

4. Sur la page **Stratégie de déploiement**, indiquez lorsque les machines du catalogue de machines doivent être modifiées avec la nouvelle image : 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.

5. Sur la page **Résumé**, vérifiez les informations et sélectionnez **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. Pour un catalogue non persistant, vous pouvez suivre l'état de mise à jour de ses images via la colonne **Mise à jour des images**, notamment **Entièrement mis à jour**, **Partiellement mis à jour**, **En attente de mise à jour** et **Préparation de l'image**.

   > **Conseil :**
   >
   > Pour afficher la colonne **Mise à jour des images**, sélectionnez l'icône **Colonnes à afficher** dans la barre d'actions, sélectionnez **Catalogue de machines > État de l'image**, puis cliquez sur **Enregistrer**.

Si vous mettez à jour un catalogue à l'aide du SDK du PowerShell, vous pouvez spécifier un modèle d'hyperviseur (`VMTemplates`), comme alternative à une image ou un instantané de l'image.

Stratégie de déploiement

La modification de l'image 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.

> **Remarque :**
>
> La stratégie de déploiement s'applique uniquement aux machines virtuelles non persistantes.

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 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.

Restaurer l'image principale

Après avoir déployé une image 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. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez le catalogue, puis sélectionnez **Restaurer image principale** dans la barre d'actions.
3. Spécifiez quand appliquer la version antérieure de l'image aux machines, comme décrit pour l'opération de déploiement.

La restauration n'est appliquée qu'aux machines qui doivent être rétablies. Pour les machines qui n'ont pas été modifiées avec l'image nouvelle ou mise à jour (par exemple, des machines avec des utilisateurs qui n'ont pas fermé leur session), les utilisateurs ne reçoivent pas de messages de notification et ne sont pas forcés 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.

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.

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. Nous vous recommandons 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 de Citrix DaaS. Cela permet à l'interface de gestion de déterminer si les machines du catalogue doivent être mises à niveau.

Pour modifier le niveau fonctionnel d'un catalogue :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez le catalogue. L'onglet **Détails** dans le volet inférieur affiche les informations de version.
3. Sélectionnez **Modifier le niveau fonctionnel**. Si l'interface de gestion détecte que le catalogue doit modifier le niveau fonctionnel, elle affiche un message. Suivez les invites. Si une ou plusieurs machines ne peut pas être modifiée, un message explique pourquoi. Pour vérifier que toutes les machines fonctionnent correctement. nous vous recommandons de résoudre ces problèmes avant de cliquer sur **Modifier**.

Une fois la mise à niveau 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.
- Vous pouvez créer un catalogue vide par clonage. Lors du clonage de catalogues, vous pouvez définir le nombre de machines à zéro pour les catalogues provisionnés par MCS et ne pas ajouter de machines pour les catalogues non provisionnés par MCS.

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet 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.

Rôles requis

Pour créer et gérer des dossiers de catalogues, vous devez disposer de l'un des rôles intégrés par défaut suivants : Administrateur cloud, Administrateur complet ou Administrateur du catalogue de machines. Si nécessaire, vous pouvez personnaliser les rôles pour la création et la gestion des dossiers de catalogue. Pour plus d'informations, consultez la section Autorisations requises.

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 de **Configuration complète** (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. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet 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. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet 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. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet 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 catalogues.

Action	Autorisations requises
Créer des dossiers de catalogues	Créer dossier de catalogue de machines
Supprimer des dossiers de catalogues	Supprimer dossier de catalogue de machines
Déplacer des dossiers de catalogues	Déplacer dossier de catalogue de machines
Renommer des dossiers de catalogues	Modifier dossier de catalogue de machines
Déplacer des catalogues vers des dossiers	Modifier dossier de catalogue de machines et Modifier propriétés du catalogue de machines

Configurer la mise à niveau automatique pour les VDA

> **Important :**
>
> - Pour garantir une mise à niveau fluide, assurez-vous de respecter les prérequis et d'examiner les problèmes connus avant de procéder à la mise à niveau des VDA vers les versions CR ou LTSR CU. Voir Mettre à niveau les VDA à l'aide de l'interface Configuration complète.

> - Lors de la mise à niveau de VDA LTSR vers des versions de mise à jour cumulative (CU) LTSR, assurez-vous que la version des agents de mise à niveau du VDA exécutés sur les VDA est 7.36.0.7 ou ultérieure. Pour plus d'informations, consultez Mettre à niveau les VDA à l'aide de l'interface Configuration complète.
> - Vous pouvez basculer entre le VDA CR et le VDA LTSR à condition de passer d'une version antérieure à une version ultérieure. Vous ne pouvez pas passer d'une version ultérieure à une version antérieure, car cela est considéré comme une rétrogradation. Par exemple, vous ne pouvez pas passer de 2212 CR à 2203 LTSR (n'importe quelle CU), mais vous pouvez mettre à niveau de 2112 CR à 2203 LTSR (n'importe quelle CU).
> - Vous pouvez également mettre à niveau les VDA à l'aide de PowerShell. Consultez la section Mettre à niveau des VDA à l'aide de PowerShell.

Grâce à cette fonctionnalité, vous pouvez effectuer les opérations suivantes :

- Mettre à niveau les VDA par catalogue
- Modifier ou annuler une mise à niveau planifiée de VDA
- Configurer les paramètres de mise à niveau de VDA après la création
- Mettre à niveau les VDA par machine

> **Remarque :**
>
> - Lorsque vous planifiez des mises à niveau de VDA pour un catalogue, seuls les VDA du catalogue sur lesquels l'agent de mise à niveau VDA est installé peuvent être mis à niveau.
> - La mise à niveau d'un VDA échoue lorsque la machine est en mode maintenance ou lorsqu'une session est en cours d'exécution sur la machine.

Types de machines pris en charge

Cette fonctionnalité s'applique aux types de machines suivants :

- Machines persistantes provisionnées par MCS (jointes à AD, jointes à Azure AD et non jointes à un domaine). Vous les déployez à l'aide de l'option **Citrix Machine Creation Services** sur la page **Gestion des machines** lors de la création du catalogue.
- Machines Remote PC Access
- Citrix HDX Plus pour ordinateurs Windows 365
- Autres machines persistantes provisionnées à l'aide de services ou de technologies de provisioning autres que Citrix. Vous pouvez ajouter ces machines à DaaS à des fins de gestion à l'aide de l'option **Autre service ou technologie** sur la page **Gestion des machines** lors de la création du catalogue.

Pour plus d'informations sur les options **Citrix Machine Creation Services** et **Autre service ou technologie**, consultez la section Gestion des machines.

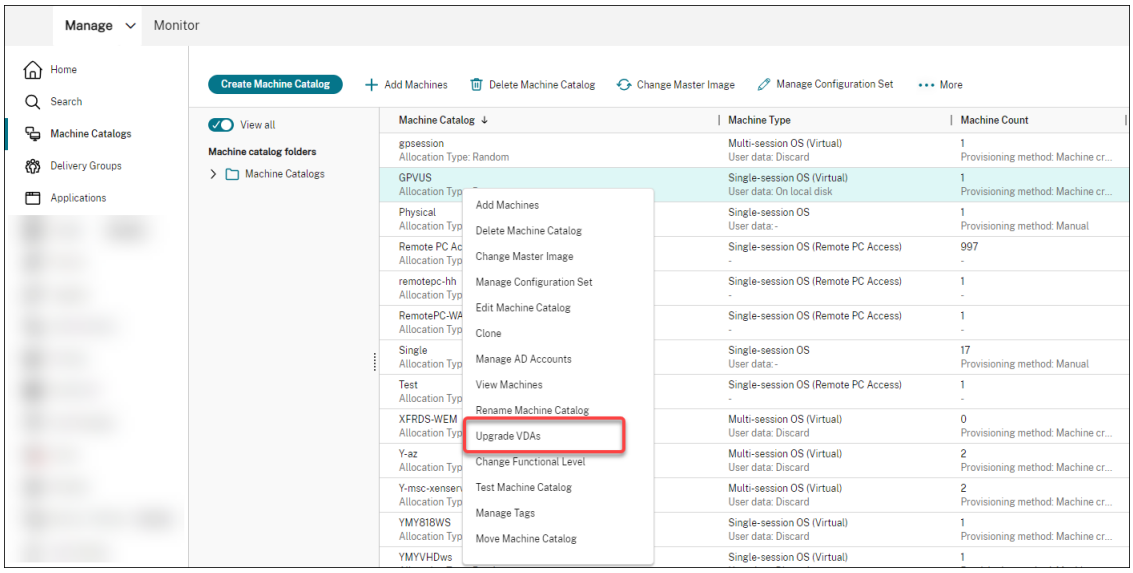
> **Remarque :**
>
> Pour les machines provisionnées par MCS, seules les machines statiques persistantes sont prises en charge. Les machines aléatoires ne sont pas prises en charge, même si elles sont persistantes.

Mettre à niveau les VDA par catalogue

> **Remarque :**
>
> Lorsque vous planifiez des mises à niveau de VDA pour un catalogue, n'oubliez pas que toutes les machines du catalogue seront incluses dans la mise à niveau. Nous vous recommandons donc de sauvegarder ces machines avant de lancer la mise à niveau.

Après avoir activé la mise à niveau de VDA pour un catalogue, vous pouvez mettre à niveau les VDA dans le catalogue immédiatement ou planifier des mises à niveau pour le catalogue. Pour ce faire, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines**.
2. Sélectionnez le catalogue, puis l'option **Mettre à niveau les VDA** dans le menu contextuel ou la barre d'actions. (Cliquez avec le bouton droit pour afficher le menu contextuel.) La fenêtre de mise à niveau du VDA s'affiche.



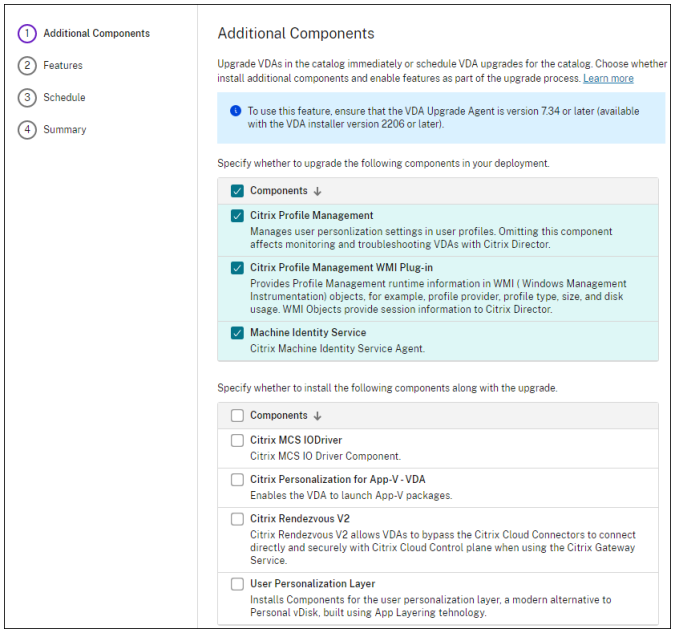
3. Choisissez si vous souhaitez mettre à niveau des composants supplémentaires dans votre déploiement. Vous pouvez également choisir d'installer certains composants en plus de la mise à niveau. Si un composant nécessite une configuration, vous devez cliquer sur le bouton **Configurer** et configurer les paramètres du composant pour continuer. Après la configuration, vous pouvez cliquer sur **Modifier** pour modifier la configuration.

Important :

- Pour utiliser la fonctionnalité des composants supplémentaires, assurez-vous que votre agent de mise à niveau VDA est à la version 7.34 ou ultérieure, incluse dans le programme d'installation du VDA version 2206 ou ultérieure.

Remarque :

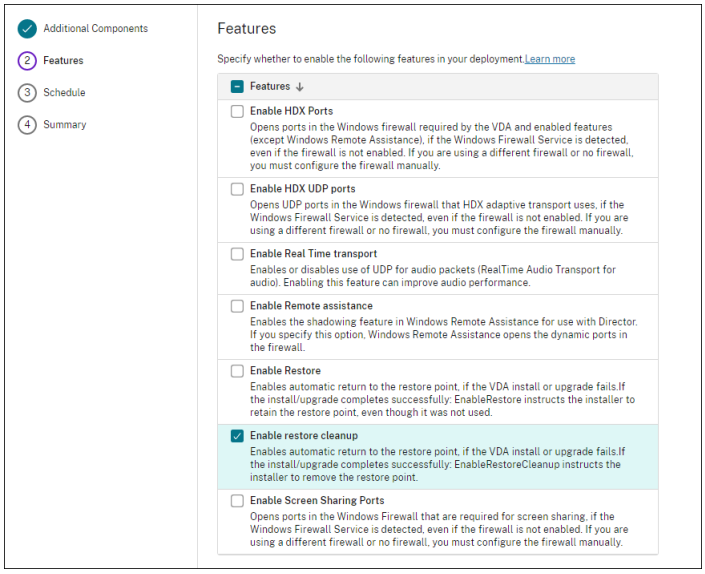
- Si vous choisissez de ne pas mettre à niveau un composant, celui-ci reste intact dans votre déploiement.
- Pour obtenir la liste complète des composants supplémentaires, consultez la section Installer des VDA.



4. Cliquez sur **Suivant**.
5. Choisissez si vous souhaitez activer l'une des fonctionnalités répertoriées. Cliquez sur **Suivant**.

Remarque :

Par défaut, la case **Activer le nettoyage de restauration** est cochée. Nous vous recommandons d'activer la fonctionnalité de restauration. Lorsque cette fonctionnalité est activée, un point de restauration du système est créé avant le début de la mise à niveau. Le point de restauration est supprimé une fois que l'installation du VDA a réussi. Pour plus d'informations, voir Restauration en cas d'échec de l'installation ou de la mise à niveau.



6. Choisissez de mettre à niveau les VDA immédiatement ou à une heure planifiée.

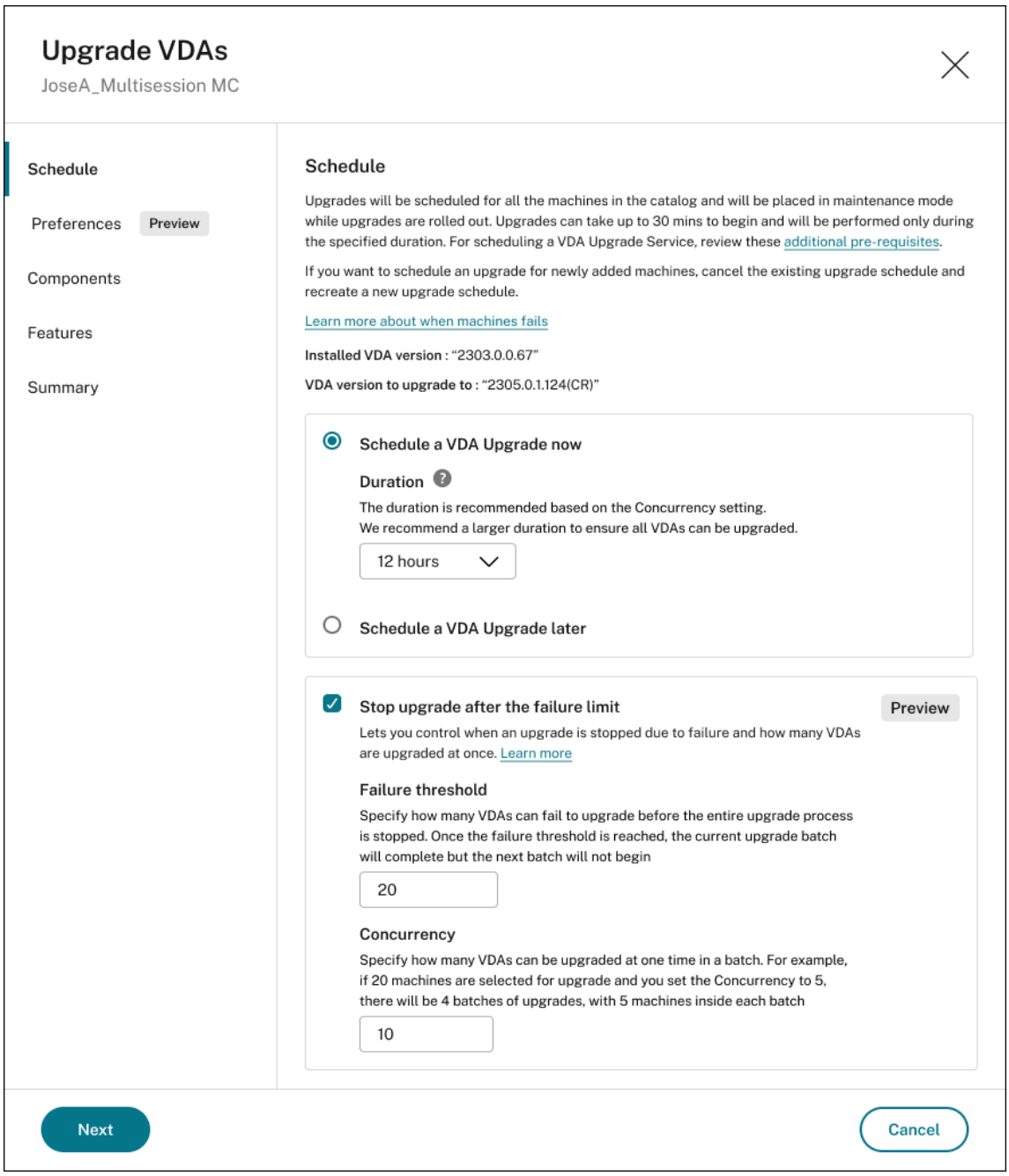
   - Pour mettre à niveau les VDA immédiatement, sélectionnez **Mettre à niveau maintenant**, puis spécifiez une durée.

     La durée est le délai, en heures, après lequel le service de mise à niveau VDA arrête d'initier des mises à niveau supplémentaires. Les mises à niveau en cours se poursuivront jusqu'à leur fin. Pendant ce temps, le DaaS commence à mettre à niveau les VDA dès qu'ils deviennent éligibles (par exemple, il n'y a plus aucune session active).

     Plus le nombre de VDA à mettre à niveau est élevé, plus cela prend du temps. Nous vous recommandons de sélectionner une valeur élevée (par exemple, 12 heures). Sinon, en fonction du nombre de VDA, il se peut que le DaaS ne puisse toujours pas mettre à niveau certains VDA dans ce délai.

   - Pour planifier les mises à niveau, sélectionnez **Mettre à niveau plus tard**, puis spécifiez quand vous souhaitez que les mises à niveau aient lieu.

     Vous pouvez planifier les mises à niveau uniquement pour les sept prochains jours. Les mises à niveau que vous planifiez s'appliquent uniquement aux machines qui figurent actuellement dans le catalogue. Si vous ajoutez des machines au catalogue ultérieurement mais que vous souhaitez également les mettre à niveau, annulez la mise à niveau planifiée, puis recréez une planification.



7. Sélectionnez l'option **Arrêter la mise à niveau après le dépassement de la limite du nombre d'échecs**.

> **Remarque :**
>
> Par défaut, la fonctionnalité est désactivée, mais elle demeure disponible pour les administrateurs.

Illustration du comportement

- Le seuil d'échecs et le niveau de simultanéité doivent être supérieurs à zéro.

- Le seuil d'échecs et le niveau de simultanéité doivent être inférieurs ou égaux au nombre total de machines dont la mise à niveau est planifiée

Seuil d'échecs	Niveau de simultanéité	Comportement
Spécifié	Non spécifié ou entrer 0	Les valeurs FailureThreshold et ConcurrencyLevel sont déterminées par l'équilibreur de charge comme précédemment.
Non spécifié ou entrer 0	Spécifié	La valeur par défaut de FailureThreshold est de 10 000 (nombre maximum de machines par catalogue) et la valeur de ConcurrencyLevel est utilisée pour le traitement par lots.
Non spécifié ou entrer 0	Non spécifié ou entrer 0	Le comportement par défaut s'applique aux niveaux de simultanéité mis à jour par l'équilibreur de charge.

8. Entrez la valeur **FailureThreshold**.

   > **Remarque :**
   >
   > Le seuil d'échecs est le nombre d'échecs au-delà duquel le VUS arrête toute installation de mise à niveau en attente à partir des lots suivants qui ne sont pas récupérés par l'agent de mise à niveau.

9. Entrez la valeur de **simultanéité**.

   > **Remarque :**
   >
   > La valeur de mise à niveau simultanée est le nombre de machines virtuelles qui peuvent être mises à niveau simultanément à tout moment au cours d'une fenêtre de mise à niveau.

10. Cliquez sur **Suivant**.
11. Vérifiez vos choix sur la page **Résumé**, puis cliquez sur **Terminer** pour appliquer vos paramètres et quitter la fenêtre.

> **Remarque :**
>
> - L'option **Mettre à niveau les VDA** n'est disponible qu'après avoir activé la mise à niveau de VDA pour le catalogue. Pour activer la mise à niveau de VDA, modifiez le catalogue.
> - Toutes les machines du catalogue sont placées en mode maintenance pendant le déploiement des mises à niveau. Les mises à niveau peuvent prendre jusqu'à 30 minutes et ne seront effectuées que pendant la période spécifiée.

Sur le nœud **Catalogues de machines**, la colonne **Mise à niveau de VDA** fournit des informations de mise à niveau de VDA pour le catalogue. Les informations suivantes peuvent apparaître :

> **Conseil :**
>
> Pour afficher la colonne **Mise à niveau de VDA**, sélectionnez **Colonnes à afficher** dans la barre d'actions, sélectionnez **Catalogue de machines > Mise à niveau de VDA**, puis cliquez sur **Enregistrer**.

- **Disponible** : une nouvelle version de VDA est disponible.
- **Programmé** : la mise à niveau de VDA a été planifiée.
- **Non configuré** : apparaît lorsque vous n'avez pas activé la mise à niveau de VDA pour le catalogue.
- **À jour** : les VDA du catalogue sont à jour.
- **Inconnu** : impossible d'obtenir les informations nécessaires à la mise à niveau de VDA. Les raisons possibles sont multiples :
  - Le VDA était utilisé pendant la mise à niveau.
  - Le nombre de mises à niveau en cours a atteint la limite maximale de 500.
  - L'agent de mise à niveau de VDA n'a pas répondu pendant la mise à niveau. Assurez-vous que l'agent s'exécute sur le VDA et peut communiquer avec Citrix DaaS.
  - Impossible d'effectuer des contrôles de validation de mise à niveau. Consultez la section Exigence de mise à niveau du VDA.

Vous pouvez également afficher l'état des mises à niveau de VDA pour un catalogue. Pour ce faire, cliquez sur le catalogue, puis vérifiez les informations **État de mise à niveau de VDA** dans l'onglet **Détails**. Les informations suivantes peuvent apparaître :

- **Non programmé** : vous avez activé la mise à niveau de VDA pour le catalogue, mais vous n'avez pas configuré de calendrier de mise à niveau.
- **Programmé** : vous avez créé un calendrier de mise à niveau pour le catalogue. Par exemple, si vous définissez la planification pour qu'elle commence à `09:00 PM, December 14, 2030`, les informations suivantes s'affichent : Programmé pour `December 14, 2030 09:00 PM UTC`.
- **En cours** : les mises à niveau de VDA ont commencé.

- **Annulé** : vous avez annulé la mise à niveau programmée.
- **Échec** : ce catalogue contient une ou plusieurs machines dont les mises à niveau de VDA ont échoué.
- **Succès** : tous les VDA du catalogue ont été mis à niveau avec succès.

Vous pouvez également résoudre les problèmes de mise à niveau de VDA à l'aide des actions recommandées pour un catalogue. Pour ce faire, cliquez sur le catalogue, puis sur l'onglet **Dépanner**.

Pour accéder rapidement aux catalogues ayant un état de mise à niveau VDA spécifique, vous pouvez utiliser des filtres. Pour plus d'informations, voir Utiliser la recherche dans l'interface de gestion Configuration complète.

Prenez en compte les informations suivantes :

- Le filtre **Mise à niveau de VDA** ou **État de mise à niveau de VDA** est disponible uniquement pour une utilisation avec les filtres suivants : **Nom** et **Catalogue de machines**.
- Lorsque vous utilisez le filtre **État de mise à niveau de VDA** ou **État de mise à niveau de VDA**, **Erreurs** et **Avertissements** dans le coin supérieur droit ne sont plus disponibles.

Modifier ou annuler une mise à niveau planifiée de VDA

Après avoir planifié les mises à niveau d'un catalogue, vous pouvez modifier ou annuler la mise à niveau programmée. Pour ce faire, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines**.
2. Sélectionnez le catalogue, puis **Modifier la mise à niveau planifiée de VDA** dans la barre d'actions. La fenêtre "Modifier la mise à niveau du VDA"s'affiche avec des informations sur la version du VDA installé et la version du VDA vers laquelle effectuer la mise à niveau.
3. Choisissez de modifier ou d'annuler la mise à niveau programmée.
    - Pour annuler la mise à niveau, cliquez sur **Annuler mise à niveau planifiée**. Rappel : L'annulation de la mise à niveau planifiée ne force pas l'arrêt de la mise à niveau en cours.
4. Cliquez sur **Terminé** pour quitter la fenêtre.

Configurer les paramètres de mise à niveau de VDA en modifiant un catalogue

Après la création du catalogue, vous pouvez configurer les paramètres de mise à niveau de VDA en modifiant le catalogue. Avant de commencer la modification, prenez en compte les points suivants :

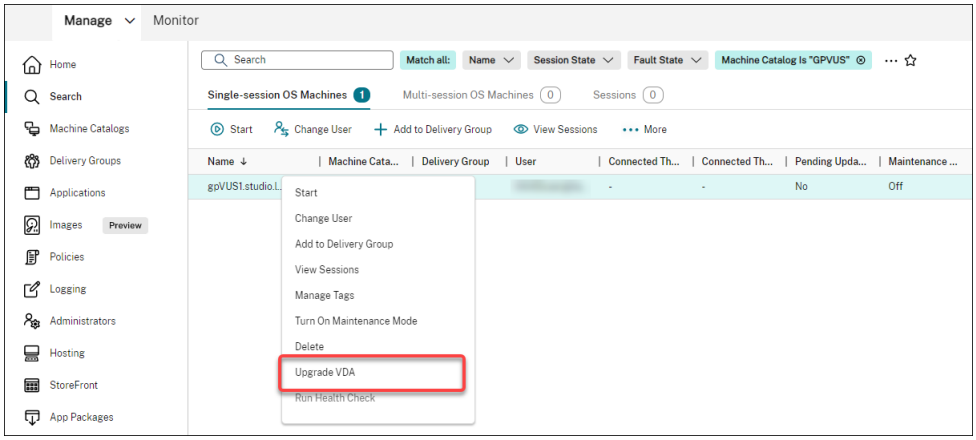
- Vérifiez que toutes les machines du catalogue se trouvent sur la même version VDA (CR ou LTSR). Sinon, certaines mises à niveau de VDA échoueront. Par exemple, si vous sélectionnez **Version LTSR de VDA la plus récente**, les mises à niveau CR de VDA échoueront.

- Les mises à niveau de certaines machines du catalogue ont peut-être commencé. Vous ne pouvez pas modifier les mises à niveau déjà en cours. Les mises à niveau en cours continuent. Celles qui n'ont pas encore démarré seront mises à niveau vers la version spécifiée.

Mettre à niveau les VDA par machine

Après avoir activé la mise à niveau de VDA pour un catalogue, vous pouvez mettre à niveau les VDA du catalogue un par un ou par lots. Pour ce faire, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Rechercher**.
2. Sélectionnez une ou plusieurs machines, puis l'option **Mettre à niveau le VDA** dans le menu contextuel ou la barre d'actions. (Cliquez avec le bouton droit pour afficher le menu contextuel.)



> **Remarque :**
>
> - Pour que l'option **Mettre à niveau le VDA** soit disponible, assurez-vous que vous avez activé la mise à niveau de VDA pour le catalogue dans lequel résident les machines sélectionnées et que l'agent de mise à niveau de VDA est installé sur ces machines. Pour activer la mise à niveau de VDA, modifiez le catalogue.
> - Les machines seront placées en mode de maintenance pendant le déploiement des mises à niveau. Le démarrage des mises à niveau peut prendre jusqu'à 30 minutes.
> - Si votre sélection contient des machines pour lesquelles les mises à niveau de VDA ne sont pas disponibles ou dont les mises à niveau sont en attente (programmées, en cours ou en attente de mises à niveau). Nous ignorerons les mises à niveau pour ces machines.

Sur le nœud **Rechercher**, vous pouvez ajouter la colonne **Mise à niveau de VDA**. Pour plus d'informations sur la façon d'ajouter une colonne personnalisée, voir Personnaliser les colonnes à afficher. La colonne est utile. Elle fournit des informations de mise à niveau de VDA pour la machine. Les informations suivantes peuvent apparaître :

- **Disponible** : une nouvelle version de VDA est disponible.
- **Programmé** : la mise à niveau de VDA a été planifiée.
- **Non configuré** : apparaît lorsque vous n'avez pas activé la mise à niveau de VDA pour la machine.
- **À jour** : le VDA est à jour.
- **Inconnu** : les informations sur la mise à niveau de VDA ne sont pas encore disponibles.

Vous pouvez également afficher l'état de la mise à niveau de VDA pour une machine. Pour ce faire, cliquez sur la machine, puis vérifiez les informations **État de mise à niveau de VDA** dans l'onglet **Détails**. Les informations suivantes peuvent apparaître :

- **Inconnu** : impossible d'obtenir les informations nécessaires à la mise à niveau de VDA. Les raisons possibles sont multiples :
  - Le VDA était utilisé pendant la mise à niveau.
  - Le nombre de mises à niveau en cours a atteint la limite maximale de 500.
  - L'agent de mise à niveau de VDA n'a pas répondu pendant la mise à niveau. Assurez-vous que l'agent s'exécute sur le VDA et peut communiquer avec Citrix DaaS.
  - Impossible d'effectuer des contrôles de validation de mise à niveau. Consultez la section Exigence de mise à niveau du VDA.
- **Programmé** : vous avez configuré un calendrier de mise à niveau. Par exemple, si vous définissez la planification pour qu'elle commence à `09:00 PM, December 14, 2030`, les informations suivantes s'affichent : Programmé pour `December 14, 2030 09:00 PM UTC`.
- **En attente de mise à niveau** : la machine est placée en mode de maintenance, en attente de mise à niveau. (Assurez-vous que les utilisateurs se sont déconnectés de leur session afin que la mise à niveau puisse continuer.)
- **En cours** : la mise à niveau de VDA a commencé.
- **Échec de la mise à niveau** : les tentatives de mise à niveau de VDA ont échoué.
- **Échec de la validation** : les tentatives de validation des paramètres de mise à niveau de VDA ont échoué.
- **Annulé** : la mise à niveau de la machine a été annulée.
- **Succès** : le VDA a été mis à niveau avec succès.

Vous pouvez également résoudre les problèmes de mise à niveau de VDA à l'aide des actions recommandées pour une machine. Pour ce faire, cliquez sur la machine, puis sur l'onglet **Dépanner**.

Pour accéder rapidement aux machines ayant un état de mise à niveau VDA spécifique, vous pouvez utiliser des filtres. Pour plus d'informations, voir Utiliser la recherche dans l'interface de gestion Configuration complète. Prenez en compte les informations suivantes :

- Le filtre **Mise à niveau de VDA** ou **État de mise à niveau de VDA** est disponible uniquement pour une utilisation avec les filtres suivants : **Nom** et **Catalogue de machines**.

- Lorsque vous utilisez le filtre **État de mise à niveau de VDA** ou **État de mise à niveau de VDA**, **Erreurs** et **Avertissements** dans le coin supérieur droit ne sont plus disponibles.

Gérer le jeu de configuration d'un catalogue

Avant de commencer, assurez-vous d'avoir configuré le déploiement de votre service WEM. Pour plus d'informations, consultez la rubrique Découvrez Workspace Environment Management Service.

> **Remarque :**
>
> Par défaut, si vous avez le rôle d'administrateur cloud, d'administrateur d'accès complet ou d'administrateur du catalogue de machines, vous pouvez gérer les jeux de configuration pour les catalogues. Si nécessaire, vous pouvez autoriser les rôles à gérer les jeux de configuration en leur accordant l'autorisation **Gérer les jeux de configuration**.

Lier un catalogue à un jeu de configuration

> **Important :**
>
> Si vos instances Citrix DaaS et du service WEM ne résident pas dans la même région, vous ne pouvez pas lier un catalogue à un jeu de configuration. Dans ce cas, migrez votre service WEM vers la même région que Citrix DaaS.

Pour lier un catalogue à un jeu de configuration, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines**.
2. Sélectionnez le catalogue de machines, puis **Gérer le jeu de configuration** dans la barre d'actions. La fenêtre **Gérer le jeu de configuration** apparaît.
3. Sélectionnez un jeu de configuration WEM auquel vous souhaitez lier le catalogue.

   > **Remarque :**
   >
   > Si le jeu de configuration sélectionné ne contient pas de paramètres relatifs à la configuration de base de WEM, l'option **Appliquer les paramètres de base au jeu de configuration** apparaît. Nous vous recommandons de sélectionner l'option permettant d'appliquer les paramètres de base au jeu de configuration.

4. Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Basculer vers un autre jeu de configuration

Pour passer à un autre jeu de configuration pour un catalogue, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines**.
2. Sélectionnez le catalogue de machines, puis **Gérer le jeu de configuration** dans la barre d'actions. La fenêtre **Gérer le jeu de configuration** apparaît.
3. Sélectionnez un autre jeu de configuration WEM auquel vous souhaitez lier le catalogue.
4. Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Annuler la liaison d'un catalogue avec le jeu de configuration

Pour annuler la liaison d'un catalogue avec le jeu de configuration, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines**.
2. Sélectionnez le catalogue de machines, puis **Gérer le jeu de configuration** dans la barre d'actions. La fenêtre **Gérer le jeu de configuration** apparaît.
3. Cliquez sur l'icône X située à droite du jeu de configuration sélectionné.
4. Cliquez sur **Enregistrer** pour enregistrer vos modifications.

Réessayer de créer un catalogue

> **Remarque :**
>
> Cette fonctionnalité s'applique uniquement aux catalogues MCS.

Les catalogues ayant échoué sont marqués d'une icône d'erreur. Pour en savoir plus, accédez à l'onglet **Dépannage** de chaque catalogue. Avant de réessayer de créer un catalogue, tenez compte des points suivants :

- Vérifiez d'abord les informations de dépannage et résolvez les problèmes. Les informations décrivent les problèmes détectés et fournissent des recommandations pour les résoudre.
- Vous ne pouvez pas modifier les paramètres associés à la gestion des systèmes d'exploitation et des machines. Le catalogue hérite ces paramètres de l'original.
- La création peut prendre un certain temps. Si nécessaire, sélectionnez **Masquer la progression** pour exécuter la création en arrière-plan.

Pour réessayer de créer un catalogue, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez le catalogue, puis accédez à l'onglet **Dépannage**.
3. Cliquez sur le lien hypertexte Réessayer pour réessayer de créer le catalogue.
4. Dans l'assistant qui apparaît, modifiez les paramètres si nécessaire. S'il n'est pas nécessaire d'apporter des modifications, vous pouvez accéder directement à la page **Résumé**.
5. Lorsque vous avez terminé, sélectionnez **Terminer** pour démarrer la création.

(VDA non provisionnés par Citrix uniquement) Générer et gérer des jetons d'inscription

Après avoir décidé d'activer l'inscription basée sur des jetons pour les machines non provisionnées par Citrix, vous devez générer des jetons par catalogue de machines, puis les partager avec les administrateurs d'installation de VDA.

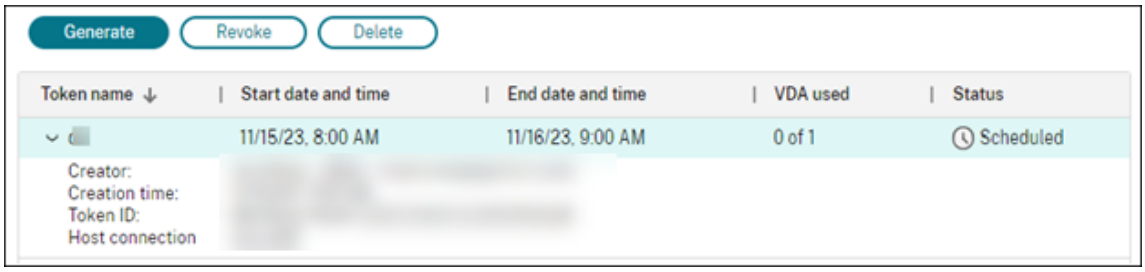
Un jeton d'inscription comporte les caractéristiques suivantes :

- Plage d'enregistrement : 1 à 100 machines VDA
- Période de validité : 1 heure à 14 jours

Pour générer un jeton pour un catalogue à l'aide de l'interface Configuration complète, procédez comme suit :

1. Dans **Configuration complète > Catalogues de machines**, recherchez un catalogue non provisionné par MCS, dont la colonne **Nombre de machines** affiche **Méthode de provisioning : Manuelle**.
2. Cliquez avec le bouton droit de la souris sur le catalogue, puis sélectionnez **Gérer les jetons d'inscription**.
3. Sur la page **Générer jeton d'inscription** qui s'affiche, fournissez les informations de jeton suivantes :
   - Entrez un nom pour le jeton.
   - Entrez sa période de validité. La période doit être comprise entre une heure et 14 jours. Le jeton n'est valide que pour la période spécifiée.
   - (Facultatif) Sélectionnez une connexion hôte pour la gestion de l'alimentation des VDA inscrits avec le jeton. Les options incluent toutes les connexions hôtes dans la zone du catalogue.
   - Entrez les limites d'utilisation des jetons (entre 1 et 100).
4. Cliquez sur **Générer**.
5. Dans la fenêtre **Jeton généré avec succès** qui s'affiche, copiez le jeton et enregistrez-le en lieu sûr, ou cliquez sur **Télécharger** pour le télécharger dans le dossier **Téléchargements**.

   Un enregistrement de jeton apparaît dans la liste des jetons.



6. Partagez le jeton avec les administrateurs d'installation du VDA.

   Pour plus d'informations sur l'installation d'un VDA et d'un jeton sur des machines, consultez la section Installer des VDA.

Gérer les jetons

Deux options s'offrent à vous pour révoquer un jeton et le rendre indisponible pour l'inscription de VDA :

- Révoquer : révoquez le jeton, mais conservez-le dans la liste à des fins de journalisation.
- Supprimer : révoquez le jeton et supprimez-le de la liste.

> **Remarque :**
>
> Les jetons expirés sont automatiquement supprimés au bout de 14 jours.

Utiliser PowerShell

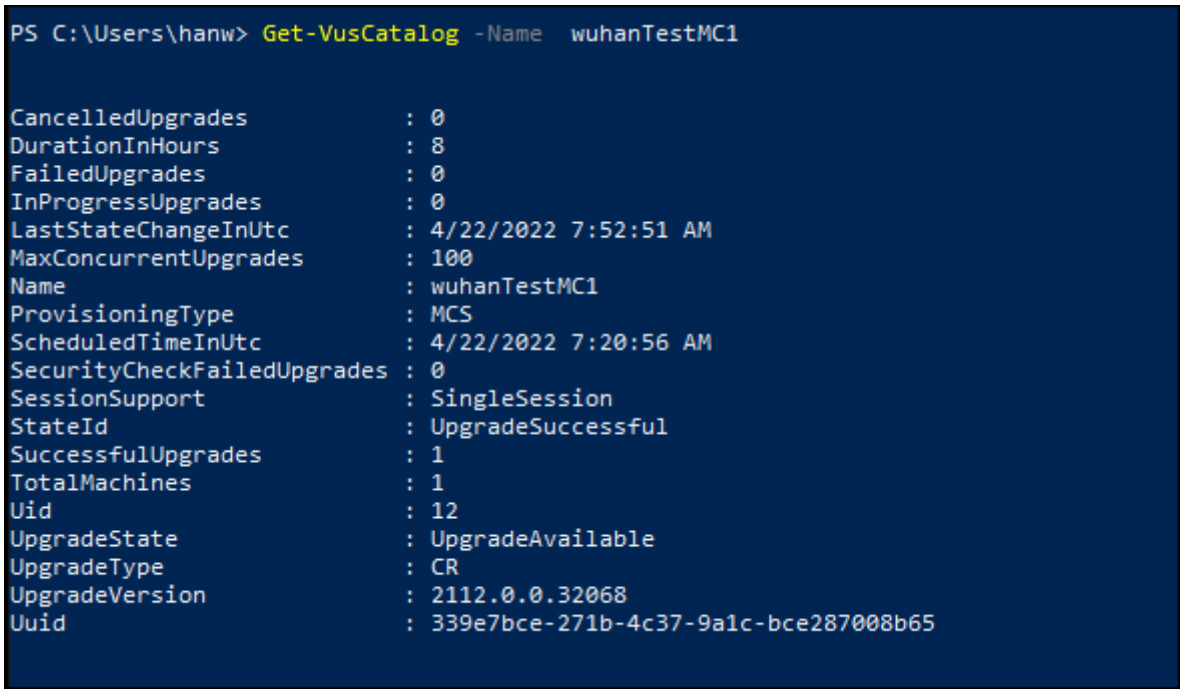
Cette section explique comment gérer les catalogues à l'aide de PowerShell :

- Utiliser PowerShell pour vérifier l'état de mise à niveau du VDA et la version du VDA
- Gérer le numéro de séquence du nom de la machine
- Activer le calendrier de redémarrage unique
- Ajouter des descriptions à une image
- Réinitialiser le disque d'OS
- Réparer les informations d'identité des comptes d'ordinateur actifs
- Modifier le paramètre réseau d'un catalogue de machines existant
- Gérer les versions d'un catalogue de machines
- Modifier la configuration du cache d'un catalogue de machines existant
- Convertissez un catalogue de machines non basé sur un profil de machine vers un catalogue de machines basé sur un profil de machine
- Récupérer les erreurs et les avertissements associés à un catalogue
- Supprimer des machines sans accès à l'hyperviseur
- Prise en charge des mises à jour du VDA via l'accès au partage de fichiers local

Utiliser PowerShell pour vérifier l'état de mise à niveau du VDA et la version du VDA

Utilisez la commande PowerShell `Get-VusCatalog` pour vérifier l'état de mise à niveau du VDA. Supposons que le nom du catalogue soit `wuhanTestMC1`. Vous pouvez taper ce qui suit dans l'invite de commandes :

- `PS C:\> Get-VusCatalog -Name wuhanTestMC1`



Dans cet exemple, `UpgradeState` est `UpgradeAvailable`, ce qui signifie que la mise à niveau du VDA est activée pour le catalogue. `StateId` est `UpgradeSuccessful`, ce qui signifie que le catalogue a été correctement mis à niveau vers la version 2112.0.0.32068 (`UpgradeVersion`).

Utilisez la commande PowerShell `Get-BrokerMachine` pour obtenir la version actuelle du VDA.


```
SessionProtocol              :
SessionSecureIcaActive       :
SessionSmartAccessTags       :
SessionStartTime             :
SessionState                 :
SessionStateChangeTime       :
SessionSupport               : MultiSession
SessionType                  :
SessionUid                   :
SessionUserName              :
SessionUserSID               :
SessionsEstablished          : 0
SessionsPending              : 0
SummaryState                 : Unregistered
SupportedPowerActions        : {}
Tags                         : {}
UUID                         : 9c0c4623-a4dc-44f9-ae4b-54c86cc76a7f
Uid                          : 4
VMToolsState                 : NotPresent
WillShutdownAfterUse         : False
WillShutdownAfterUseReason   : None
WindowsConnectionSetting     : LogonEnabled
ZoneHealthy                  : False
ZoneName                     : My Resource Location
ZoneUid                      : ae0366c2-3001-459d-89ff-0b159c9d436d

AgentVersion                 : 2112.0.0.32068
AllocationType               : Static
ApplicationsInUse            : {}
AssignedClientName           :
AssignedIPAddress            :
AssignedUserSIDs             : {}
AssociatedTenantId           :
AssociatedUserFullNames      : {}
AssociatedUserNames          : {}
AssociatedUserSIDs           : {}
AssociatedUserUPNs           : {}
AzureADJoinedMode            : NotAadJoined
BrowserName                  :
Capabilities                 : {}
CatalogName                  : wuhanTestMC1
CatalogUUID                  : 339e7bce-271b-4c37-9a1c-bce287008b65
CatalogUid                   : 12
CbpVersion                   :
ColorDepth                   :
ControllerDNSName            :
DNSName                      : wuhanVUSTest02.WHCloud.Internal
DeliveryType                 :
Description                  :
DesktopConditions            : {}
```

Utilisez la commande PowerShell `Get-VusAvailableVdaVersion` pour obtenir la dernière version du VDA.

```
PS C:\Users\hanw> Get-VusAvailableVdaVersion

UpgradeType Version
----------- -------
         CR 2203.0.0.33220
       LTSR 2203.0.0.33220
```


Gérer le numéro de séquence du nom de la machine

Pour personnaliser le numéro de séquence des machines déployées à l'aide de MCS, via les commandes PowerShell, procédez comme suit :

1. Ouvrez Powershell en tant qu'administrateur sur le Delivery Controller.
2. Exécutez la commande `asnp citrix*` pour charger les modules Citrix.
3. Exécutez la commande suivante pour vérifier le nombre de démarrages pour le pool d'identités du catalogue :

   ```
   Get-AcctIdentityPool -IdentityPoolName xxx
   <!--NeedCopy-->
   ```

   L'élément `IdentityPoolName` est le nom du catalogue.
4. Si vous souhaitez définir ce nombre sur une valeur différente, exécutez la commande suivante et spécifiez l'élément StartCount sous la forme X :

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount X
   <!--NeedCopy-->
   ```
5. Ajoutez les machines au catalogue selon le nombre requis.
6. Une fois les machines créées, exécutez la commande suivante pour rétablir la valeur initiale Y :

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount Y
   <!--NeedCopy-->
   ```

Activer le programme 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`

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.


```
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.

```
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 **Ancien nom** avec **Nouveau nom**.

```
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**.

```
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.

```
Set-BrokerCatalogRebootSchedule -Name Accounting
-WarningMessage "Save your work"
-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
<!--NeedCopy-->
```

- Pour afficher tous les programmes de redémarrage désactivés, puis activer tous les programmes de redémarrage désactivés.


```
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.

```
Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
    %m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
<!--NeedCopy-->
```

- Pour configurer le fuseau horaire du catalogue nommé **MyCatalog**.

```
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. Cette fonctionnalité est utile pour les administrateurs qui souhaitent ajouter des étiquettes descriptives lors de la mise à jour d'une image principale utilisée par un catalogue, par exemple, *Office 365 installé*. Utilisez les commandes suivantes pour ajouter ou afficher des descriptions d'images :

- `NewProvScheme`. Un nouveau paramètre, `masterImageNote`, vous permet d'ajouter une note à une image. Par exemple :

```
C:\PS>New-ProvScheme -ProvisioningSchemeName XenPS -HostingUnitName
    XenHu -IdentityPoolName idPool1 -MasterImageVM XDHyp:\HostingUnits\
    XenHU\Base.vm\Base.snapshot -MasterImageNote "Office365 installed"
<!--NeedCopy-->
```

- `Publish-ProvMasterVMImage`. Utilisez ce paramètre pour publier la note. Par exemple :

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName MyScheme -
    MasterImageVM XDHyp:\HostingUnits\HostUnit1\RhoneCC_baseXP.vm\base.
    snapshot -MasterImageNote "Visual Studio 2019 installed"
<!--NeedCopy-->
```

- `Get-ProvSchemeMasterVMImageHistory`. Affichez des informations sur chaque image. Par exemple :


```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall

VMImageHistoryUid : 3cba3a75-89cd-4868-989b-27feb378fec5

ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42

ProvisioningSchemeName : MyScheme

MasterImageVM : /Base.vm/base.snapshot

Date : 17/05/2021 09:27:50

MasterImageNote : Office365 installed
<!--NeedCopy-->
```

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 s'applique aux environnements de virtualisation Azure, Google Cloud, SCVMM, VMware et XenServer.

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.

   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-->
```


> **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.

5. Exécutez `Get-ProvTask` pour obtenir l'état des tâches renvoyées par la commande `Reset-ProvVMDisk`.

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 les informations d'identité

Pour réinitialiser les informations d'identité, procédez comme suit :

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 :

```
1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
       PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
       $password -Target IdentityInfo
2  <!--NeedCopy-->
```


Description 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 Azure AD).
- `PrivilegedUserPassword` : mot de passe pour PrivilegedUserName.
- `Target` : cible de l'action de réparation. Le paramètre IdentityInfo peut réparer le mot de passe/la clé de confiance du compte, et le paramètre UserCertificate peut réparer les attributs du certificat utilisateur des identités de machines jointes à Azure AD hybride.

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name
    > -Identity -ResetIdentityInfo
<!--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 Citrix DaaS uniquement)
- Clés de confiance uniquement : si la machine virtuelle n'est pas jointe au domaine AD (pour Citrix DaaS uniquement)
- Mot de passe uniquement : si la machine virtuelle est jointe au domaine AD (pour Citrix Virtual Apps and Desktops uniquement)

- Pour réinitialiser toutes les configurations du disque d'identité, exécutez ces commandes dans l'ordre suivant :

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
    PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
    $password -Target IdentityInfo
<!--NeedCopy-->
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
     -Identity
<!--NeedCopy-->
```

4. Tapez **y** pour confirmer l'action. Vous pouvez également ignorer l'invite de confirmation à l'aide du paramètre `-Force`. Par exemple :

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
    Identity -Force
<!--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 le paramètre réseau d'un catalogue de machines existant

Vous pouvez modifier le paramètre réseau d'un schéma de provisioning existant afin de créer les nouvelles machines virtuelles sur le nouveau sous-réseau. Utilisez le paramètre `-NetworkMapping` dans la commande `Set-ProvScheme` pour modifier le paramètre réseau.

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.

Modifier la configuration du cache d'un catalogue de machines existant

Après avoir créé un catalogue non persistant avec MCSIO activé, vous pouvez exécuter 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 :

```
1  New-ProvScheme -ProvisioningSchemeName $CatalogName -
       HostingUnitUid $HostingUnitUid `
2  -IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
3  -MasterImageVM $MasterImage `
4  -ServiceOffering $ServiceOffering `
5  -NetworkMap $NetworkMap `
6  -SecurityGroup $SecurityGroup `
7  -UseWriteBackCache -WriteBackCacheDiskSize 8
8  <!--NeedCopy-->
```

Modifier la configuration du cache

Exécutez la commande `Set-ProvScheme`. Par exemple :

```
1  Set-ProvScheme -ProvisioningSchemeName $provScheme.
       ProvisioningSchemeName -WriteBackCacheDisk32 -
       WriteBackCacheMemorySize 128
2  <!--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.

Convertir un catalogue de machines non basé sur un profil de machine en 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 prennent les valeurs de propriété du profil de la machine.

> **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 :

     ```
     1  Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
           -MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
           machineprofile.folder<ResourceGroupName><TemplateSpecName
           ><VersionName>
     2  <!--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-->
```

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.

Supprimer des machines sans accès à l'hyperviseur

Lors de la suppression d'une machine virtuelle ou d'un schéma de provisioning, MCS doit supprimer les balises de la machine virtuelle, et parfois également du disque de base, afin que les ressources incluses dans les options de suppression ne soient plus suivies ou identifiées par MCS. Cependant, certaines de ces ressources ne sont accessibles que via l'hyperviseur. Utilisez l'option `PurgeDBOnly` du PowerShell `Remove-ProvVM` pour supprimer de la base de données les objets de ressources de machine virtuelle tels que la machine virtuelle, le disque de base, l'image dans ACG, etc., même si vous n'avez pas accès à l'hyperviseur.

Cette option est activée sur :

- Tous les hyperviseurs pris en charge
- Les machines virtuelles persistantes et non persistantes

Limitations

Vous ne pouvez pas utiliser les commandes -PurgeDBOnly et -ForgetVM en même temps.

Utiliser la commande PurgeDBOnly

Lors de l'exécution de la commande PowerShell `Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -ForgetVM`, l'opération de suppression peut échouer dans les scénarios suivants :

- La connexion hôte est en mode maintenance
- Informations d'identification non valides
- Échec de l'authentification
- Opération non autorisée

- L'hyperviseur est inaccessible

> **Remarque :**
>
> Remove-provVM -ForgetVM cible uniquement les machines virtuelles persistantes. Si l'une des machines virtuelles de la liste n'est pas persistante, l'opération échoue.

Lorsque l'opération échoue parce que l'hyperviseur est inaccessible, l'invite suivante s'affiche :

```
Try to use -PurgeDBOnly option to clean DDC database.
```

Utilisez l'option `-PurgeDBOnly` dans la commande PowerShell `Remove-ProvVM` pour supprimer les références à une machine virtuelle dans la base de données MCS. Par exemple,

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -
PurgeDBOnly
```

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

Logiciels requis

- 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)
- Remote PowerShell SDK version 7.42 ou ultérieure (publié après le 16 février 2024)

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 avec l'état `Power State Unknown`, reportez-vous à CTX131267 pour obtenir des conseils.
- 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.
- Si un Cloud Connector ne fonctionne pas correctement, les opérations de provisioning MCS (telles que les mises à jour de catalogue) prennent beaucoup plus de temps que d'habitude et les performances de la console de gestion se dégradent considérablement.

Autres ressources

Pour plus d'informations sur la gestion de catalogues d'hyperviseurs spécifiques, consultez :

Gérer un catalogue AWS

January 25, 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 sur les ressources suivantes :

- Machine virtuelle
- Volume du disque racine
- Volume du disque d'identité
- Interface réseau élastique (ENI)
- 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 les machines virtuelles et les balises créées par Citrix d'une seule machine virtuelle ou d'une liste de machines d'un catalogue.

> **Remarque :**
>
> Avec le paramètre `ForgetVM`, les machines virtuelles sont supprimées de la base de données du schéma de provisionning de Citrix, mais elles demeurent tout de même dans l'hyperviseur.

- `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.

Pour ce faire :

1. Ouvrez une fenêtre **PowerShell**.
2. Exécutez `asnp citrix*` pour charger des modules PowerShell spécifiques 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 et des balises créées par Cirix des ressources.

   - Exécutez `Remove-ProvVM` avec `ForgetVM` pour supprimer des machines virtuelles de la base de données Citrix et des balises des 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 créées par Citrix sont désormais supprimées. Les balises créées par Citrix sont supprimées des ressources suivantes :

      - Machine virtuelle
      - Volume du disque racine

- Volume du disque d'identité
- Interface réseau élastique

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 de la plateforme AWS. Les balises du tableau sont représentées au format "clé":"valeur".

Nom de la ressource	Balise
Disque d'identification	"Name": "VMName_IdentityDisk" "XdConfig": "XdProvisioned=true" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Image	"XdConfig": "XdProvisioned=true" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Interface réseau élastique	"Description": "XD Nic" "XdConfig": "XdProvisioned=true" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disque OS	"Name": "VMName_rootDisk" "XdConfig": "XdProvisioned=true" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" [when AwsCaptureInstanceProperties = true] "Citrix Resource": ""

Nom de la ressource	Balise
Machine virtuelle de préparation	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “Name”: “Preparation - CatalogName - xxxxxxxxxx” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true] “Citrix Resource”: “”
Instantané publié	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “XdConfig”: “XdProvisioned=true” S’il ne s’agit pas d’un instantané pour AMI travailleur de volume, alors “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Modèle	[when AwsCaptureInstanceProperties = true] “XdConfig”: “XdProvisioned=true” [when AwsCaptureInstanceProperties = true] “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [when AwsCaptureInstanceProperties = true] “CitrixResource”: “”
VM dans le catalogue	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “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”

Nom de la ressource	Balise
	[when AwsCaptureInstanceProperties = true and AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “XdConfig”: “XdProvisioned=true”
AMI travailleur de volume	
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” “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 Google Cloud Platform

February 13, 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.

Ajouter des machines à un catalogue

Pour ajouter des machines à un catalogue, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez le catalogue de machines auquel vous souhaitez ajouter des machines.
3. Sélectionnez **Ajouter des machines** dans la barre d'actions.
4. Sur la page **Machines virtuelles**, spécifiez le nombre de machines que vous souhaitez ajouter, puis sélectionnez **Suivant**.
5. Sur la page **Identités des machines**, sélectionnez un compte Active Directory, puis **Suivant**.
6. 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**.
7. Sur la page **Résumé**, vérifiez les informations et sélectionnez **Terminer**.

Mettre à jour les machines

Cette fonctionnalité peut être utile dans les cas où vous souhaitez mettre à jour votre image principale ou le niveau fonctionnel minimum.

Pour mettre à jour des machines, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez le catalogue de machines qui contient les machines que vous souhaitez mettre à jour.
3. Sélectionnez **Modifier image principale** dans la barre d'actions.
4. Sur la page **Image**, sélectionnez une MV et le niveau fonctionnel minimum pour le catalogue, puis sélectionnez **Suivant**.
5. Sur la page **Stratégie de déploiement**, spécifiez quand vous souhaitez mettre à jour les machines, puis sélectionnez **Suivant**.
6. Sur la page **Résumé**, vérifiez les informations et sélectionnez **Terminer**.

Restaurer la mise à jour d'une machine

Pour restaurer une mise à jour de machine, procédez comme suit :

> **Important :**

> Ne renommez, supprimez ou déplacez pas les images principales. Sinon, vous ne pouvez pas restaurer la mise à jour.

1. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
2. Sélectionnez le catalogue de machines dans lequel vous souhaitez restaurer la mise à jour de la machine.
3. Sélectionnez **Restaurer image principale** dans la barre d'actions.
4. Sur la page **Aperçu**, vérifiez les informations, puis sélectionnez **Suivant**.
5. Sur la page **Stratégie de déploiement**, configurez la stratégie de déploiement, puis sélectionnez **Suivant**.
6. Sur la page **Résumé**, vérifiez les informations et sélectionnez **Terminer**.

Gestion de l'alimentation

Citrix DaaS vous permet de gérer l'alimentation des machines Google Cloud. 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 :

- 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, les mises à jour de propriétés prises en charge par cette fonctionnalité sont le profil de machine, l'offre de services et les paramètres de catalogue personnalisés.

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,

   - Mise à jour du profil de machine

```
`Set-ProvScheme –ProvisioningSchemeName "my-catalog" –
   MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
   machineprofileinstance.vm"
<!--NeedCopy-->
```

   - Mise à jour de l'offre de services

```
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-->
```

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-->
```

> **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.

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 de la plate-forme GCP. Les balises du tableau sont représentées au format "clé":"valeur".

Nom de la ressource	Balise
Disque d'identification	"CitrixResource": "internal" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Image	"CitrixResource": "internal" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Nom de la ressource	Balise
Disque OS	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
machine virtuelle de préparation	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Instantané publié	“CitrixResource”: “internal”
Bucket de stockage	“CitrixResource”: “internal”
Modèle	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
machine virtuelle dans le catalogue	“CitrixResource”: “internal” “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” 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

May 17, 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. Consultez Créer un catalogue de machines HPE Moonshot.

Gestion de l'alimentation

Citrix DaaS 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 les catalogues de machines

Gérer un catalogue Microsoft Azure

May 17, 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.
> - Une machine virtuelle peut mettre un peu plus de temps à démarrer après que vous avez modifié le type de stockage vers un niveau inférieur.

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 appliquer `StorageTypeAtShutdown` aux nouvelles machines virtuelles ajoutées à un catalogue existant.

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> '

$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName

Set-ProvScheme -ProvisioningSchemeName $ProvScheme.
   ProvisioningSchemeName -CustomProperties $customProperties
<!--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 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.

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
<!--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`.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. Mettez à jour les machines virtuelles existantes pour activer `StorageTypeAtShutdown`.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    StartsNow -DurationInMinutes -1
<!--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 démarrage :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName vm1 -StartsNow -DurationInMinutes 120
```



```
2 <!--NeedCopy-->
```

- Pour planifier une mise à jour un week-end :

```
1 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
    catalog" -VMName "vm1" -StartTimeInUTC "10/15/2022
    9:00am" -DurationInMinutes (New-TimeSpan -Days 2).
    TotalMinutes
2 <!--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.

```
1 Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
2 <!--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.

Modifier le cryptage des disques

Vous pouvez modifier le cryptage des disques dans les environnements de virtualisation Azure et effectuer les actions suivantes :

- Créer un catalogue de machines MCS avec un jeu de cryptage de disque (DES) différent de celui de l'image principale à l'aide de la commande `New-ProvScheme`. Par exemple :

```
$customProperties = @"
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/>
</CustomProperties>
"@
New-ProvScheme -CleanOnBoot `
-ProvisioningSchemeName $provisioningSchemeName `
-HostingUnitName $hostingUnitName `
-IdentityPoolName $identityPoolName `
-InitialBatchSizeHint $numberOfVms `
-masterImagePath $masterImagePath `
-NetworkMapping $networkMapping `
-CustomProperties $customProperties
<!--NeedCopy-->
```

- Modifier le type de cryptage des disques en remplaçant une clé DES par une autre clé DES d'un catalogue de machines MCS existant et de machines virtuelles existantes à l'aide des commandes `Set-ProvScheme` et `Set-ProvVMUpdateTimeWindow`. Après avoir redémarré les machines virtuelles, vous constaterez que la clé DES a été mise à jour. 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="DiskEncryptionSetId" Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/providers/Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Mettre à jour un catalogue de machines MCS et une machine virtuelle qui n'étaient pas initialement compatibles avec l'utilisation de clés CMEK afin qu'ils disposent d'un cryptage par clé de cryptage gérée par le client (CMEK) (DES), d'un cryptage de disque sur l'hôte ou d'un cryptage double, en exécutant les commandes `Set-ProvScheme` et `Set-ProvVMUpdateTimeWindow`. Pour plus d'informations sur les différents types de cryptage, consultez Cryptage côté serveur Azure, Cryptage de disque sur l'hôte Azure et Cryptage double sur disque géré.

- Mettre à jour un catalogue de machines MCS et des machines virtuelles initialement cryptés afin de supprimer le cryptage, en exécutant les commandes `Set-ProvScheme` et `Set-ProvVMUpdateTimeWindow`. 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="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
    -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Activer le cryptage de disque avec un point de terminaison privé (un catalogue de machines MCS utilisant une connexion hôte pour laquelle `ProxyHypervisorTrafficThroughConnector` est activé). Pour plus d'informations sur `ProxyHypervisorTrafficThroughConnector`, consultez Créer un environnement sécurisé pour le trafic géré par Azure. Pour plus d'informations sur l'activation du cryptage de disque avec des points de terminaison privés, consultez Activer le cryptage de disque avec un point de terminaison privé.

Activer le cryptage de disque avec un point de terminaison privé

Actuellement, la limitation d'Azure ne vous permet pas d'utiliser le cryptage côté serveur avec des clés gérées par le client pour les points de terminaison privés. Toutefois, vous pouvez mettre à jour un catalogue de machines MCS et des machines virtuelles pour crypter les points de terminaison avec une clé DES.

Mettre à jour un catalogue de machines avec des points de terminaison privés Voici la procédure détaillée pour mettre à jour un catalogue de machines avec des points de terminaison privés :

1. Créez un catalogue sans cryptage de disque via `ProxyHypervisorTrafficThroughConnector`. Pour plus d'informations sur `ProxyHypervisorTrafficThroughConnector`, consultez Créer un environnement sécurisé pour le trafic géré par Azure.
2. Exécutez `Set-ProvScheme` pour mettre à jour le catalogue avec `DiskEncryptionSetId`.

> **Remarque :**
>
> Vous pouvez configurer `DiskEcryptionSetId` via `CustomProperties` ou `MachineProfile`. Lorsque vous le définissez à la fois dans `CustomProperties` et `MachineProfile`, les propriétés définies dans `CustomProperties` sont appliquées.

Exemple avec l'utilisation de `CustomProperties` :

```
$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/456c683e2ed7/resourceGroups/testrg/
    providers/Microsoft.Compute/diskEncryptionSets/
    diskEncryptionSet1"/>
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
<!--NeedCopy-->
```

Exemple avec l'utilisation de MachineProfile : utilisez une machine virtuelle sur laquelle le cryptage de disque est activé ou qui dispose d'une spécification de modèle avec des paramètres de cryptage de disque :

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
    folder\testrg.resourcegroup\new-template.vm"
<!--NeedCopy-->
```

Vous pouvez également mettre à jour un profil de machine à l'aide de l'interface Configuration complète.

3. Exécutez `Set-ProvVMUpdateTimeWindow` pour mettre à jour les machines virtuelles du catalogue. Par exemple :

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. Après avoir redémarré les machines virtuelles, vous constaterez que le cryptage de disque a été mis à jour sur les disques de la machine virtuelle dans le portail Azure.
5. Avant d'ajouter de nouvelles machines virtuelles au catalogue, désactivez le cryptage de disque en exécutant la commande `Set-ProvScheme`.

   > **Remarque :**
   >
   > Cette étape est obligatoire parce que vous mettez à jour un catalogue de points de terminaison privés. Si vous ne procédez pas à cette étape, des erreurs s'afficheront lorsque vous tenterez d'ajouter de nouvelles machines virtuelles au catalogue.

   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="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. Ajoutez des machines virtuelles au catalogue.

Mettre à jour des machines virtuelles individuelles du catalogue Voici la procédure détaillée pour mettre à jour des machines virtuelles individuelles du catalogue :

1. Créez un catalogue sans cryptage de disque via `ProxyHypervisorTrafficThroughConnector`. Pour plus d'informations sur `ProxyHypervisorTrafficThroughConnector`, consultez Créer un environnement sécurisé pour le trafic géré par Azure.
2. Exécutez `Set-ProvVM` pour mettre à jour la machine virtuelle du catalogue avec `DiskEncryptionSetId`.

   > **Remarque :**
   >
   > Vous pouvez configurer `DiskEcryptionSetId` via `CustomProperties` ou `MachineProfile`.

   Exemple avec l'utilisation de `CustomProperties` :

   ```
   $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/456c683e2ed7/resourceGroups/testrg/
       providers/Microsoft.Compute/diskEncryptionSets/
       diskEncryptionSet1" />
   </CustomProperties>'
   Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
       CustomProperties $customProperties
   <!--NeedCopy-->
   ```

   Exemple avec l'utilisation de MachineProfile :

   ```
   Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
       MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
       folder\testrg.resourcegroup\new-template.vm"
   <!--NeedCopy-->
   ```

3. Exécutez `Set-ProvVMUpdateTimeWindow` pour mettre à jour les machines virtuelles du catalogue. Par exemple :

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
       VMName azu01 -StartsNow -DurationInMinutes -1
   ```



```
<!--NeedCopy-->
```

4. Après avoir redémarré les machines virtuelles, vous constaterez que le cryptage de disque a été mis à jour sur les disques de la machine virtuelle dans le portail Azure.
5. Ajoutez des machines virtuelles au catalogue.

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-->
```


Récupérer les informations de nom de région pour les machines virtuelles Azure, les disques gérés, les instantanés, le disque dur virtuel Azure et les modèles ARM

Vous pouvez afficher les informations de nom de région pour une machine virtuelle Azure, des disques gérés, des instantanés, un disque dur virtuel Azure et des modèles ARM. Ces informations sont affichées pour les ressources de l'image principale lorsqu'un catalogue de machines est affecté. Une propriété PowerShell appelée `RegionName` affiche les informations relatives au nom de la région lorsque vous exécutez la commande PowerShell avec le paramètre `AdditionalData`.

Par exemple, utilisez la commande PowerShell suivante pour obtenir des informations sur une machine virtuelle dans Azure.

```
PS C:\Windows\system32> (get-item XDHyp:\HostingUnits\myAzureNetwork\
    image.folder\hu-dev-testing-rg.resourcegroup\hu-dev-tsvda.vm).
    AdditionalData
Key Value
HardDiskSizeGB 127
ResourceGroupName HU-DEV-TESTING-RG
RegionName East US
TemplateIsWindowsTemplate True
LicenseType
ServiceOfferingDescription Standard_B2ms
ServiceOfferingMemory 8192
ServiceOfferingCores 2
SupportedMachineGenerations Gen1,Gen2
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SecurityType
SecureBootEnabled
VTpmEnabled
<!--NeedCopy-->
```

Identifier les ressources créées par MCS

Voici les balises que MCS ajoute aux ressources de la plate-forme Azure. 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"

Nom de la ressource	Balise
Carte d'interface réseau	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal"
Disque OS	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal"
MV 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" CitrixSchemaVersion: 2.0 "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Compte de stockage	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal"
machine virtuelle dans le catalogue	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "CitrixResource": "Internal"
Disque WBC	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "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.

Supprimer les balises

Lorsque vous créez un catalogue ou une machine virtuelle, des balises sont créées sur les ressources suivantes :

- Groupe de ressources
- Machine virtuelle
- Disque OS
- Disque d'identité
- Interface réseau
- Compte de stockage

Vous pouvez supprimer des machines virtuelles et des catalogues de machines de la base de données Citrix et supprimer les balises. Vous pouvez utiliser :

- `Remove-ProvVM` avec le paramètre `ForgetVM` pour supprimer les machines virtuelles et les balises d'une seule machine virtuelle ou d'une liste de machines virtuelles d'un catalogue de machines virtuelles.
- `Remove-ProvScheme` avec le paramètre `ForgetVM` pour supprimer un catalogue de machines de la base de données Citrix et les balises d'un catalogue de machines complet.

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 spécifiques à Citrix.
3. Exécutez `Remove-ProvVM` pour supprimer des machines virtuelles de la base de données Citrix et les balises des machines virtuelles.
   Par exemple :

   ```
   1 Remove-ProvVM -ProvisioningSchemeName "ProvisioningSchemeName" -
       VMName "vmname" -ForgetVM
   2 <!--NeedCopy-->
   ```

4. Exécutez `Remove-ProvScheme` pour supprimer un catalogue de machines de la base de données Citrix et les balises des catalogues de machines. Par exemple :

   ```
   1 Remove-ProvScheme -ProvisioningSchemeName "ProvisioningSchemeName
       " -ForgetVM
   2 <!--NeedCopy-->
   ```

   > **Remarque :**
   >
   > Une fois que vous avez utilisé le paramètre `ForgetVM` dans `Remove-ProvScheme`, MCS supprime tous les instantanés, y compris les instantanés du disque de base si le schéma de provisioning est présent dans le groupe Bring your own resource (BYORG) ou dans le groupe de ressources géré par Citrix.

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 les catalogues de machines

Gérer un catalogue Microsoft System Center Virtual Machine Manager

January 25, 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 (VMM).

> **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 de la plateforme SCVMM. 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" Entrée de propriété personnalisée : "XdConfig:" XdProvisioned=True"
VM dans le catalogue	Chaîne de balise : "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" 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 12, 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>"
<!--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.

Rechercher l'ID du dossier à l'aide des commandes PowerShell

Exécutez la commande Powershell `Get-HypConfigurationDataForItem` pour rechercher l'ID d'un dossier existant dans un hyperviseur VMware.

Créez une connexion d'hébergement et un groupe de ressources pour un Hyperviseur VMware. Effectuez ensuite les étapes suivantes pour rechercher l'ID d'un dossier sur cet Hyperviseur.

1. Déterminez le chemin d'accès `XDHyp` à la racine de l'arborescence des dossiers de mv. Par exemple :

```
XDHyp:\Connections\VMwareConn\Datacenter.datacenter
<!--NeedCopy-->
```

2. Utilisez `Get-HypConfigurationDataForItem` pour récupérer l'arborescence. Par exemple :

```
Get-HypConfigurationDataForItem -LiteralPath XDHyp:\Connections\
    VMwareConn\Datacenter.datacenter
<!--NeedCopy-->
```

3. Exécutez la commande suivante pour identifier l'ID du dossier à partir du fichier de sortie XML. Dans cet exemple, recherchez l'ID de dossier de `ExampleFolder` dans le fichier de sortie XML.

```
$result = Get-HypConfigurationDataForItem -LiteralPath XDHyp:\
    Connections\VMwareConn\Datacenter.datacenter
$result.VmPlacementFolder
<!--NeedCopy-->
```

Fichier de sortie XML :

```
<?xml version="1.0" encoding="utf-16"?>
<CtxVmPlacementFolder xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Name>vm</Name>
<Id>group-v4</Id>
<SubFolder>
<CtxVmPlacementFolder>
  <Name>vCLS</Name>
  <Id>group-v75</Id>
```



```
    <SubFolder />
  </CtxVmPlacementFolder>
  <CtxVmPlacementFolder>
    <Name>MyOtherFolder</Name>
    <Id>group-v1110</Id>
    <SubFolder />
  </CtxVmPlacementFolder>
  <CtxVmPlacementFolder>
    <Name>ExampleFolder</Name>
    <Id>group-v4658</Id>
    <SubFolder />
  </CtxVmPlacementFolder>
  </SubFolder>
  </CtxVmPlacementFolder>
  <!--NeedCopy-->
```

Trouver l'ID de dossier dans vSphere

Accédez au MOB sur n'importe quel système ESXi ou vCenter Server pour trouver l'ID de dossier des machines virtuelles.

Managed Object Browser (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**. Pour ce faire, vous pouvez utiliser l'interface Configuration complète ou les commandes PowerShell.
   - Si vous utilisez l'interface de configuration complète, voir 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 :

```
1 Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -
     VMName ("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,
     Identity -DestinationStorageId datastore1,datastore1
2 <!--NeedCopy-->
```

4. Obtenez l'ID de tâche de la migration. Par exemple :

```
1 ,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk -
     ProvisioningSchemeName xxxxx -DiskType OS,Identity -
     DestinationStorageId datastore1,datastore1
2 <!--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 l'interface de configuration complète pour supprimer l'ancien stockage.

Identifier les ressources créées par MCS

Voici les balises que MCS ajoute aux ressources de la plateforme VMware. 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

Gérer un catalogue XenServer

January 25, 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 du catalogue XenServer. Consultez la section Créer un catalogue XenServer.

Identifier les ressources créées par MCS

Lorsque Machine Creation Services (MCS) génère des ressources telles que des disques, il attribue une balise d’identification ProvisioningScheme pour optimiser l’utilisation de ces ressources.

Les balises sont utiles aux administrateurs, car elles leur permettent de mieux gérer et organiser les ressources. Par exemple, si des ressources, telles que des disques inutilisés, sont balisées, les administrateurs peuvent facilement identifier où la ressource a été créée, ce qui rend le processus de nettoyage plus efficace.

Voici les balises que MCS ajoute aux ressources de la plateforme XenServer. Les balises du tableau sont représentées au format “clé”:”valeur”.

Nom de la ressource	Balise
Copie du disque sur chaque réseau ou stockage local (sur site uniquement)	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Disque d’identification	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Disque OS	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
machine virtuelle de préparation	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
VM dans le catalogue	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
Disque WBC	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

Récupérer des informations sur le schéma de provisioning

Pour récupérer des informations détaillées sur le schéma de provisioning, vous pouvez exécuter les commandes PowerShell suivantes. Remplacez `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx` par l’ID réel du schéma de provisioning :

1. Remplacer l’identifiant de l’espace réservé par l’identifiant réel du schéma de provisioning

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
<!--NeedCopy-->
```

2. Récupérez des informations détaillées sur le schéma de provisioning :

```
Get-ProvisioningScheme -Id $provisioningSchemeId
<!--NeedCopy-->
```

Récupérer la liste des ressources créées par MCS

Exécutez les commandes suivantes pour obtenir une liste complète des ressources créées par MCS.

1. Remplacez l’identifiant de l’espace réservé par l’identifiant réel du schéma de provisioning.

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
<!--NeedCopy-->
```

2. Récupérez la liste complète des ressources créées par MCS.


```
Get-ProvResource -ProvisioningSchemeUid $provisioningSchemeId |
    ConvertTo-JSON -Depth 6
<!--NeedCopy-->
```

L'exécution renvoie le résultat suivant :

- Le nom et l'ID du schéma de provisioning.
- Une liste des versions d'images de provisioning dans le schéma de provisioning. Chaque entrée comprend les éléments suivants :
  - Le nom et l'identifiant de l'image.
  - L'ID du disque et l'ID de stockage du disque.
- Une liste des machines virtuelles de provisioning. Chaque entrée comprend les éléments suivants :
  - L'ID du disque du système d'exploitation et l'ID de son disque parent.
  - ID de stockage du disque du système d'exploitation.
  - Le disque d'identité et son ID de stockage.

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

Gestion de l'alimentation

December 4, 2023

Avec Citrix DaaS, vous pouvez gérer l'alimentation des 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

May 17, 2024

Pour plus d'informations sur les autorisations requises, consultez À propos des autorisations AWS.

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, consultez :
   - Cycle de vie des instances
   - Cryptage Amazon EBS
   - Prérequis pour la veille prolongée
   - Activer la mise en veille prolongée pour une instance
   - Mise en veille prolongée de votre instance à la demande ou de votre instance Spot
3. Utilisez cette instance comme image principale pour créer une AMI.
4. 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.
5. 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.
6. 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.

```
1 New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot
2 -CustomProperties "AwsCaptureInstanceProperties,true;"
3 -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.

Créer un catalogue de machines avec prise en charge de la mise en veille prolongée

Lorsque vous créez des catalogues de machines, vous pouvez utiliser un profil de machine compatible avec la mise en veille prolongée.

1. Dans l'assistant de création de catalogue, suivez les instructions jusqu'à la sélection du profil de machine.
2. Sur la page **Modèle de machine**, cliquez sur **Sélectionner un profil de machine**, puis sélectionnez un profil de machine.
3. Sur la page **Machine virtuelle**, cliquez sur l'icône **Modifier** et sélectionnez une machine virtuelle.

   > **Remarque :**
   >
   > Si le mode veille prolongée est activé pour le profil de machine, le système affiche uniquement les machines virtuelles qui peuvent être mises en veille prolongée.

4. Suivez les instructions qui s'affichent à l'écran pour effectuer les réglages. La page **Résumé** affiche l'état de mise en veille prolongée du catalogue.

   > **Remarque :**
   >
   > Lors de la modification d'un catalogue de machines, lorsque vous remplacez le profil de machine compatible avec la mise en veille prolongée par un profil non compatible, il vous est demandé de reconfigurer vos machines virtuelles en conséquence.

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.

Pour voir les options de gestion de l'alimentation, dans l'interface **Gérer > Configuration complète**, cliquez avec le bouton droit sur les machines virtuelles en veille prolongée.

Vous pouvez également voir l'état de l'alimentation, **Suspension** et **Suspendu**, pour chaque machine virtuelle en fonction des opérations d'alimentation que vous effectuez sur les machines virtuelles.

Gérer l'alimentation des machines virtuelles Azure

June 12, 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 VM ne sont créées que lorsque Citrix DaaS initie une action d'alimentation une fois le provisioning 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 aucune machine virtuelle tant que Citrix DaaS n'a pas lancé une action d'alimentation pour celle-ci. Ensuite, l'état de la machine virtuelle dans l'interface Configuration complète passe à **Activé**. 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 VM 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 déconseillée. Par conséquent, vous devez recréer 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.

Conservation d'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 **true** pour conserver une machine virtuelle lorsqu'elle est mise hors tension, ou définissez la propriété sur **false** 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 propriétés `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. Vous ne pouvez pas supprimer 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 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` :
  - À la mise 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 incluant la propriété personnalisée `FailSafeStorageType`, procédez comme suit :

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 `Request-ProvVMUpdate`.

1. Exécutez la commande Request-ProvVMUpdate. Par exemple :

```
Request-ProvVMUpdate -ProvisioningSchemeName <String> -VMName <
    List-Of-Vm-Names>
<!--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 :

- Logiciels 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 :

- Interface Configuration complète, ou
- Commandes PowerShell

Créer un catalogue à l'aide de l'interface Configuration complète

1. Connectez-vous à Citrix Cloud. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.
2. Dans **Gérer > Configuration complète**, sélectionnez **Catalogues de machines** dans le volet gauche.
3. Sélectionnez **Créer un catalogue de machines**. L'assistant de création de catalogues s'ouvre.
4. Sur la page **Type de machine**, sélectionnez le type de machine avec **OS mono-session** pour ce catalogue.
5. 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)**.
6. Sur la page **Expérience de bureau**, sélectionnez l'expérience de bureau aléatoire ou statique selon vos besoins.
7. 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.
8. Sur la page **Types de stockage et de licence**, sélectionnez le stockage et la licence à utiliser pour ce catalogue.
9. 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. Les séries VM GPU sont disponibles en version Technical Preview.

10. Sur la page **Cartes d'interface réseau**, ajoutez les cartes d'interface réseau que vous souhaitez que les machines virtuelles utilisent.
11. Sur la page **Paramètres du disque**, sélectionnez le type de stockage et la taille du disque de cache en écriture différée.
12. Sur la page **Groupe de ressources**, sélectionnez le groupe de ressources pour provisionner les machines virtuelles.
13. Sur la page **Identités des machines**, sélectionnez **Créer de nouveaux comptes Active Directory**. Spécifiez ensuite un schéma d'affectation de nom de compte.

14. 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.
15. 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 :
  - actuellement, modifier le profil de machine en profil qui prend en charge la mise en veille prolongée à l'aide de l'interface Configuration complète. 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 pour des machines virtuelles existantes compatibles avec la mise en veille prolongée à l'aide de l'interface Configuration complète, 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 la section Gérer Citrix DaaS à l'aide des Remote PowerShell SDK.

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 -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 -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 :
  - actuellement, modifier le profil de machine en profil qui prend en charge la mise en veille prolongée à l'aide de l'interface Configuration complète. 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 :

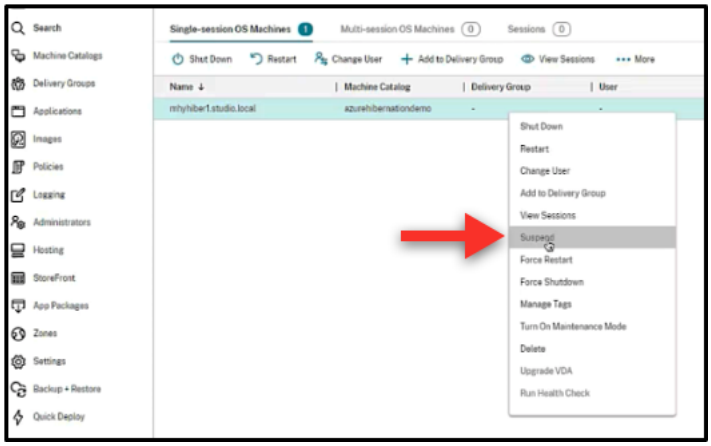
- Suspendre
- Reprendre

Suspendre Vous pouvez suspendre une machine virtuelle de l'une des manières suivantes :

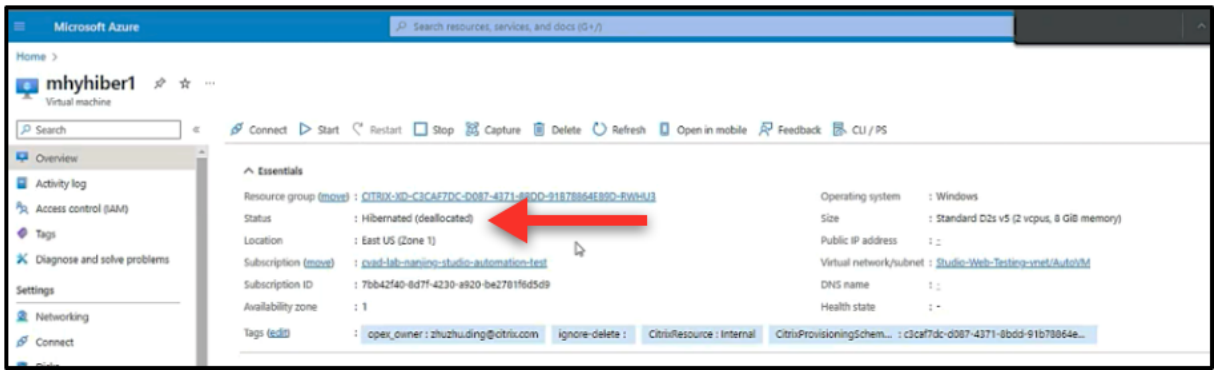
- **Manuellement** à l'aide de l'interface Configuration complète
- **Automatiquement** à l'aide de la stratégie de délai d'expiration : pour plus d'informations, voir Paramètres divers.

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**.

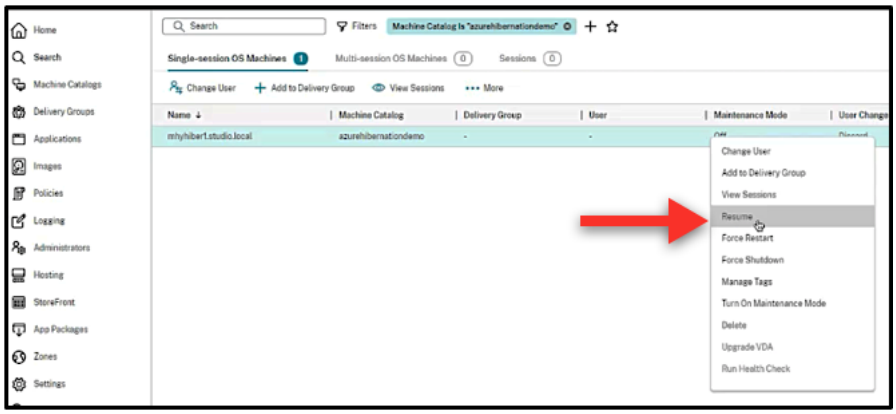


Vous pouvez vérifier l'état de la machine virtuelle sur le portail Azure.

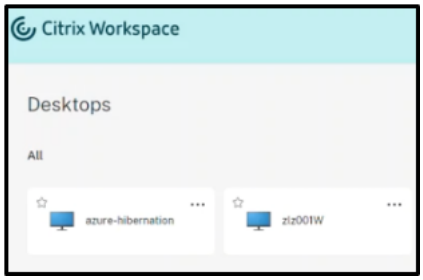


Reprendre Pour reprendre une machine virtuelle mise en veille prolongée, utilisez l'une des méthodes suivantes :

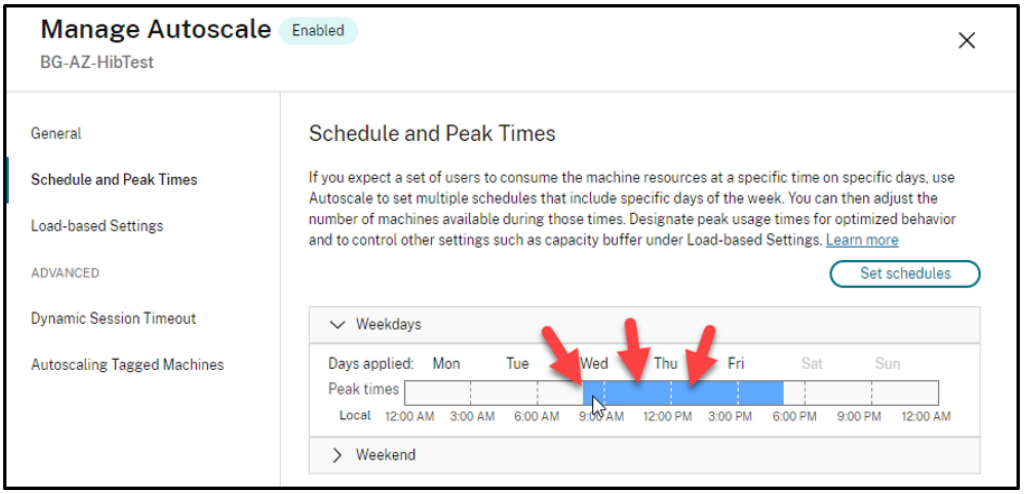
- **Manuellement** :
  - Les administrateurs peuvent reprendre la machine virtuelle à l'aide de l'interface Configuration complète.



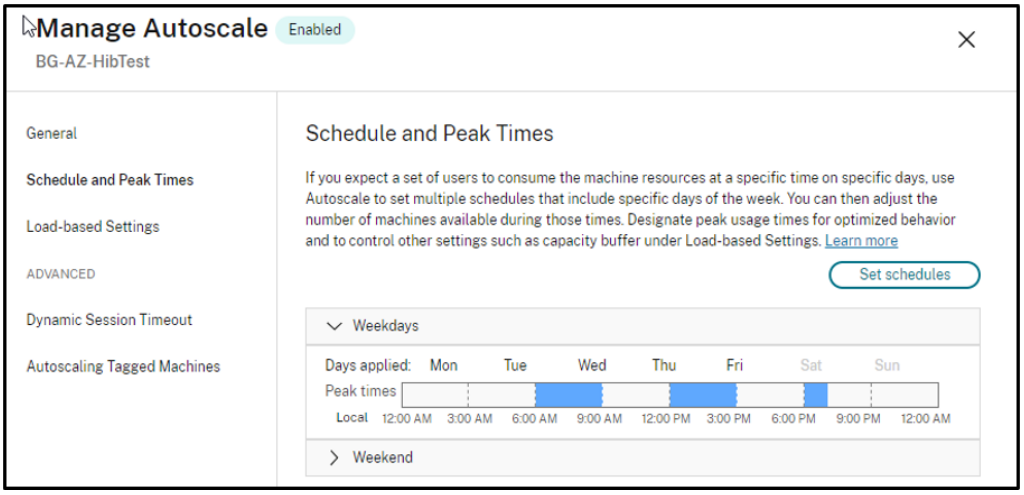
  - Les utilisateurs finaux peuvent démarrer la machine virtuelle à l'aide du menu Citrix Workspace une fois qu'ils ont cliqué sur l'icône du bureau.



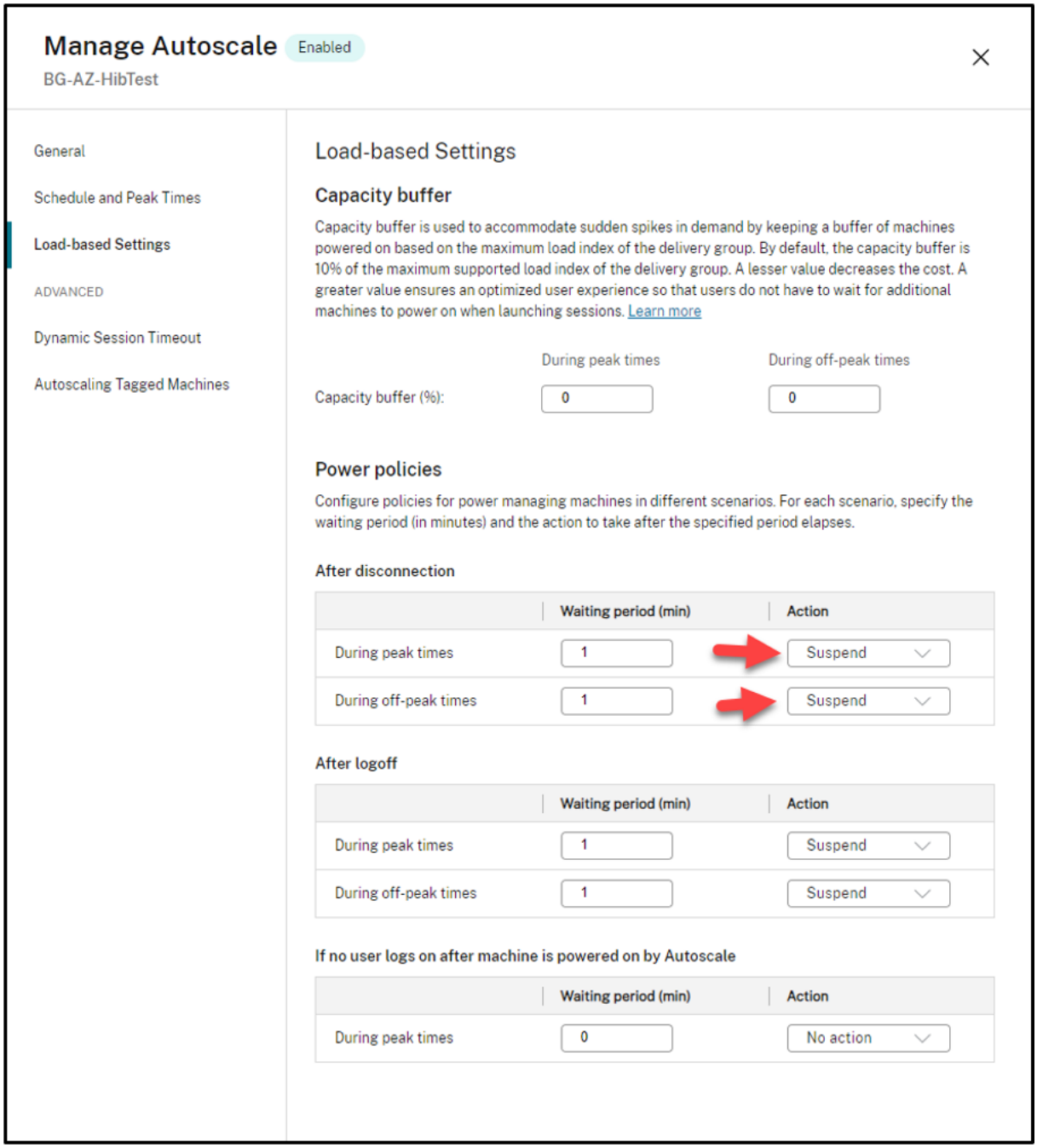
- **Automatiquement** :
  - Autoscale peut automatiquement allumer les machines mises en veille prolongée si vous configurez correctement les heures de pointe. Vous pouvez définir les heures de pointe par intervalles de 30 minutes en cliquant sur le calendrier. Chaque cadre bleu représente une plage 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

April 17, 2023

Cet article décrit les fonctionnalités de sécurité des différents hyperviseurs pris en charge. Les fonctionnalités de sécurité incluent :

- Groupe de sécurité
- Démarrage sécurisé
- Fonctionnalités de chiffrement

Groupe de sécurité

April 17, 2023

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 :

- Groupe de sécurité dans AWS
- Groupe de sécurité dans Microsoft Azure
- Groupe de sécurité dans Google Cloud Platform

Groupe 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.

Groupe de sécurité dans Microsoft Azure

Citrix DaaS 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.

Groupe 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

May 17, 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, elle 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).

Consultez les informations suivantes pour en savoir plus sur les hyperviseurs pris en charge :

- 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 12, 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.

Consultez les informations suivantes pour en savoir plus sur les hyperviseurs pris en charge :

- 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 DaaS prend en charge les clés de chiffrement 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.

Déploiement rapide

November 24, 2023

Introduction

Dans Citrix DaaS, l'interface **Gérer > Déploiement rapide** permet un déploiement rapide des applications et des bureaux lorsque vous utilisez Microsoft Azure pour héberger vos bureaux et vos applications. Cette interface offre une configuration de base, sans fonctionnalités avancées.

Utilisez Déploiement rapide pour :

- Provisionner des machines virtuelles et des catalogues qui fournissent des bureaux et des applications hébergés dans Microsoft Azure.
- Créer des catalogues Remote PC Access pour les machines existantes.

Avec Déploiement rapide, vous pouvez utiliser un abonnement Azure géré par Citrix ou votre propre abonnement Azure.

(Bien que les noms soient similaires, Déploiement rapide est distinct de la méthode de création rapide de catalogues dans l'interface Déploiement rapide.)

Par ailleurs, l'interface **Configuration complète** offre également des fonctionnalités de configuration avancées. Pour plus d'informations concernant les options de l'onglet **Gérer**, reportez-vous à la section Interfaces de gestion.

Différences entre les interfaces de gestion

Le tableau suivant compare les interfaces Configuration complète et Déploiement rapide.

Fonctionnalité	Déploiement rapide	Configuration complète
Déploiement avec Azure	Oui	Oui *
Déployer avec d'autres services cloud	Non	Oui
Déployer avec des hyperviseurs locaux	Non	Oui
Images préparées par Citrix disponibles	Oui	Non
Expérience utilisateur simplifiée	Oui	Non

* Lorsque vous utilisez un abonnement Azure géré par Citrix, vous devez utiliser Déploiement rapide lors de la création d'une image ou d'un catalogue.

Si vous avez déjà utilisé Configuration complète pour créer et gérer des catalogues, Déploiement rapide présente les différences suivantes.

- Terminologie différente.
  - Dans Déploiement rapide, vous créez un catalogue.
  - Dans Configuration complète (Studio), vous créez un catalogue de machines. Dans la pratique, il est souvent appelé simplement catalogue.
- Emplacement des ressources et des Cloud Connector.
  - Déploiement rapide crée automatiquement un emplacement de ressources contenant deux Cloud Connector lorsque vous créez votre premier catalogue.
  - Dans Configuration complète, la création d'un emplacement de ressources et l'ajout de Cloud Connectors sont des étapes distinctes que vous devez effectuer dans Citrix Cloud avant de créer un catalogue.
- Images utilisées pour créer des catalogues.
  - Déploiement rapide propose plusieurs images des machines Windows et Linux préparées par Citrix. Vous pouvez utiliser ces images pour créer des catalogues.

    Vous pouvez également utiliser ces images pour créer d'autres images, puis personnaliser celles-ci en fonction de vos besoins de déploiement uniques. Cette fonctionnalité est connue sous le nom de générateur d'images. Vous pouvez également importer des images à partir de votre propre abonnement Azure.
  - Dans Configuration complète, vous personnalisez les images de l'hôte pris en charge que vous utilisez. Les images préparées par Citrix ne sont pas disponibles.

- Affichage des catalogues :
  - Les catalogues créés dans Déploiement rapide sont visibles dans les affichages Déploiement rapide et Configuration complète.
  - Les catalogues créés dans Configuration complète ne sont pas visibles dans Déploiement rapide.
- Groupes de mise à disposition :
  - Vous ne créez pas de groupes de mise à disposition dans Déploiement rapide. Dans Déploiement rapide, vous spécifiez les machines, les applications, les bureaux et les utilisateurs (abonnés) dans le catalogue.

    Citrix crée automatiquement un groupe de mise à disposition pour chaque catalogue Déploiement rapide en utilisant le même nom que le catalogue. Cette action se produit en arrière-plan. Aucune intervention de votre part n'est requise pour créer le groupe de mise à disposition. Le groupe de mise à disposition apparaît uniquement dans l'interface Configuration complète, et non dans Déploiement rapide.
  - Dans Configuration complète, vous créez un groupe de mise à disposition et indiquez les machines qu'il contient. Vous pouvez également spécifier des applications, des bureaux et des utilisateurs. Vous pouvez aussi créer des groupes d'applications.
- Mise en page et interface utilisateur.
  - L'interface de Déploiement rapide a une mise en page et un style différents de Configuration complète. Déploiement rapide contient davantage de conseils à l'écran.

Les interfaces ne sont pas mutuellement exclusives. Vous pouvez utiliser Déploiement rapide pour créer des catalogues, puis utiliser Configuration complète pour créer d'autres catalogues.

Gérer les catalogues créés dans l'interface Déploiement rapide

Après avoir créé un catalogue dans l'interface Déploiement rapide, vous pouvez continuer à gérer ce catalogue dans cette interface. Pour plus d'informations, consultez la section Gérer les catalogues dans Déploiement rapide. Vous pouvez également utiliser l'interface Configuration complète.

Lorsque vous créez un catalogue dans Déploiement rapide, ce catalogue (plus le groupe de mise à disposition et la connexion d'hébergement qui sont créés automatiquement en arrière-plan) se voient attribuer une étendue `Citrix managed object`. Les étendues sont utilisées dans l'administration déléguée pour regrouper des objets.

Les catalogues, les groupes de mise à disposition et les connexions avec l'étendue `Citrix managed object` sont interdits de certaines actions dans l'interface Configuration complète. (L'autorisation de ces actions dans Configuration complète peut nuire à la capacité du système à

prendre en charge à la fois le déploiement rapide et la configuration complète, de sorte que ces actions sont désactivées.) Dans l'interface Configuration complète :

- **Catalogue :** La plupart des actions de gestion de catalogue ne sont pas disponibles. Vous ne pouvez pas supprimer un catalogue.
- **Groupe de mise à disposition :** La plupart des actions de gestion de groupe de mise à disposition sont disponibles. Vous ne pouvez pas supprimer le groupe de mise à disposition.
- **Connexion :** La plupart des actions de gestion de connexions ne sont pas disponibles. Vous ne pouvez pas supprimer une connexion. Vous ne pouvez pas créer de connexion basée sur une connexion avec l'étendue `Citrix managed object`.

Si vous créez un catalogue dans Déploiement rapide à l'aide de votre propre abonnement Azure (que vous avez ajouté à Déploiement rapide) et que vous souhaitez gérer le catalogue (ainsi que son groupe de mise à disposition et sa connexion) entièrement dans Configuration complète, vous pouvez *convertir* le catalogue.

- La conversion d'un catalogue limite sa gestion à l'interface Configuration complète uniquement. Une fois qu'un catalogue est converti, vous ne pouvez plus utiliser l'interface Déploiement rapide pour gérer ce catalogue.
- Une fois le catalogue converti, les actions qui étaient auparavant indisponibles dans Configuration complète peuvent être sélectionnées. (L'étendue `Citrix managed object` est supprimée du catalogue, du groupe de mise à disposition et de la connexion d'hébergement convertis.)
- Pour convertir un catalogue :

  Dans le tableau de bord **Gérer > Déploiement rapide**, cliquez n'importe où dans l'entrée du catalogue. Dans l'onglet **Détails**, sous **Paramètres avancés**, sélectionnez **Convertir le catalogue**. Lorsque vous y êtes invité, confirmez la conversion.
- Vous ne pouvez pas convertir un catalogue créé dans Déploiement rapide à l'aide d'un abonnement Citrix Managed Azure.

Remplacement de l'ancienne interface de Déploiement rapide d'Azure

Déploiement rapide remplace une ancienne interface nommée Déploiement rapide d'Azure. Déploiement rapide inclut tous les catalogues que vous avez créés à l'aide de Déploiement rapide d'Azure.

Si vous avez commencé à créer un catalogue dans Déploiement rapide d'Azure, mais que vous ne l'avez pas terminé, ce catalogue apparaît dans la liste de catalogues de Déploiement rapide. Toutefois, la seule action possible sur ce catalogue dans Déploiement rapide est la suppression.

Exigences

- Le Déploiement rapide prend en charge uniquement les charges de travail Azure. Il n'est pas disponible avec d'autres types d'hôtes cloud, services ou hyperviseurs.
- Le Déploiement rapide est disponible uniquement dans Citrix DaaS pour Azure, éditions Premium, Advanced et Workspace Premium Plus.
- Vous devez disposer d'un compte Citrix Cloud et d'un abonnement à Citrix DaaS.
- Si vous avez commandé le Consumption Fund Azure géré par Citrix, vous pouvez utiliser un abonnement Azure géré par Citrix lorsque vous créez des catalogues et des images.

  Si vous n'avez pas commandé Consumption Fund (ou si vous préférez utiliser votre propre abonnement Azure), vous devez disposer d'un abonnement Azure.
- Vous devez disposer des autorisations appropriées dans Citrix DaaS pour voir l'onglet **Gérer**. Pour de plus amples informations, veuillez consulter la section Administration déléguée.

> **Important :**
>
> Pour être sûr d'obtenir les informations importantes sur Citrix Cloud et les services Citrix auxquels vous êtes abonné, vérifiez que vous pouvez recevoir toutes les notifications par e-mail. Par exemple, Citrix envoie des e-mails de notification informatifs mensuels détaillant votre consommation Azure (utilisation).
>
> Dans le coin supérieur droit de la console Citrix Cloud, développez le menu situé à droite des champs Nom du client et OrgID. Sélectionnez **Paramètres du compte**. Dans l'onglet **Mon profil**, sélectionnez toutes les entrées de la section **Notifications par e-mail**.

Considération Citrix Gateway

Si vous utilisez votre propre Citrix Gateway, il doit avoir accès au VNet spécifié dans l'assistant de création de catalogues. Un VPN peut fournir cet accès.

Le Citrix Gateway Service fonctionne automatiquement avec les catalogues Déploiement rapide.

Prochaine étape

Suivez les instructions de configuration Déploiement rapide dans Mise en route.

Après avoir configuré votre déploiement à l'aide de Déploiement rapide, vous pouvez continuer d'utiliser cette interface pour les tâches de gestion suivantes.

- Gérez le catalogue. La gestion des catalogues inclut l'ajout ou la suppression de machines, la gestion des applications et la gestion des programmes de gestion de l'alimentation.

- Gérez les images. La gestion des images inclut la préparation ou l'importation d'images, la mise à jour des catalogues avec une nouvelle image, le changement de nom ou la suppression d'une image, et l'installation ou la mise à niveau d'un VDA sur une image.
- Ajoutez ou supprimez des utilisateurs dans un catalogue.
- Gérez les emplacements des ressources.

Commencer avec Déploiement rapide

May 23, 2023

Cet article résume les tâches de configuration pour fournir des bureaux et des applications à l'aide de l'interface Déploiement rapide de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Nous vous recommandons de consulter chaque procédure avant de la mettre en œuvre, afin que vous sachiez à quoi vous attendre.

Pour utiliser Déploiement rapide pour configurer un déploiement Remote PC Access, reportez-vous à la section Remote PC Access.

Résumé des tâches de configuration

Les sections suivantes de cet article vous guident dans les tâches de configuration :

1. Passez en revue et effectuez les tâches nécessaires dans Configuration système requise et préparation.
2. Configurez un déploiement rapide de preuve de concept ou un déploiement de production.
3. Fournissez l'URL de l'espace de travail à vos utilisateurs.

Configuration système requise et préparation

- Inscrivez-vous à Citrix Cloud et Citrix DaaS.

  En outre, si vous envisagez d'utiliser Azure géré par Citrix, veillez à commander le Citrix Azure Consumption Fund (en plus de Citrix DaaS), via Citrix ou Azure Marketplace.

- **Licences Windows :** assurez-vous de disposer d'une licence adaptée pour les Services Bureau à distance pour exécuter des charges de travail Windows Server ou Azure Virtual Desktop Licensing pour Windows 10. Pour plus d'informations, consultez la section Configurer un serveur de licences Microsoft RDS.

- Si vous prévoyez d'utiliser un abonnement Azure géré par Citrix et que vous souhaitez attacher des VDA à un domaine à l'aide de la stratégie de groupe Active Directory, vous devez être un administrateur autorisé à effectuer cette action dans Active Directory. Pour plus de détails, voir Responsabilité du client.
- La configuration des connexions à votre réseau local d'entreprise comporte des exigences supplémentaires.
  - Toute connexion (Azure VNet peering ou SD-WAN) : Exigences pour toutes les connexions.
  - Connexions Azure VNet peering : Configuration requise et préparation pour Azure VNet peering.
  - Connexions SD-WAN : Configuration requise et préparation de la connexion SD-WAN.
- Si vous envisagez d'utiliser vos propres images Azure lors de la création d'un catalogue, celles-ci doivent répondre à certaines exigences.
- Exigences en termes de connexion Internet :Configuration requise pour le système et la connectivité.
- Limites de ressources dans un déploiement Citrix DaaS : Limites.

Systèmes d'exploitation pris en charge

Lorsque vous utilisez Déploiement rapide avec un abonnement Azure géré par Citrix :

- Windows 10 session unique
- Windows 10 sessions multiples
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux et Ubuntu

Lorsque vous utilisez Déploiement rapide avec un abonnement Azure géré par le client :

- Windows 10 Enterprise session unique
- Windows 10 Enterprise Virtual Desktop sessions multiples
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux et Ubuntu

Configurer un déploiement rapide de preuve de concept

Cette procédure nécessite un abonnement Azure géré par Citrix.

1. Créez un catalogue à l'aide de la création rapide.
2. Ajoutez vos utilisateurs à Managed Azure AD.
3. Ajoutez vos utilisateurs au catalogue.
4. Informez vos utilisateurs de l'URL Workspace.

Configurer un déploiement de production

1. Si vous utilisez votre propre Active Directory ou Azure Active Directory pour authentifier les utilisateurs, connectez-vous et définissez cette méthode dans Citrix Cloud.
2. Si vous utilisez des machines jointes à un domaine, vérifiez que vous disposez d'entrées de serveur DNS valides.
3. Si vous utilisez votre propre abonnement Azure (au lieu d'un abonnement Azure géré par Citrix), ajoutez votre abonnement Azure.
4. Créez ou importez une image. Bien que vous puissiez utiliser l'une des images préparées par Citrix telle quelle dans un catalogue, elles sont principalement destinées à des déploiements de preuve de concept.
5. Si vous utilisez un abonnement Azure géré par Citrix et que vous souhaitez que vos utilisateurs puissent accéder à des éléments de votre réseau (tels que les serveurs de fichiers), configurez une connexion Peering de réseau virtuel Azure ou Citrix SD-WAN.
6. Créez un catalogue à l'aide de la création personnalisée.
7. Si vous créez un catalogue de machines à sessions multiples ajoutez des applications au catalogue, si nécessaire.
8. Si vous utilisez Azure géré par Citrix AD pour authentifier vos utilisateurs, ajoutez des utilisateurs à l'annuaire.
9. Ajoutez des utilisateurs au catalogue.
10. Informez vos utilisateurs de l'URL Workspace.

Après avoir configuré le déploiement, utilisez le tableau de bord **Déploiement rapide > Surveiller** pour voir l'utilisation des bureaux, les sessions et les machines.

URL Workspace

Après avoir créé des catalogues et y avoir alloué des utilisateurs, indiquez aux utilisateurs où trouver leurs bureaux et applications : l'URL Workspace. L'URL Workspace est la même pour tous les catalogues et utilisateurs.

L'URL Workspace est disponible à deux emplacements :

- Dans **Gérer > Déploiement rapide** dans Citrix DaaS, affichez l'URL en développant **Accès utilisateur et authentification** sur la droite.
- À partir de la console Citrix Cloud, sélectionnez **Configuration de l'espace de travail** dans le menu supérieur gauche. L'onglet **Accès** contient l'URL Workspace.

Pour plus d'informations sur la personnalisation de l'URL Workspace, consultez Personnaliser l'URL de l'espace de travail.

Une fois que les utilisateurs ont accédé à l'URL Workspace et se sont authentifiés, ils peuvent démarrer leurs bureaux et leurs applications.

Obtenir de l'aide

- Consultez l'article Dépannage .
- Si vous rencontrez toujours des problèmes avec Citrix DaaS, ouvrez un ticket en suivant les instructions de la section Comment obtenir de l'aide.

Création de catalogues avec Déploiement rapide

May 17, 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.

Utilisez les procédures décrites dans cet article pour créer un catalogue de machines Microsoft Azure à l'aide de l'interface de gestion Déploiement rapide.

Consultez l'ensemble de la procédure avant de créer un catalogue, afin de savoir à quoi vous attendre.

Pour créer un catalogue à l'aide de l'interface Configuration complète, reportez-vous à la section Créer des catalogues de machines.

Types de machines

Un catalogue Déploiement rapide peut contenir l'un des types de machines suivants :

- **Statique :** le catalogue contient des machines statiques à session unique (également appelées bureaux personnels, dédiés ou persistants). Statique signifie que lorsqu'un utilisateur démarre un bureau, celui-ci « appartient » à cet utilisateur. Toute modification apportée par cet utilisateur au bureau est conservée lors de la fermeture de session. Plus tard, lorsque cet utilisateur revient sur Citrix Workspace et démarre un bureau, il s'agira du même bureau.
- **Aléatoire :** le catalogue contient des machines aléatoires à session unique (également appelées bureaux non persistants). Aléatoire signifie que lorsqu'un utilisateur démarre un bureau, toute modification apportée par cet utilisateur à ce bureau est supprimée après la fermeture de session. Plus tard, lorsque cet utilisateur revient sur Citrix Workspace et démarre un bureau, il peut s'agir ou non du même bureau.
- **Sessions multiples :** le catalogue contient des machines avec des applications et des bureaux. Plusieurs utilisateurs peuvent simultanément accéder à chacune de ces machines. Les utilisateurs peuvent lancer un bureau ou des applications depuis leur espace de travail. Les sessions d'application peuvent être partagées. Le partage de session n'est pas autorisé entre une application et un bureau.
  - Lorsque vous créez un catalogue à sessions multiples, vous sélectionnez la charge de travail : légère (par exemple saisie de données), moyenne (comme les applications bureautiques), lourde (comme l'ingénierie) ou personnalisée. Chaque option représente un nombre spécifique de machines et de sessions par machine, ce qui donne le nombre total de sessions prises en charge par le catalogue.
  - Si vous sélectionnez la charge de travail personnalisée, vous sélectionnez l'une des combinaisons disponibles d'unités centrales, de RAM et de stockage. Saisissez le nombre de machines et de sessions par machine, ce qui donne le nombre total de sessions prises en charge par le catalogue.

Lors du déploiement de postes de travail, les types de machines statiques et aléatoires sont parfois appelés « types de bureaux ».

Méthodes de création d'un catalogue avec Déploiement rapide

Il existe plusieurs façons de créer et de configurer un catalogue :

- La **création rapide** est le moyen le plus rapide de démarrer. Vous fournissez un minimum d'informations et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) s'occupe du reste. Un catalogue à création rapide est idéal pour un environnement de test ou une preuve de concept.
- La **création personnalisée** permet plus de choix de configuration que la création rapide. Elle est plus adaptée à un environnement de production qu'un catalogue à création rapide.

- Les catalogues **Remote PC Access** contiennent des machines existantes (généralement physiques) auxquelles les utilisateurs accèdent à distance. Pour plus de détails et des instructions sur ces catalogues, consultez Remote PC Access.

Voici une comparaison entre la création rapide et la création personnalisée :

Création rapide	Création personnalisée
Moins d'informations à fournir.	Plus d'informations à fournir.
Moins de choix pour certaines fonctionnalités.	Plus de choix pour certaines fonctionnalités.
Authentification utilisateur Azure Active Directory gérée par Citrix.	Choix entre : Azure Active Directory géré par Citrix ou votre Active Directory/Azure Active Directory.
Aucune connexion à votre réseau local.	Choix entre : aucune connexion à votre réseau local, à Azure VNet peering et au SD-WAN.
Utilise une image Windows 10 préparée par Citrix. Cette image contient un VDA de bureau actuel.	Choix entre : les images préparées par Citrix, les images que vous importez depuis Azure ou les images que vous avez créées dans Citrix DaaS à partir d'une image préparée ou importée par Citrix.
Chaque bureau dispose d'un stockage sur disque standard (HDD) Azure.	Plusieurs options de stockage sont disponibles.
Bureaux statiques uniquement.	Bureaux statiques, aléatoires ou à sessions multiples.
Un programme de gestion de l'alimentation ne peut pas être configuré pendant la création. La machine hébergeant le bureau s'éteint à la fin de la session. (Vous pouvez modifier ce paramètre ultérieurement.)	Un programme de gestion de l'alimentation peut être configuré lors de la création. (Un programme de gestion de l'alimentation Déploiement rapide diffère d'un programme de gestion de l'alimentation que vous pouvez créer à l'aide de l'interface de gestion Configuration complète.)
Vous devez utiliser un abonnement Azure géré par Citrix.	Vous pouvez utiliser l'abonnement Azure géré par Citrix ou votre propre abonnement Azure.

Pour plus de détails concernant la procédure, voir :

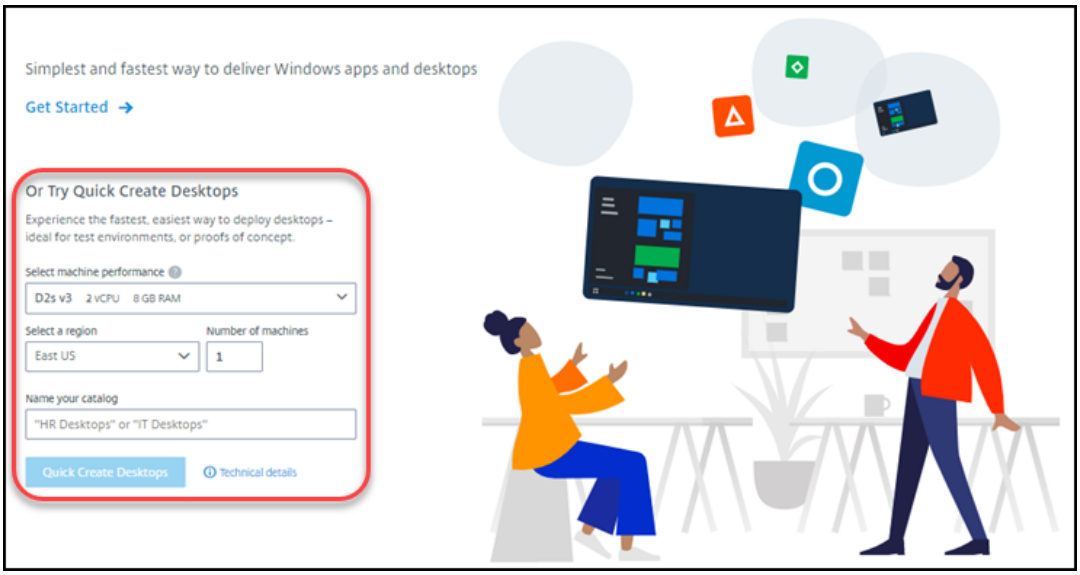
- Créer un catalogue Déploiement rapide en utilisant la création rapide
- Créer un catalogue Déploiement rapide en utilisant la création personnalisée

> **Important :**
>
> Lorsque vous créez pour la première fois un catalogue (ou une image) à l'aide d'un abonnement Azure géré par Citrix, il vous est demandé de reconnaître votre responsabilité pour les frais encourus et d'y consentir. Des rappels de ce consentement peuvent également apparaître lors de la création d'autres catalogues ou images à l'aide de l'abonnement Azure géré par Citrix.

Créer un catalogue Déploiement rapide en utilisant la création rapide

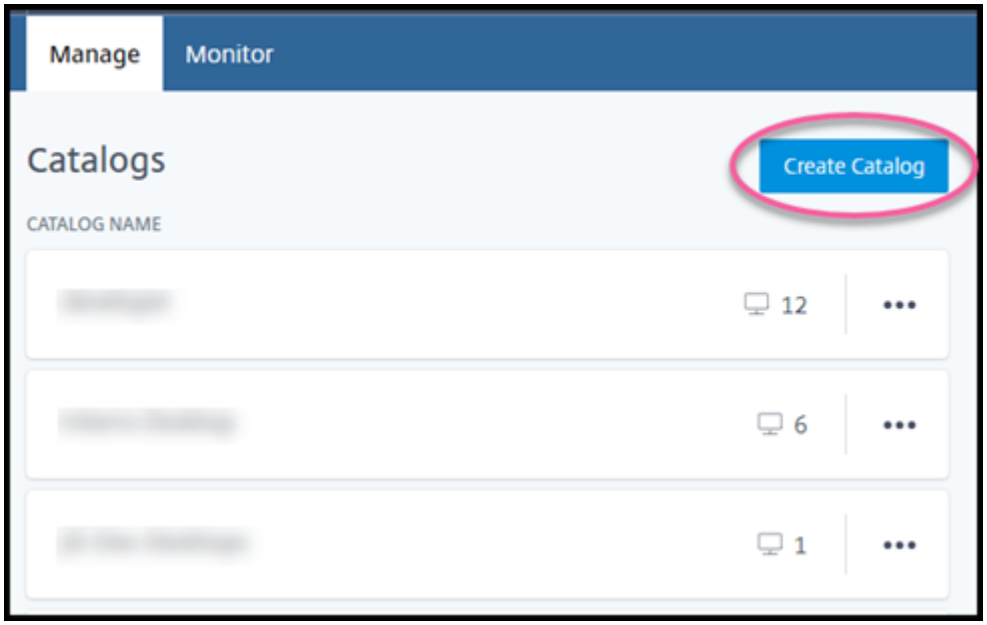
La méthode de création rapide utilise un abonnement Azure géré par Citrix et une image Windows 10 préparée par Citrix pour créer un catalogue contenant des machines statiques. Les paramètres de gestion de l'alimentation utilisent les valeurs prédéfinies de gestion économique de l'alimentation. Il n'y a pas de connexion à votre réseau d'entreprise. Les utilisateurs doivent être ajoutés à l'aide de Azure géré par Citrix AD.

1. Connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.
3. Sélectionnez **Gérer > Déploiement rapide**.
4. Si un catalogue n'a pas encore été créé, vous accédez à la page d'**accueil**. Choisissez l'une des options suivantes :
   - Configurez le catalogue sur cette page. Passez aux étapes 6 à 10.

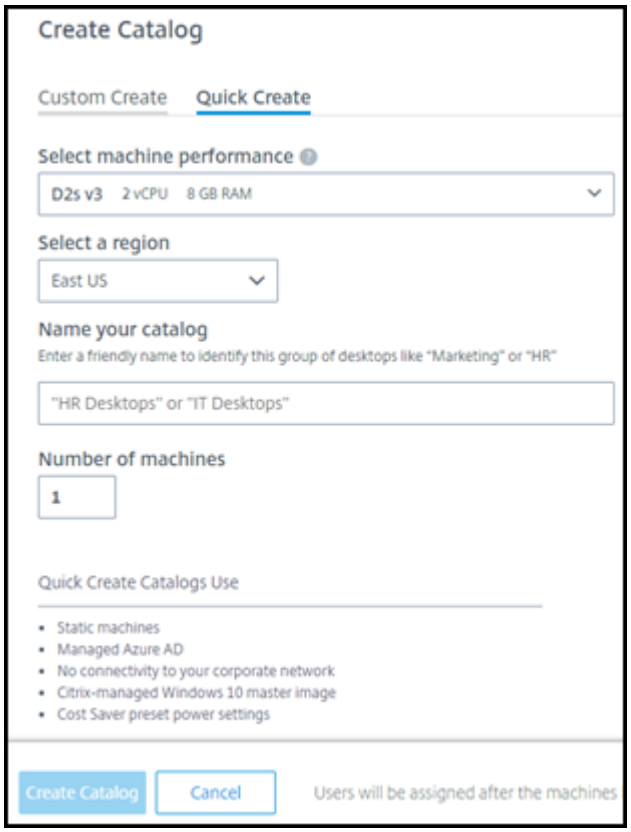


   - Sélectionnez **Mise en route**. Vous accédez au tableau de bord **Gérer > Déploiement rapide** . Sélectionnez **Créer un catalogue**.

5. Si un catalogue a déjà été créé (et que vous en créez un autre), vous accédez au tableau de bord **Gérer > Déploiement rapide**. Sélectionnez **Créer un catalogue**.



6. Sélectionnez **Création rapide** en haut de la page, si ce n'est pas déjà fait.



- **Performances de la machine :** sélectionnez le type de machine. Chaque choix comprend une combinaison unique d'unités centrales, de RAM et de stockage. Les machines plus

performantes ont des coûts mensuels plus élevés.
- **Région :** sélectionnez la région dans laquelle vous souhaitez créer les machines. Vous pouvez sélectionner une région proche de vos utilisateurs.
- **Nom :** saisissez un nom pour le catalogue. Ce champ est obligatoire et il n'y a pas de valeur par défaut.
- **Nombre de machines :** saisissez le nombre de machines souhaitées.

7. Lorsque vous avez terminé, sélectionnez **Créer un catalogue**. (Si vous créez le premier catalogue à partir de la page d'**accueil**, sélectionnez **Création rapide de bureaux**.)
8. S'il s'agit du premier catalogue que vous créez à l'aide d'un abonnement Azure géré par Citrix, lorsque vous y êtes invité, reconnaissez votre responsabilité pour les frais associés.

Pendant la création du catalogue, le nom du catalogue est ajouté à la liste des catalogues, ce qui indique l'avancement de la création.

Citrix DaaS crée également automatiquement un emplacement de ressources et ajoute deux Citrix Cloud Connectors.

Que faire ensuite :

- Vous pouvez ajouter des utilisateurs à l'annuaire Azure AD géré pendant la création du catalogue.
- Une fois le catalogue créé, ajoutez des utilisateurs au catalogue.

Créer un catalogue Déploiement rapide en utilisant la création personnalisée

Si vous utilisez un abonnement Azure géré par Citrix et que vous prévoyez d'utiliser une connexion à vos ressources réseau locales, créez une connexion réseau avant de créer le catalogue. Pour permettre à vos utilisateurs d'accéder à vos ressources réseau locales ou à d'autres ressources réseau, vous devez également obtenir des informations Active Directory pour cet emplacement.

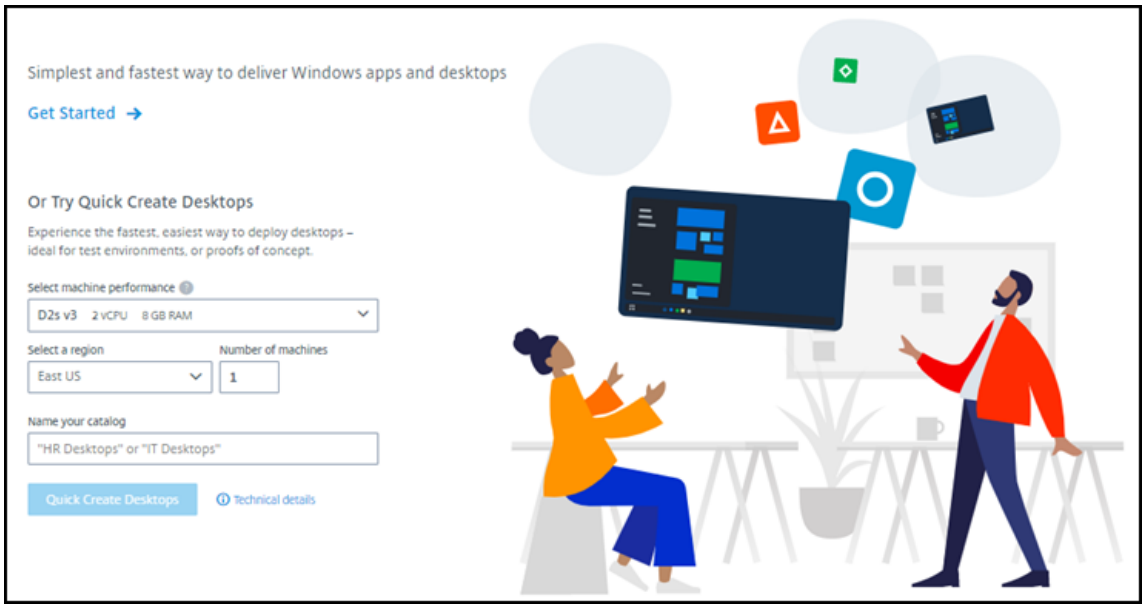
Si vous ne disposez pas d'un abonnement Azure géré par Citrix, vous pouvez :

- Commandez l'Azure Consumption Fund via Azure Marketplace, qui vous fournit un abonnement Azure géré par Citrix.
- Importez (ajoutez) un ou plusieurs de vos propres abonnements Azure à Citrix DaaS avant de créer un catalogue.

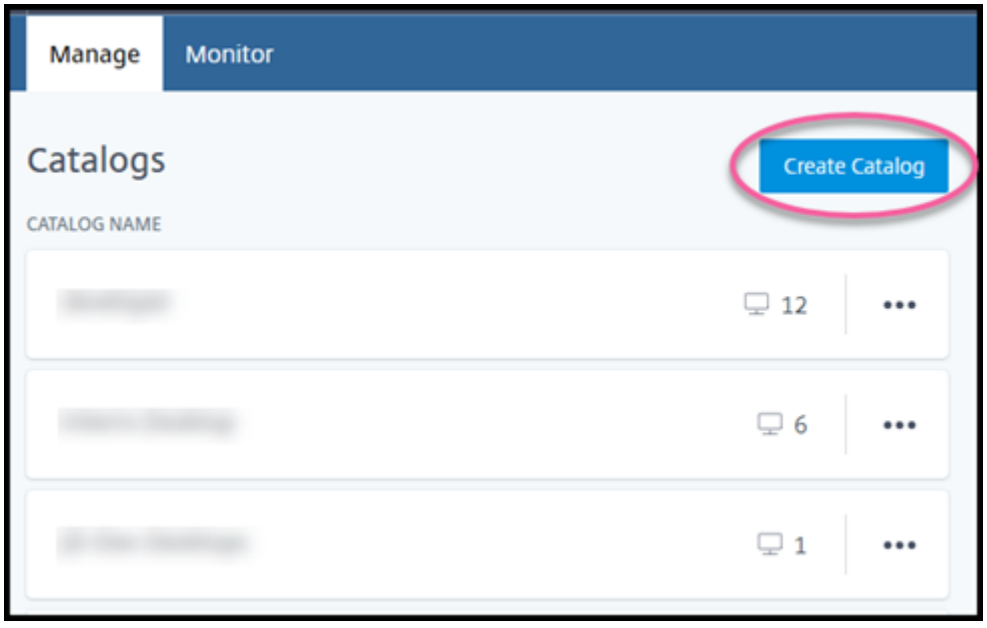
Pour créer un catalogue :

1. Connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.
3. Sélectionnez **Gérer > Déploiement rapide**.

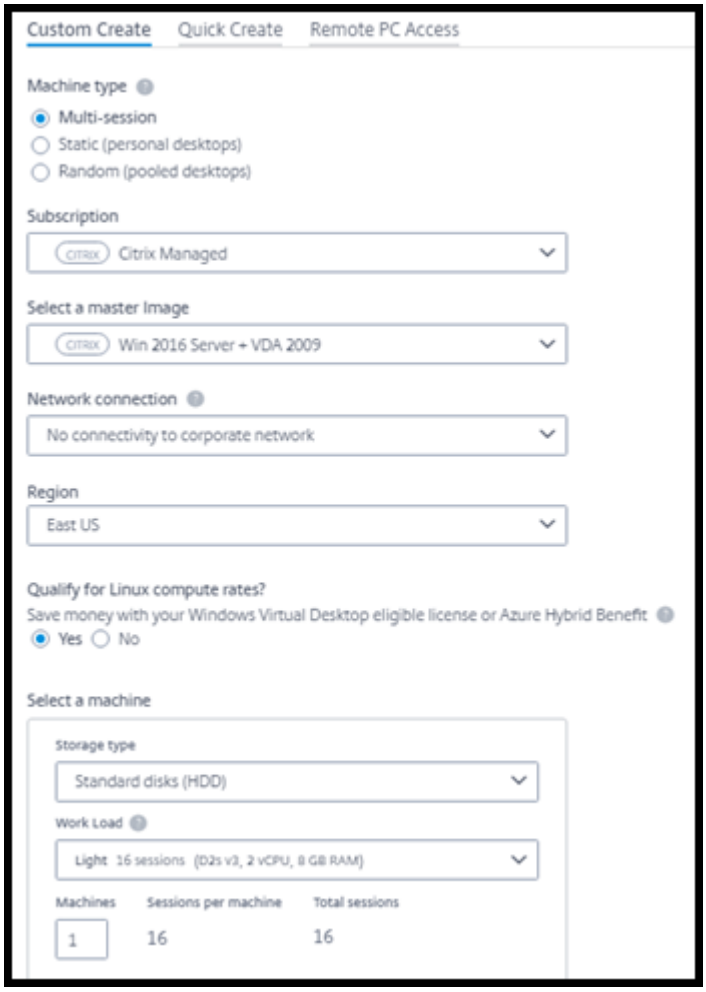
4. Si un catalogue n'a pas encore été créé, vous accédez à la page d'**accueil**. Sélectionnez **Mise en route**. À la fin de la page d'introduction, vous accédez au tableau de bord **Gérer > Déploiement rapide** . Sélectionnez **Créer un catalogue**.



Si un catalogue a déjà été créé, vous accédez au tableau de bord **Gérer > Déploiement rapide** . Sélectionnez **Créer un catalogue**.



5. Sélectionnez **Création personnalisée** en haut de la page, si ce n'est pas déjà fait.



6. Renseignez les champs suivants : (Certains champs sont valides uniquement pour certains types de machines. L'ordre des champs peut différer.)

   - **Type de machine** : sélectionnez un type de machine Pour plus d'informations, consultez la section Types de machines.
   - **Abonnement** : Sélectionnez un abonnement Azure.
   - **Image principale :** sélectionnez une image de système d'exploitation à utiliser pour les machines du catalogue.
   - **Connexion réseau :** sélectionnez la connexion réseau à utiliser pour accéder aux ressources de votre réseau.

     Si vous avez sélectionné un abonnement Azure géré par Citrix, les choix qui s'offrent à vous sont les suivants :

     - **Aucune connectivité :** l'utilisateur ne peut pas accéder aux emplacements et aux ressources de votre réseau d'entreprise local.

  - *Connexions :* sélectionnez une connexion précédemment créée, telle qu'un VNet peering ou une connexion SD-WAN.

  Si vous avez sélectionné un abonnement Azure géré par le client, sélectionnez le groupe de ressources, le réseau virtuel et le sous-réseau appropriés.

- **Région :** (disponible uniquement si vous avez sélectionné **Aucune connectivité** dans **Connexion réseau**.) Sélectionnez la région dans laquelle vous souhaitez créer les bureaux. Vous pouvez sélectionner une région proche de vos utilisateurs.

  Si vous avez sélectionné une connexion dans **Connexion réseau**, le catalogue utilise la région de ce réseau.

- **Vous êtes éligible aux taux de calcul Linux ?** (Disponible uniquement si vous avez sélectionné une image Windows.) Vous pouvez économiser de l'argent lorsque vous utilisez votre licence éligible ou Azure Hybrid Benefit.

  Avantage Windows Virtual Desktop : licences Windows 10 ou Windows 7 éligibles pour les licences utilisateurs pour :

  - Microsoft 365 E3/ES
  - Avantages d'utilisation de Microsoft 365 A3/AS/Student
  - Microsoft 365 F3
  - Microsoft 365 Business Premium
  - Windows 10 Entreprise E3/E5
  - Windows 10 Education A3/A5
  - VDA Windows 10 par utilisateur

  Licence d'accès client aux services Bureau à distance par utilisateur ou par appareil avec Software Assurance pour les charges de travail Windows Server.

  Avantage Azure Hybrid : licences Windows Server avec Software Assurance active ou les licences d'abonnement éligibles équivalentes. Voir https://azure.microsoft.com/en-us/pricing/hybrid-benefit/.

- **Machine :**

  - **Type de stockage**. HDD ou SSD.
  - **Performances de la machine** (pour types de machines **Statique** ou **Aléatoire**) ou **Charge de travail** (pour le type de machine à sessions multiples). Les choix comprennent uniquement les options correspondant au type de génération (gen1 ou gen2) de l'image que vous avez sélectionnée.

    Si vous sélectionnez la charge de travail personnalisée, saisissez le nombre de machines et de sessions par machine dans le champ **Performances des machines**.
  - **Machines**. Le nombre de machines que vous souhaitez dans ce catalogue.

- **Schéma de dénomination de machines :** voir Schéma de dénomination de machines.
- **Nom :** saisissez un nom pour le catalogue. Ce nom figure sur le tableau de bord **Gérer**.
- **Planification de l'alimentation :** par défaut, la case **Je configurerai cette option plus tard** est cochée. Pour plus de détails, voir Programmes de gestion de l'alimentation. (Ce programme de gestion de l'alimentation diffère des fonctionnalités de gestion de l'alimentation disponibles dans l'interface de gestion Configuration complète de Citrix DaaS.)
- **Rejoignez le domaine Active Directory local :** (disponible uniquement si vous avez sélectionné une connexion Azure VNet peering dans **Connexion réseau**.) Sélectionnez **Oui** ou **Non**. Si vous sélectionnez **Oui**, saisissez les éléments suivants :
  - Nom de domaine complet du domaine (par exemple, Contoso.com).
  - Unité d'organisation : pour utiliser l'unité d'organisation par défaut (ordinateurs), laissez ce champ vide.
  - Nom du compte de Citrix DaaS : doit être un administrateur de domaine ou d'entreprise au format nom@domaine ou domaine\nom.
  - Mot de passe pour le nom de compte Citrix DaaS.
- **Paramètres avancés :** reportez-vous à la section Paramètres d'emplacement des ressources lors de la création d'un catalogue.

7. Lorsque vous avez terminé, sélectionnez **Créer un catalogue**.
8. S'il s'agit du premier catalogue que vous créez à l'aide d'un abonnement Azure géré par Citrix, lorsque vous y êtes invité, reconnaissez votre responsabilité pour les frais associés.

Le tableau de bord **Gérer > Déploiement rapide** indique quand votre catalogue est créé. Citrix DaaS crée également automatiquement un emplacement de ressources et ajoute deux Citrix Cloud Connectors.

Que faire ensuite :

- Si vous ne l'avez pas déjà fait, configurez la méthode d'authentification pour que vos utilisateurs s'authentifient sur Citrix Workspace.
- Une fois le catalogue créé, ajoutez des utilisateurs au catalogue.
- Si vous avez créé un catalogue à sessions multiples, ajoutez des applications (avant ou après l'ajout d'utilisateurs).

Paramètres d'emplacement des ressources lors de la création d'un catalogue

Lors de la création d'un catalogue, vous pouvez éventuellement configurer plusieurs paramètres d'emplacement de ressources.

Lorsque vous sélectionnez **Paramètres avancés** dans la boîte de dialogue de création de catalogue, Citrix DaaS récupère les informations d'emplacement des ressources.

- Si vous disposez déjà d'un emplacement des ressources pour le domaine et la connexion réseau sélectionnés pour le catalogue, vous pouvez l'enregistrer pour qu'il soit utilisé par le catalogue que vous créez.

  Si cet emplacement des ressources ne possède qu'un seul Cloud Connector, un autre est installé automatiquement. Vous pouvez éventuellement spécifier des paramètres avancés pour le Cloud Connector que vous ajoutez.
- Si aucun emplacement de ressources n'est configuré pour le domaine et la connexion réseau sélectionnés pour le catalogue, vous êtes invité à en configurer un.

Configuration des paramètres avancés :

- (Obligatoire uniquement lorsque l'emplacement des ressources est déjà configuré.) Le nom de l'emplacement des ressources.
- Type de connectivité externe : via le service Citrix Gateway ou depuis votre réseau d'entreprise.
- Paramètres de Cloud Connector :
  - (Disponible uniquement en cas d'utilisation d'un abonnement Azure géré par le client) Performances de la machine. Cette sélection est utilisée pour les Cloud Connectors dans l'emplacement des ressources.
  - (Disponible uniquement lorsque vous utilisez un abonnement Azure géré par le client) Groupe de ressources Azure. Cette sélection est utilisée pour les Cloud Connectors dans l'emplacement des ressources. La valeur par défaut est le groupe de ressources utilisé pour la dernière fois par l'emplacement des ressources (le cas échéant).
  - l'unité d'organisation. La valeur par défaut est la dernière unité d'organisation utilisée par l'emplacement des ressources (le cas échéant).

Lorsque vous avez terminé les paramètres avancés, sélectionnez **Enregistrer** pour revenir à la boîte de dialogue de création du catalogue.

Une fois que vous avez créé un catalogue, plusieurs actions d'emplacement des ressources sont disponibles. Pour plus de détails, voir Actions d'emplacement des ressources.

Schéma de dénomination de machines

Pour spécifier un schéma de dénomination de machines lors de la création d'un catalogue, sélectionnez **Spécifier un schéma de dénomination de machines**. Utilisez entre 1 et 4 caractères génériques (caractère hash) pour indiquer où des chiffres ou des lettres séquentiels apparaissent dans le nom. Règles :

- Le schéma de dénomination doit contenir entre un et quatre caractères génériques. Tous les caractères génériques doivent être regroupés.
- Le nom complet, y compris les caractères génériques, doit comporter entre 2 et 15 caractères.
- Un nom ne peut pas inclure des blancs (espaces), des barres obliques, des barres obliques inverses, des deux-points, des astérisques, des crochets, des pipe, des virgules, des tildes, des points d'exclamation, des signes de dollar, des signes de pourcentage, des carets, des parenthèses, des accolades ou des traits de soulignement.
- Un nom ne peut pas commencer par un point.
- Un nom ne peut contenir que des chiffres.
- N'utilisez pas les caractères suivantes à la fin d'un nom : `-GATEWAY`, `-GW`, et `-TAC`.

Indiquez si les valeurs séquentielles sont des chiffres (0-9) ou des lettres (A-Z).

Par exemple, un schéma de dénomination de `PC-Sales-##` (avec **0 à 9** sélectionné) donne lieu à des comptes d'ordinateur nommés `PC-Sales-01`, `PC-Sales-02`, `PC-Sales-03`, etc.

Laissez suffisamment de place pour d'éventuels autres éléments.

- Par exemple, un schéma de dénomination comportant 2 caractères génériques et 13 autres caractères (par exemple, `MachineSales-##`) utilise le nombre maximal de caractères (15).
- Une fois que le catalogue contient 99 machines, la création suivante échoue. Citrix DaaS essaie de créer une machine à trois chiffres (100), mais cette opération générerait un nom de 16 caractères. Le maximum est de 15.
- Ainsi, dans cet exemple, un nom plus court (par exemple `PC-Sales-##`) permet d'aller au-delà de 99 machines.

Si vous ne spécifiez pas de schéma de dénomination de machine, Citrix DaaS utilise le schéma de dénomination par défaut `DAS%%%%%-**-###`.

- `%%%%%` = cinq caractères alphanumériques aléatoires correspondant au préfixe d'emplacement des ressources
- `**` = deux caractères alphanumériques aléatoires pour le catalogue
- `###` = trois chiffres.

Informations connexes

- Catalogues Remote PC Access
- Créer un catalogue dans un réseau utilisant un serveur proxy
- Afficher les informations sur le catalogue
- Gérer les catalogues dans Déploiement rapide

Gérer les catalogues dans Déploiement rapide

April 27, 2022

Cet article décrit les tâches de gestion de catalogue que vous pouvez utiliser pour gérer les catalogues créés dans Déploiement rapide.

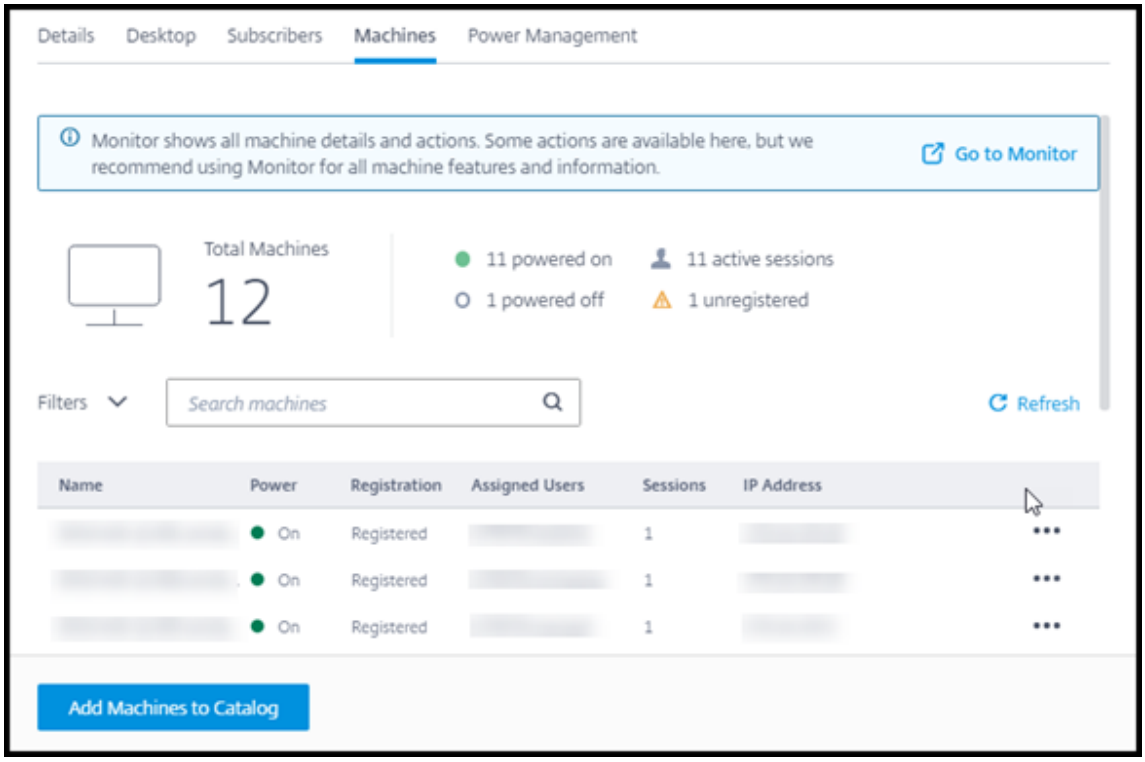
N'oubliez pas : si vous avez utilisé Déploiement rapide pour créer un catalogue et avez ensuite utilisé l'interface Configuration complète pour effectuer des tâches de gestion sur ce catalogue, vous ne pouvez plus utiliser l'interface Déploiement rapide pour ce catalogue.

(Pour plus d'informations concernant la gestion des catalogues dans l'interface de gestion Configuration complète, reportez-vous à la section Gérer les catalogues de machines.)

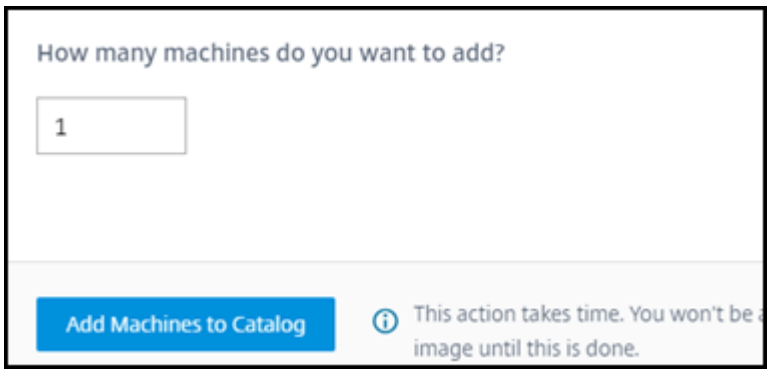
Ajouter des machines à un catalogue

Pendant que des machines sont ajoutées à un catalogue de déploiement rapide, vous ne pouvez pas apporter d'autres modifications à ce catalogue.

1. Dans **Gérer > Déploiement rapide**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Machines**, sélectionnez **Ajouter des machines au catalogue**.



3. Saisissez le nombre de machines que vous souhaitez ajouter au catalogue.



4. (Valide uniquement si le catalogue est joint à un domaine.) Saisissez le nom d'utilisateur et le mot de passe du compte Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).
5. Sélectionnez **Ajouter des machines au catalogue**.

Vous ne pouvez pas réduire le nombre de machines pour un catalogue. Vous pouvez toutefois utiliser les paramètres de calendriers de gestion de l'alimentation pour contrôler le nombre de machines sous tension ou supprimer des machines individuelles depuis l'onglet **Machines**. Reportez-vous à la section Gérer les machines dans un catalogue pour plus d'informations sur la suppression de machines de l'onglet **Machines**.

Modifier le nombre de sessions par machine

La modification du nombre de sessions par machine à sessions multiples peut affecter l'expérience utilisateur. L'augmentation de cette valeur peut réduire les ressources de calcul allouées à des sessions simultanées.

Recommandation : observez vos données d'utilisation pour déterminer l'équilibre approprié entre l'expérience utilisateur et le coût.

1. Dans **Gérer > Déploiement rapide**, sélectionnez un catalogue contenant des machines à sessions multiples.
2. Dans l'onglet **Détails**, sélectionnez **Modifier** en regard de **Sessions par machine**.
3. Saisissez un nouveau nombre de sessions par machine.
4. Sélectionnez **Mettre à jour le nombre de sessions**.
5. Confirmez votre demande.

Cette modification n'affecte pas les sessions en cours. Lorsque vous modifiez le nombre maximum de sessions par une valeur inférieure à celle des sessions actuellement actives d'une machine, la nouvelle valeur est implémentée via l'attrition normale des sessions actives.

Si un échec survient avant le début du processus de mise à jour, l'affichage **Détails** du catalogue conserve le nombre correct de sessions. Si un échec survient pendant le processus de mise à jour, l'écran indique le nombre de sessions souhaitées.

Gérer les machines dans un catalogue

> **Remarque :**
>
> La plupart des actions disponibles dans **Gérer > Déploiement rapide** sont également disponibles dans l'onglet **Surveiller** dans Déploiement rapide.

Pour sélectionner des actions dans **Gérer > Déploiement rapide** :

1. Dans **Gérer > Déploiement rapide**, cliquez n'importe où dans l'entrée d'un catalogue.
2. Dans l'onglet **Machines**, recherchez la machine que vous souhaitez gérer. Dans le menu des points de suspension de cette machine, sélectionnez l'action souhaitée :

   - **Redémarrer :** redémarre la machine sélectionnée.
   - **Démarrer :** démarre la machine sélectionnée. Cette action n'est disponible que si la machine est hors tension.
   - **Arrêt :** arrête la machine sélectionnée. Cette action n'est disponible que si la machine est sous tension.
   - **Activer/désactiver le mode de maintenance :** active le mode de maintenance (s'il est désactivé) ou le désactive (s'il est activé) pour la machine sélectionnée. Par défaut, le mode de maintenance d'une machine est désactivé.

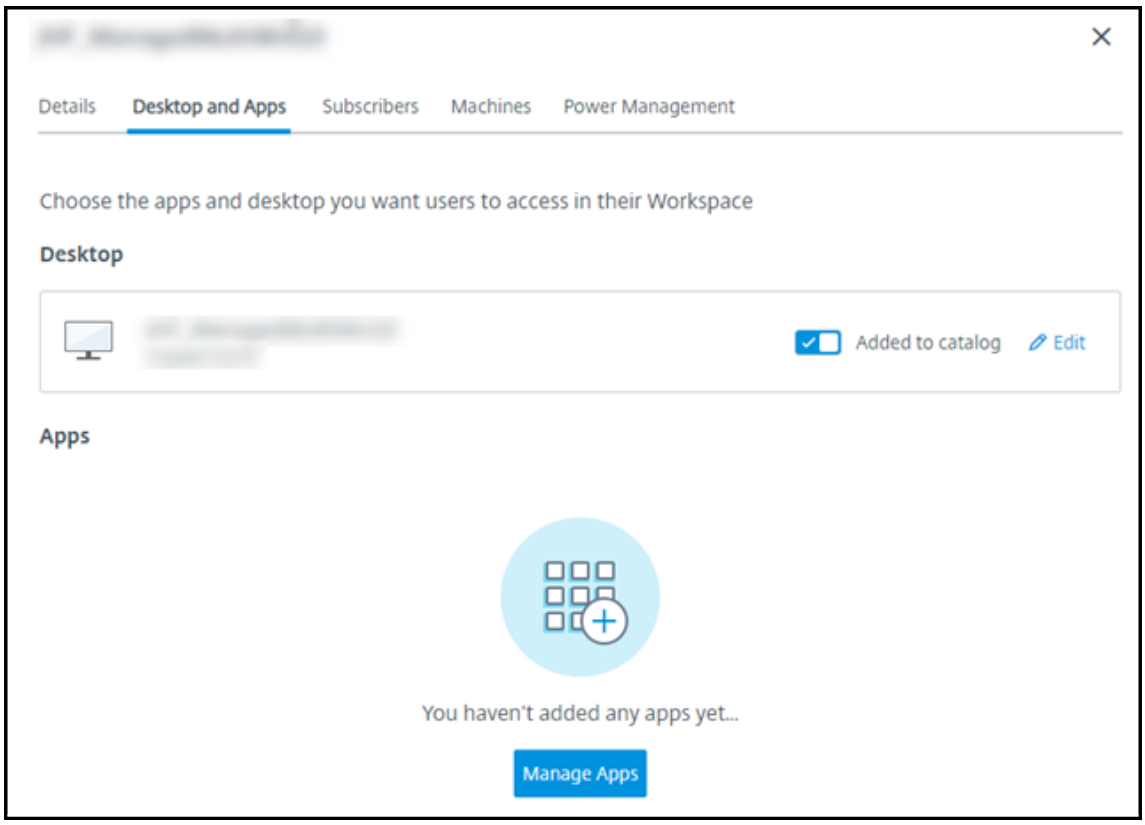
     L'activation du mode de maintenance empêche toute nouvelle connexion à la machine. L'utilisateur peut se connecter à des sessions existantes sur cette machine, mais ne peut pas démarrer de nouvelles sessions sur cette machine.

     Vous pouvez placer une machine en mode de maintenance avant d'appliquer des correctifs ou pour le dépannage.
   - **Supprimer :** supprime la machine sélectionnée. Cette action est disponible uniquement lorsque le nombre de sessions de la machine est égal à zéro. Confirmez la suppression.

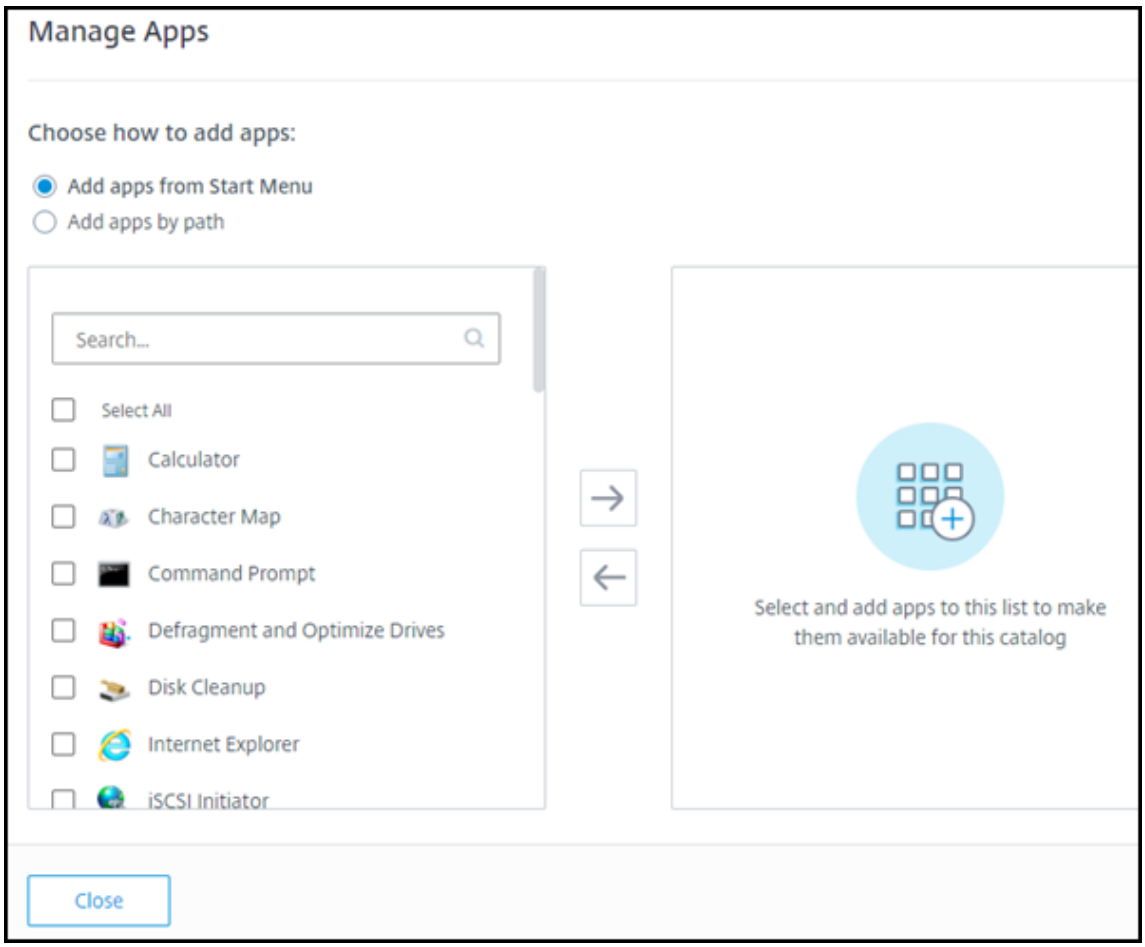
     Lorsqu'une machine est supprimée, toutes les données de la machine sont supprimées.
   - **Forcer le redémarrage :** force le redémarrage de la machine sélectionnée. Sélectionnez cette action uniquement en cas d'échec d'une action **Redémarrer** de la machine.

Ajouter des applications à un catalogue

1. Dans **Gérer > Déploiement rapide**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Bureau et applications**, sélectionnez **Gérer les applications**.

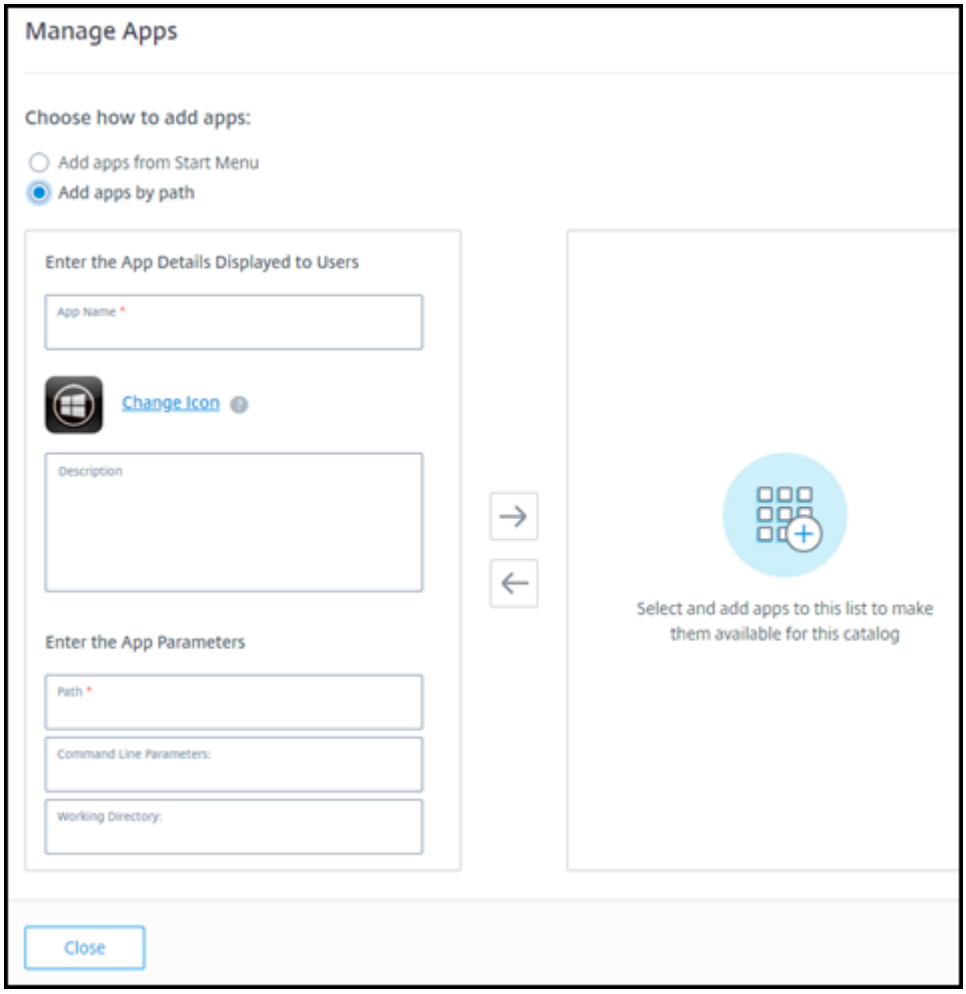


3. Sélectionnez la façon dont vous ajoutez des applications : dans le menu **Démarrer** des machines du catalogue ou à partir d'un autre chemin sur les machines.
4. Pour ajouter des applications à partir du menu **Démarrer** :



- Sélectionnez les applications disponibles dans la colonne de gauche. (Utilisez la fonction **Recherche** pour personnaliser la liste des applications.) Sélectionnez la flèche droite entre les colonnes. Les applications sélectionnées se déplacent vers la colonne de droite.
- De même, pour supprimer des applications, sélectionnez-les dans la colonne de droite. Sélectionnez la flèche gauche entre les colonnes.
- Si le menu **Démarrer** contient plusieurs versions de la même application qui portent le même nom, vous ne pouvez en ajouter qu'une. Pour ajouter une autre version de cette application, modifiez le nom de cette version. Vous pourrez ensuite ajouter cette version de l'application.

5. Pour ajouter des applications par chemin d'accès :



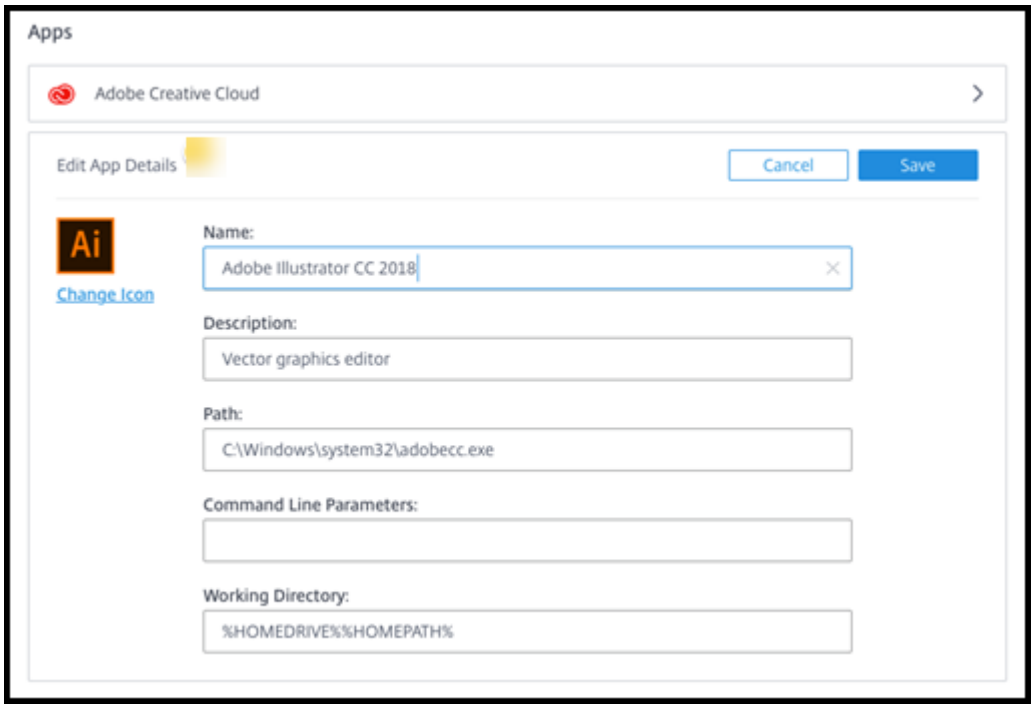
- Saisissez le nom de l'application. Il s'agit du nom que les utilisateurs voient dans Citrix Workspace.
- L'icône affichée est l'icône que les utilisateurs voient dans Citrix Workspace. Pour sélectionner une autre icône, sélectionnez **Changer d'icône** et accédez à l'icône que vous souhaitez afficher.
- (Facultatif) Saisissez une description de l'application.
- Saisissez le chemin d'accès à l'application. Ce champ est obligatoire. Vous pouvez également ajouter des paramètres de ligne de commandes et le répertoire de travail. Pour plus de détails sur les paramètres de ligne de commande, voir Passer des paramètres aux applications publiées.

6. Lorsque vous avez terminé, sélectionnez **Fermer**.

Sur les VDA Windows Server 2019, certaines icônes d'application peuvent ne pas apparaître correctement pendant la configuration et dans l'espace de travail des utilisateurs. Pour résoudre le problème, une fois l'application publiée, modifiez l'application et utilisez la fonction **Changer d'icône** pour attribuer une autre icône qui s'affiche correctement.

Modifier une application dans un catalogue

1. Dans **Gérer > Déploiement rapide**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Bureau et applications**, cliquez n'importe où sur la ligne contenant l'application que vous souhaitez modifier.
3. Sélectionnez l'icône en forme de crayon.



4. Saisissez vos modifications dans l'un des champs suivants :
   - **Nom :** le nom que les utilisateurs voient dans Citrix Workspace.
   - **Description**
   - **Chemin :** chemin d'accès à l'exécutable.
   - **Paramètres de ligne de commande :** pour plus d'informations, voir Passer des paramètres aux applications publiées.
   - **Répertoire de travail**
5. Pour modifier l'icône que les utilisateurs voient dans leur Citrix Workspace, sélectionnez **Changer d'icône** et accédez à l'icône que vous souhaitez afficher.
6. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

Passer des paramètres aux applications publiées

Lorsque vous associez des types de fichier à une application publiée, les symboles pourcentage et astérisque (entre guillemets) sont ajoutés à la fin de la ligne de commandes 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 commandes pour éviter la validation de ligne de commandes. 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 pourcentage et astérisque. Ajoutez une espace entre le guillemet de clôture du chemin et le guillemet d'ouverture pour les symboles de pourcentage et d'astérisque.

  Par exemple, la ligne de commandes pour l'application publiée Windows Media Player est : `"C:\Program Files\Windows Media Player\mplayer1.exe" "%*"`

Supprimer des applications d'un catalogue

La suppression d'une application d'un catalogue ne la supprime pas des machines. Elle l'empêche simplement d'apparaître dans Citrix Workspace.

1. Dans **Gérer > Déploiement rapide**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Bureau et applications**, sélectionnez l'icône de corbeille en regard des applications que vous souhaitez supprimer.

Supprimer un catalogue

Lorsque vous supprimez un catalogue, toutes les machines du catalogue sont définitivement détruites. La suppression d'un catalogue ne peut pas être annulée.

1. Dans **Gérer > Déploiement rapide**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Détails**, sélectionnez **Supprimer le catalogue**.
3. Confirmez la suppression.

Pour aider à identifier les comptes de machines Active Directory résiduels que vous devez supprimer, vous pouvez télécharger une liste de noms de machines et de Cloud Connector.

Gérer les calendriers de gestion de l'alimentation

Un calendrier de gestion de l'alimentation concerne toutes les machines d'un catalogue. Un calendrier assure :

- Une expérience utilisateur optimale : les machines sont disponibles pour les utilisateurs lorsqu'elles sont nécessaires.
- La sécurité : les sessions de bureau qui restent inactives pendant un intervalle spécifié sont déconnectées, ce qui oblige l'utilisateur à lancer une nouvelle session dans son espace de travail.
- La gestion des coûts et des économies d'énergie : les machines dont les bureaux restent inactifs sont mises hors tension. Les machines sont sous tension pour répondre à la demande planifiée et réelle.

Vous pouvez configurer un calendrier de gestion de l'alimentation lorsque vous créez un catalogue personnalisé ou le faire ultérieurement. Si aucun calendrier n'est sélectionné ou configuré, une machine s'éteint à la fin d'une session.

Vous ne pouvez pas sélectionner ou configurer un calendrier de gestion de l'alimentation lorsque vous créez un catalogue avec la création rapide. Par défaut, les catalogues créés à l'aide de la création rapide utilisent le calendrier prédéfini Économique. Vous pouvez sélectionner ou configurer un calendrier différent ultérieurement pour ce catalogue.

La gestion du calendrier comprend :

- connaître les informations contenues dans un calendrier ;
- créer un calendrier.

Informations contenues dans un calendrier

Le diagramme suivant illustre les paramètres de calendrier d'un catalogue contenant des machines à sessions multiples. Les paramètres d'un catalogue diffèrent légèrement s'il contient des machines à session unique (aléatoires ou statiques).

Un calendrier de gestion de l'alimentation contient les informations suivantes.

Calendriers prédéfinis Citrix DaaS propose plusieurs calendriers prédéfinis. Vous pouvez également configurer et enregistrer des calendriers personnalisés. Bien que vous puissiez supprimer des horaires prédéfinis personnalisés, vous ne pouvez pas supprimer les horaires prédéfinis fournis par Citrix.

Fuseau horaire Utilisé avec le réglage des machines sous tension pour établir les heures de travail et après les heures de travail, en fonction du fuseau horaire sélectionné.

Ce paramètre est valide pour tous les types de machines.

Machines sous tension : heures de travail et après les heures de travail Les jours de la semaine et les heures de début/fin de la journée qui constituent vos heures de travail. Ce paramètre indique généralement les intervalles où vous souhaitez que les machines soient sous tension. Tout moment en dehors de ces intervalles est considéré comme étant après les heures de travail. Plusieurs paramètres de calendrier vous permettent de saisir des valeurs distinctes pour les heures de travail et après les heures de travail. D'autres paramètres s'appliquent en permanence.

Ce paramètre est valide pour tous les types de machines.

Déconnecter les sessions de bureau en cas d'inactivité La durée d'inactivité d'un bureau (le temps où celui-ci n'est pas utilisé) avant que la session ne soit déconnectée. Une fois qu'une session est déconnectée, l'utilisateur doit accéder à Workspace et redémarrer un bureau. Il s'agit d'un paramètre de sécurité.

Ce paramètre est valide pour tous les types de machines. Un seul paramètre s'applique en permanence.

Éteindre les bureaux inactifs Il s'agit du temps qu'une machine peut rester déconnectée avant d'être mise hors tension. Une fois qu'une machine est mise hors tension, l'utilisateur doit se rendre dans Workspace et redémarrer un bureau. Il s'agit d'un paramètre d'économie d'énergie.

Par exemple, supposons que vous souhaitiez que les bureaux se déconnectent après avoir été inactifs pendant 10 minutes. Ensuite, mettez les machines hors tension si elles restent déconnectées pendant 15 minutes supplémentaires.

Si Tom cesse d'utiliser son bureau pour assister à une réunion d'une heure, le bureau sera déconnecté au bout de 10 minutes. Après 15 minutes supplémentaires, la machine sera mise hors tension (25 minutes au total).

Du point de vue de l'utilisateur, les deux paramètres d'inactivité (déconnexion et mise hors tension) ont le même effet. Si Tom s'éloigne de son bureau pendant 12 minutes ou une heure, il doit redémarrer un bureau depuis Workspace. La différence entre les deux horloges affecte l'état de la machine virtuelle fournissant le bureau.

Ce paramètre est valide pour les machines à session unique (statiques ou aléatoires). Vous pouvez saisir des valeurs pour les heures de travail et après les heures de travail.

Fermer les sessions déconnectées Il s'agit du temps qu'une machine peut rester déconnectée avant la fermeture de la session.

Ce paramètre est valide pour les machines à sessions multiples. Un seul paramètre s'applique en permanence.

Délai de mise hors tension Il s'agit de la durée minimale pendant laquelle une machine doit être mise sous tension avant d'être éligible à la mise hors tension (ainsi que d'autres critères). Ce paramètre empêche les machines de s'allumer et de s'éteindre sans cesse pendant les demandes de session volatiles.

Ce paramètre est valide pour les machines à sessions multiples et s'applique en permanence.

Nombre minimum de machines en fonctionnement Il s'agit du nombre de machines qui doivent rester sous tension, indépendamment de la durée pendant laquelle elles sont inactives ou déconnectées.

Ce paramètre est valide pour les machines aléatoires et à sessions multiples. Vous pouvez saisir des valeurs pour les heures de travail et après les heures de travail.

Tampon de capacité Un tampon de capacité permet de répondre aux pics soudains de la demande, en gardant un tampon de machines sous tension. Le tampon est indiqué en pourcentage de la demande de session actuelle. Par exemple, si 100 sessions sont actives et que la mémoire tampon de capacité est de 10 %, Citrix DaaS fournit une capacité de 110 sessions. Un pic de demande peut survenir pendant les heures de travail ou l'ajout de nouvelles machines au catalogue.

Une valeur moindre diminue le coût. Une valeur supérieure contribue à assurer une expérience utilisateur optimisée. Lors du lancement de sessions, l'utilisateur n'a pas besoin d'attendre que des machines supplémentaires s'allument.

Lorsqu'un nombre plus que suffisant de machines est présent pour prendre en charge le nombre de machines sous tension nécessaires dans le catalogue (y compris le tampon de capacité), les machines supplémentaires sont mises hors tension. La mise hors tension peut se produire en raison d'une heure creuse, de fermetures de session ou d'un nombre réduit de machines dans le catalogue. La décision d'éteindre une machine doit répondre aux critères suivants :

- La machine est sous tension et n'est pas en mode de maintenance.
- La machine est enregistrée comme disponible ou attend de s'enregistrer après la mise sous tension.
- La machine n'a aucune session active. Toutes les sessions restantes sont terminées. (La machine était inactive pendant la période d'inactivité.)

- La machine est sous tension pendant au moins « X » minutes, où « X » correspond au délai de mise hors tension spécifié pour le catalogue.

  Dans un catalogue statique, une fois que toutes les machines du catalogue sont affectées, le tampon de capacité ne joue aucun rôle dans la mise sous tension ou hors tension des machines.

Ce paramètre est valide pour tous les types de machines. Vous pouvez saisir des valeurs pour les heures de travail et après les heures de travail.

Créer un calendrier de gestion de l'alimentation

1. Dans **Gérer > Déploiement rapide**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Gestion de l'alimentation**, déterminez si l'un des calendriers prédéfinis (dans le menu en haut) répondent à vos besoins. Sélectionnez un préréglage pour voir les valeurs qu'il utilise. Si vous souhaitez utiliser un préréglage, laissez-le sélectionné.
3. Si vous modifiez les valeurs de n'importe quel champ (par exemple, jours, heures ou intervalles), la sélection de préréglage passe automatiquement à **Personnalisé**. Un astérisque indique que les paramètres personnalisés n'ont pas été enregistrés.
4. Définissez les valeurs souhaitées pour le calendrier personnalisé.
5. Sélectionnez **Personnalisé** en haut, puis enregistrez les paramètres actuels en tant que nouveau préréglage. Saisissez un nom pour le nouveau préréglage et cochez la case.
6. Lorsque vous avez terminé, sélectionnez **Enregistrer les modifications**.

Vous pourrez par la suite modifier ou supprimer un préréglage personnalisé à l'aide des icônes de crayon ou de corbeille du menu **Préréglages**. Vous ne pouvez pas modifier ou supprimer des préréglages courants.

Informations connexes

- Mettre à jour un catalogue avec une nouvelle image
- Ajouter et supprimer des utilisateurs dans un catalogue

Abonnements Azure dans Déploiement rapide

May 17, 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.

Introduction

Lorsque vous créez un catalogue ou une image dans Déploiement rapide, vous choisissez parmi les abonnements Azure disponibles. Déploiement rapide prend en charge les abonnements Azure gérés par Citrix ainsi que vos propres abonnements Azure gérés par le client.

- Pour utiliser votre propre abonnement Azure, vous devez d'abord importer (ajouter) un ou plusieurs de ces abonnements à Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Cette action permet à Citrix DaaS d'accéder à vos abonnements Azure.
- L'utilisation d'un abonnement Azure géré par Citrix ne nécessite aucune configuration d'abonnement. Toutefois, un abonnement Azure géré par Citrix n'est disponible que lorsque vous commandez Citrix Azure Consumption Fund, en plus de Citrix DaaS.

Certaines fonctionnalités de Citrix DaaS diffèrent selon que le catalogue utilise un abonnement Azure géré par Citrix ou votre propre abonnement Azure.

Abonnement Azure géré par Citrix	Votre propre abonnement Azure
Prend en charge les machines jointes au domaine ou n'appartenant pas au domaine.	Prend en charge uniquement les machines jointes au domaine.
Prend en charge les catalogues à création rapide et à création personnalisée.	Prend en charge uniquement les catalogues à création personnalisée.
Toujours disponible lors de la création de catalogues et d'images.	Vous devez ajouter l'abonnement Azure au service avant de créer un catalogue.
Pour l'authentification utilisateur, prend en charge Azure Active Directory géré par Citrix ou votre propre Active Directory.	Peut connecter votre propre Active Directory et Azure Active Directory.
Les options de connexion réseau incluent **Aucune connectivité**.	Les options de connexion réseau incluent uniquement vos propres réseaux virtuels.
Lorsque vous utilisez le peering de réseau virtuel Azure pour vous connecter à vos ressources, vous devez créer une connexion homologue de réseau virtuel dans Citrix DaaS.	Sélectionnez un réseau virtuel existant.
Lorsque vous importez une image depuis Azure, vous spécifiez l'URI de l'image.	Lorsque vous importez une image, vous pouvez sélectionner un disque dur virtuel ou parcourir le stockage dans l'abonnement Azure.

Abonnement Azure géré par Citrix	Votre propre abonnement Azure
Peut créer une machine bastion dans l'abonnement Azure du client pour résoudre les problèmes de machines.	Il n'est pas nécessaire de créer une machine bastion, car vous pouvez déjà accéder aux machines de votre abonnement.

Afficher les abonnements Azure

Pour afficher les détails de l'abonnement Azure, dans **Gérer > Déploiement rapide**, développez **Abonnements Cloud** sur la droite. Sélectionnez ensuite une entrée d'abonnement.

- La page **Détails** inclut le nombre de machines, ainsi que les numéros et noms des catalogues et des images utilisant l'abonnement.
- La page **Emplacements des ressources** répertorie les emplacements de ressources où l'abonnement est utilisé.

Ajouter des abonnements Azure gérés par le client

Pour utiliser un abonnement Azure géré par le client, vous devez l'ajouter à Citrix DaaS avant de créer un catalogue ou une image qui utilise cet abonnement. Deux options s'offrent à vous lorsque vous ajoutez vos abonnements Azure :

- **Si vous êtes administrateur général pour le répertoire et que vous disposez d'autorisations de propriétaire pour l'abonnement :** il suffit de vous authentifier auprès de votre compte Azure.
- **Si vous n'êtes pas administrateur général et que vous disposez d'autorisations de propriétaire sur l'abonnement :** avant d'ajouter l'abonnement à Citrix DaaS, créez une application Azure dans votre Azure Active Directory, puis ajoutez cette application en tant que contributeur de l'abonnement. Lorsque vous ajoutez cet abonnement à Citrix DaaS, vous fournissez des informations pertinentes sur l'application.

Ajouter des abonnements Azure gérés par le client si vous êtes administrateur général

Cette tâche nécessite des autorisations d'administrateur global pour le répertoire et des autorisations de propriétaire pour l'abonnement.

1. Dans **Gérer > Déploiement rapide**, développez **Abonnements Cloud** sur la droite.
2. Sélectionnez **Ajouter un abonnement Azure**.
3. Sur la page **Ajouter des abonnements**, sélectionnez **Ajouter votre abonnement Azure**.

4. Sélectionnez le bouton qui permet à Citrix DaaS d'accéder à vos abonnements Azure en votre nom.
5. Sélectionnez **Authentifier le compte Azure**. Vous accédez à la page de connexion Azure.
6. Saisissez vos informations d'identification Azure.
7. Vous êtes automatiquement renvoyé à Citrix DaaS. La page **Ajouter un abonnement** répertorie les abonnements Azure découverts. Utilisez la zone de recherche pour filtrer la liste, si nécessaire. Sélectionnez un ou plusieurs abonnements. Lorsque vous avez terminé, sélectionnez **Ajouter des abonnements**.
8. Confirmez que vous souhaitez ajouter les abonnements sélectionnés.

Les abonnements Azure que vous avez sélectionnés sont répertoriés lorsque vous développez **Abonnements**. Les abonnements ajoutés peuvent être sélectionnés lorsque vous créez un catalogue ou une image.

Ajouter des abonnements Azure gérés par le client si vous n'êtes pas administrateur général

L'ajout d'un abonnement Azure lorsque vous n'êtes pas administrateur général est un processus en deux étapes :

- Avant d'ajouter un abonnement à Citrix DaaS, créez une application dans Azure AD, puis ajoutez cette application en tant que contributeur de l'abonnement.
- Ajoutez l'abonnement à Citrix DaaS en utilisant des informations sur l'application que vous avez créée dans Azure.

Créer une application dans Azure Active Directory et l'ajouter en tant que contributeur

1. Enregistrez une nouvelle application dans Azure Active Directory :
   a) À partir d'un navigateur, accédez à https://portal.azure.com.
   b) Dans le menu supérieur gauche, sélectionnez **Azure Active Directory**.
   c) Dans la liste **Gérer**, sélectionnez **Enregistrements d'applications**.
   d) Sélectionnez **+ Nouvelle inscription**.
   e) Sur la page **Enregistrer une application**, fournissez les informations suivantes :
      - **Nom :** saisissez le nom de la connexion
      - **Type d'application :** sélectionnez une **application Web/API**
      - **URI de redirection :** laissez ce champ vide
   f) Sélectionnez **Créer**.
2. Créez la clé d'accès secrète de l'application et ajoutez l'attribution de rôle :

a) Dans la procédure précédente, sélectionnez **Enregistrement de l'application** pour afficher les détails.

b) Notez l'**ID d'application** et l'**ID de répertoire**. Vous l'utiliserez ultérieurement lors de l'ajout de votre abonnement à Citrix DaaS.

c) Sous **Gérer**, sélectionnez **Certificats et secrets**.

d) Sur la page **Clés secrètes clients**, sélectionnez **+ Nouvelle clé secrète client**.

e) Sur la page **Ajouter une clé secrète client**, fournissez une description et sélectionnez un intervalle d'expiration. Sélectionnez ensuite **Ajouter**.

f) Notez la valeur de la clé secrète client. Vous l'utiliserez ultérieurement lors de l'ajout de votre abonnement à Citrix DaaS.

g) Sélectionnez l'abonnement Azure que vous souhaitez lier (ajouter) à Citrix DaaS, puis sélectionnez **Contrôle d'accès (IAM)**.

h) Dans la zone **Ajouter une attribution de rôle**, sélectionnez **Ajouter**.

i) Dans l'onglet **Ajouter une attribution de rôle**, sélectionnez les éléments suivants :

- **Rôle :** contributeur
- **Attribuer l'accès à :** utilisateur, groupe ou principal du service Azure Active Directory
- **Sélectionnez :** nom de l'application Azure que vous avez créée précédemment.

j) Sélectionnez **Save**.

Ajoutez votre abonnement à Citrix DaaS Vous avez besoin de l'ID d'application, de l'ID de répertoire et de la valeur de la clé secrète client de l'application que vous avez créée dans Azure AD.

1. Dans **Gérer > Déploiement rapide**, développez **Abonnements Cloud** sur la droite.
2. Sélectionnez **Ajouter un abonnement Azure**.
3. Sur la page **Ajouter des abonnements**, sélectionnez **Ajouter vos abonnements Azure**.
4. Sélectionnez **J'ai une application Azure avec un rôle de contributeur pour l'abonnement**
5. Saisissez l'ID de locataire (ID de répertoire), l'ID client (ID d'application) et la clé secrète client de l'application que vous avez créée dans Azure.
6. Sélectionnez **Sélectionner votre abonnement**, puis sélectionnez l'abonnement souhaité.

Ensuite, à partir de la page **Détails** de l'abonnement dans le tableau de bord Citrix DaaS, vous pouvez mettre à jour la clé secrète client ou remplacer l'application Azure à partir du menu des points de suspension.

Si Citrix DaaS ne peut pas accéder à un abonnement Azure après son ajout, plusieurs actions de gestion de l'alimentation du catalogue et de machines individuelles ne sont pas autorisées. Un message permet d'ajouter à nouveau l'abonnement. Si l'abonnement a été initialement ajouté à l'aide d'une application Azure, vous pouvez remplacer l'application Azure.

Ajouter des abonnements Azure gérés par Citrix

Un abonnement Azure géré par Citrix prend en charge un certain nombre de machines. (Dans ce contexte, les *machines* font référence aux machines virtuelles sur lesquelles un VDA Citrix est installé. Ces machines fournissent des applications et des bureaux aux utilisateurs. Il n'inclut pas d'autres machines dans un emplacement de ressources, telles que Cloud Connectors.)

Si votre abonnement Azure géré par Citrix est susceptible d'atteindre sa limite bientôt et que vous disposez de suffisamment de licences Citrix, vous pouvez demander un autre abonnement Azure géré par Citrix. Le tableau de bord contient une notification lorsque vous vous rapprochez de la limite.

Vous ne pouvez pas créer de catalogue (ou ajouter des machines à un catalogue) si le nombre total de machines pour tous les catalogues qui utilisent cet abonnement Azure géré par Citrix dépasserait la limite.

Par exemple, supposons une limite hypothétique de 1 000 machines par abonnement Azure géré par Citrix.

- Supposons que vous ayez deux catalogues (`Cat1` et `Cat2`) qui utilisent le même abonnement Azure géré par Citrix. `Cat1` contient actuellement 500 machines et `Cat2` en contient 250.
- Au fur et à mesure que vous planifiez les besoins futurs en capacité, vous ajoutez 200 machines à `Cat2`. L'abonnement Azure géré par Citrix prend désormais en charge 950 machines (500 dans `Cat 1` et 450 dans `Cat 2`). Le tableau de bord indique que l'abonnement est proche de sa limite.
- Lorsque vous avez besoin de 75 machines supplémentaires, vous ne pouvez pas utiliser cet abonnement pour créer un catalogue avec 75 machines (ou ajouter 75 machines à un catalogue existant). Cela dépasserait la limite d'abonnement. Au lieu de cela, vous demandez un autre abonnement Azure géré par Citrix. Vous pouvez ensuite créer un catalogue en utilisant cet abonnement.

Lorsque vous disposez de plusieurs abonnements Azure gérés par Citrix :

- Rien n'est partagé entre ces abonnements.
- Chaque abonnement porte un nom unique.
- Vous pouvez choisir parmi les abonnements Azure gérés par Citrix (et tous les abonnements Azure gérés par le client que vous avez ajoutés) lorsque :
  - vous créez un catalogue ;
  - vous créez ou importez une image ;
  - vous créez un peering de réseau virtuel ou une connexion SD-WAN.

Exigence :

- Vous devez disposer de suffisamment de licences Citrix pour justifier l'ajout d'un autre abonnement Azure géré par Citrix. Pour reprendre l'exemple hypothétique précédent, si vous disposez de 2 000 licences Citrix en prévision du déploiement d'au moins 1 500 machines via des abonnements gérés par Citrix, vous pouvez ajouter un autre abonnement Azure géré par Citrix.

Pour ajouter un abonnement Azure géré par Citrix :

1. Contactez votre représentant Citrix pour demander un autre abonnement Azure géré par Citrix. Vous êtes averti lorsque vous pouvez continuer.
2. Dans **Gérer > Déploiement rapide**, développez **Abonnements Cloud** sur la droite.
3. Sélectionnez **Ajouter un abonnement Azure**.
4. Sur la page **Ajouter des abonnements**, sélectionnez **Ajouter un abonnement Azure géré par Citrix**.
5. Sur la page **Ajouter un abonnement géré par Citrix**, sélectionnez **Ajouter un abonnement** au bas de la page.

Si vous êtes averti qu'une erreur s'est produite lors de la création d'un abonnement Azure géré par Citrix, contactez le support Citrix.

Supprimer les abonnements Azure

Avant de pouvoir supprimer un abonnement Azure, vous devez supprimer tous les catalogues et images qui l'utilisent.

Si vous possédez un ou plusieurs abonnements Azure gérés par Citrix, vous ne pouvez pas tous les supprimer. Vous devez en conserver au moins un.

1. Dans **Gérer > Déploiement rapide**, développez **Abonnements Cloud** sur la droite.
2. Sélectionnez l'entrée d'abonnement.
3. Dans l'onglet **Détails**, sélectionnez **Supprimer l'abonnement**.
4. Sélectionnez **Authentifier le compte Azure**. Vous accédez à la page de connexion Azure.
5. Saisissez vos informations d'identification Azure.
6. Vous êtes automatiquement renvoyé à Citrix DaaS. Confirmez la suppression, puis sélectionnez **Oui, Supprimer l'abonnement**.

Mettre à jour les clés secrètes client expirées

Lorsque la clé secrète client d'un abonnement expire, vous ne pouvez pas créer de catalogues de machines pour celui-ci et une alerte apparaît dans l'entrée de l'abonnement. Pour résoudre ce problème, deux possibilités s'offrent à vous :

- Mettre à jour la clé secrète client de l'application Azure en cours d'utilisation
- Basculer vers une application Azure avec une date d'expiration valide

Mettre à jour la clé secrète client de l'application Azure en cours d'utilisation

Pour continuer à utiliser l'application Azure existante pour accéder aux ressources Azure, procédez comme suit :

1. Dans Azure, créez une clé secrète client pour l'application Azure en cours d'utilisation. Notez la nouvelle clé secrète et la date d'expiration à des fins d'utilisation ultérieure. Pour plus d'informations, consultez la section Créer un secret d'application dans Azure.
2. Dans DaaS, indiquez les informations relatives à la nouvelle clé secrète dans l'abonnement. Les étapes détaillées sont les suivantes :

    a) Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** de Citrix DaaS pour Azure, développez **Abonnements Cloud** sur la droite.
    b) Cliquez sur l'abonnement dont les clés secrètes doivent être mises à jour.
    c) Sur la page d'abonnement qui s'affiche, cliquez sur le menu des points de suspension dans le volet **Détails de l'application Azure**, puis sélectionnez **Mettre à jour le secret client**.
    d) Sur la page **Mettre à jour le secret client**, saisissez la nouvelle **clé secrète client** et sa **date d'expiration**.
    e) Cliquez sur **Mettre à jour le secret**.

Basculer vers une application Azure avec une date d'expiration valide

Pour passer à une application Azure valide pour accéder aux ressources Azure, obtenez les informations nécessaires sur l'application et indiquez-les dans l'abonnement en procédant comme suit :

1. Dans Azure, procurez-vous une application Azure valide et notez-en les détails. Assurez-vous que le rôle de *contributeur* est attribué à la nouvelle application Azure. Pour plus d'informations, consultez la section Créer une application dans Azure Active Directory et l'ajouter en tant que contributeur.
2. Dans DaaS, indiquez les détails de l'application Azure dans l'abonnement. Les étapes détaillées sont les suivantes :

    a) Dans le tableau de bord **Gérer > Déploiement rapide d'Azure** de Citrix DaaS pour Azure, développez **Abonnements Cloud** sur la droite.
    b) Cliquez sur l'abonnement dont les clés secrètes doivent être mises à jour.
    c) Sur la page d'abonnement qui s'affiche, cliquez sur le menu des points de suspension dans le volet **Détails de l'application Azure**, puis sélectionnez **Remplacer l'application Azure**.
    d) Sur la page **Remplacer l'application Azure**, saisissez les détails de la nouvelle application Azure dans les champs correspondants suivants : **ID de répertoire (locataire)**, **ID d'**

application (client), **Clé secrète client** et **Date d'expiration de la clé secrète pour le principal du service**.

e) Cliquez sur **Remplacer l'application**.

Images dans Déploiement rapide

May 17, 2024

Lorsque vous créez un catalogue pour fournir des bureaux ou des applications, une image est utilisée (avec d'autres paramètres) comme modèle de création des machines.

Déploiement rapide fournit un ensemble d'images préparées que vous pouvez utiliser pour créer et personnaliser une image dans Déploiement rapide. Vous pouvez également importer (ajouter) des images à partir de votre propre abonnement Azure.

Images préparées par Citrix

Déploiement rapide fournit plusieurs images préparées par Citrix :

- Windows 11 Pro (mono-session)
- Windows 11 Enterprise Virtual Desktop (multi-session)
- Windows 11 Enterprise Virtual Desktop (multi-session) avec Office 365 ProPlus
- Windows 10 Pro (mono-session)
- Windows 10 Enterprise Virtual Desktop (multi-session)
- Windows 10 Enterprise Virtual Desktop (multi-session) avec Office 365 ProPlus
- Windows Server 2022 (multi-session)
- Windows Server 2019 (multi-session)
- Windows Server 2016 (multi-session)
- Linux Ubuntu 22.04 LTS (mono-session)
- Linux Ubuntu 22.04 LTS (multi-session)

Les images préparées par Citrix sont dotées d'un agent Citrix Virtual Delivery Agent (VDA) actuel et d'outils de dépannage installés. Le VDA est le mécanisme de communication entre les machines de vos utilisateurs et l'infrastructure Citrix Cloud qui gère Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Les images fournies par Citrix sont dotées d'une notation **CITRIX**.

Les images préparées par Citrix ne sont pas disponibles dans l'interface Configuration complète de Citrix DaaS.

Vous pouvez également importer et utiliser votre propre image depuis Azure.

Méthodes d'utilisation des images dans Déploiement rapide

Vous pouvez :

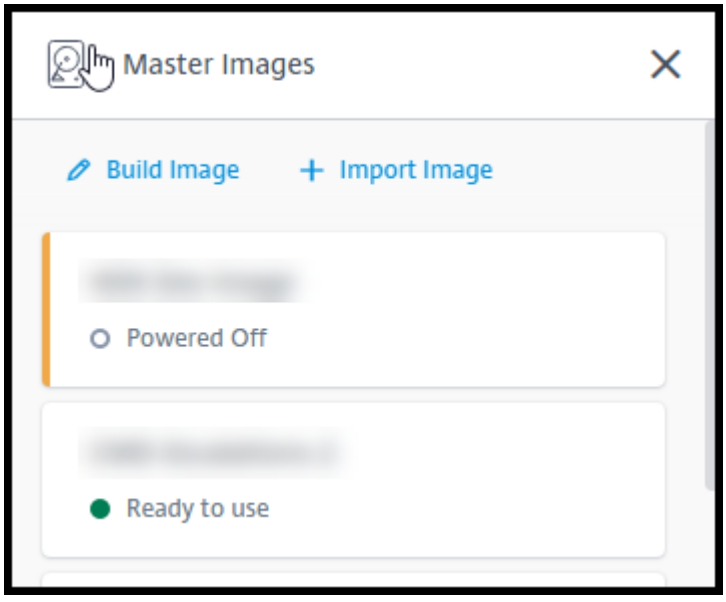
- **Utiliser une image préparée par Citrix lors de la création d'un catalogue.** Ce choix est recommandé uniquement pour les déploiements de preuve de concept.
- **Utiliser une image préparée par Citrix pour créer une autre image.** Une fois la nouvelle image créée, vous la personnalisez en ajoutant des applications et d'autres logiciels dont vos utilisateurs ont besoin. Vous pouvez ensuite utiliser cette image personnalisée lors de la création d'un catalogue.
- **Importer une image depuis Azure.** Une fois que vous avez importé une image depuis Azure, vous pouvez ensuite utiliser cette image lors de la création d'un catalogue.

  Vous pouvez également utiliser cette image pour créer une nouvelle image, puis la personnaliser en ajoutant des applications. Vous pouvez ensuite utiliser cette image personnalisée lors de la création d'un catalogue.

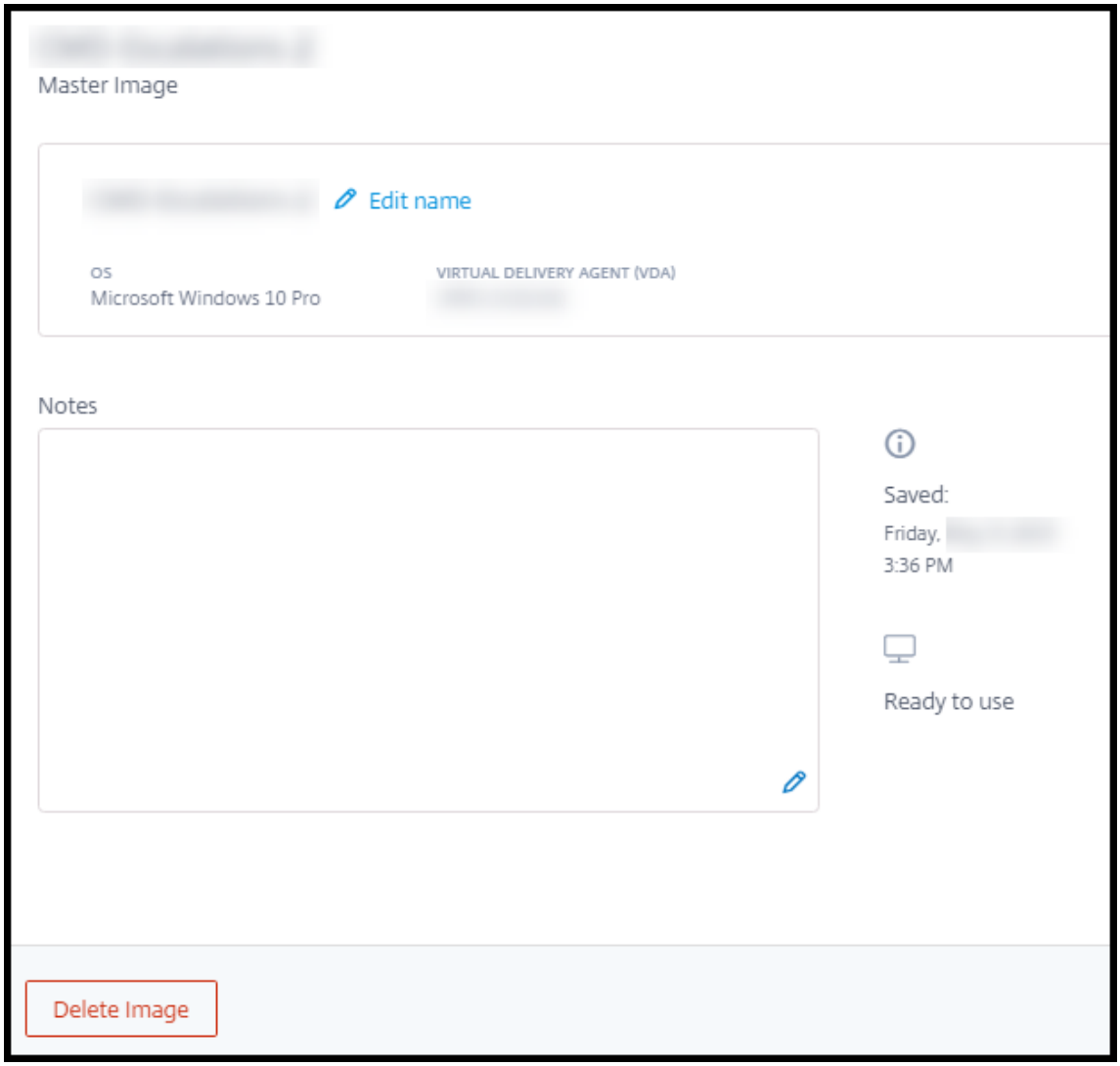
Lorsque vous créez un catalogue, Citrix DaaS vérifie que l'image utilise un système d'exploitation valide et dispose d'un VDA Citrix et d'outils de dépannage installés (ainsi que d'autres vérifications).

Afficher les informations sur l'image

1. Dans **Gérer > Déploiement rapide**, développez **Images principales** sur la droite. L'écran répertorie les images préparées par Citrix et toutes les images que vous avez importées.



2. Sélectionnez une image pour afficher ses détails.



À partir de la fiche de détails, vous pouvez :

- changer (modifier) le nom de l'image ;
- ajouter et modifier des notes (disponibles uniquement pour les images que vous avez préparées ou importées, et non pour les images préparées par Citrix) ;
- supprimer l'image.

Préparer une nouvelle image

La préparation d'une nouvelle image comprend la création de l'image, puis sa personnalisation. Lorsque vous créez une image, une machine virtuelle est créée pour charger la nouvelle image.

Exigences :

- Vous devez connaître les caractéristiques de performance dont les machines ont besoin. Par ex-

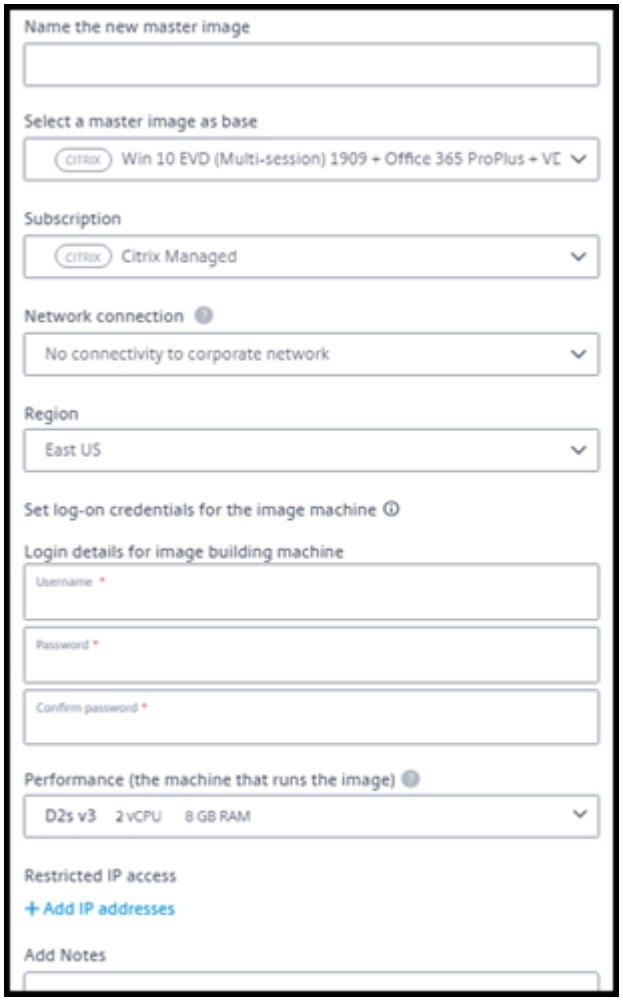
emple, l'exécution d'applications CAD peut nécessiter une unité centrale, une RAM et un stockage différents de ceux des autres applications bureautiques.
- Si vous envisagez d'utiliser une connexion à vos ressources locales, configurez cette connexion avant de créer l'image et le catalogue. Pour plus de détails, consultez la section Connexions réseau.

Lorsque vous utilisez une image Ubuntu préparée par Citrix pour créer une nouvelle image, un mot de passe racine est créé pour la nouvelle image. Vous pouvez modifier ce mot de passe racine, mais uniquement pendant le processus de création et de personnalisation de l'image. (Vous ne pouvez pas modifier le mot de passe racine après l'utilisation de l'image dans un catalogue.)

- Lorsque l'image est créée, le compte administrateur que vous avez spécifié (**Informations de connexion pour la machine de création d'image**) est ajouté au groupe `sudoers`.
- Une fois que vous êtes connecté via RDP à la machine contenant la nouvelle image, lancez l'application Terminal et tapez `sudo passwd root`. Lorsque vous y êtes invité, indiquez le mot de passe que vous avez spécifié lors de la création de l'image. Après vérification, vous êtes invité à entrer un nouveau mot de passe pour l'utilisateur racine.

Pour créer une image :

1. Dans **Gérer > Déploiement rapide**, développez **Images principales** sur la droite.
2. Sélectionnez **Créer image**.



3. Saisissez des valeurs dans les champs suivants :

   - **Nom :** saisissez un nom pour la nouvelle image.
   - **Image principale :** sélectionnez une image existante. Il s'agit de l'image de base utilisée pour créer la nouvelle image.
   - **Abonnement :** sélectionnez un abonnement Azure.
   - **Connexion réseau :**
     - Si vous utilisez un abonnement Azure géré par Citrix, sélectionnez **Aucune connectivité** ou une connexion précédemment créée.
     - Si vous utilisez votre propre abonnement Azure géré par le client, sélectionnez votre groupe de ressources, votre réseau virtuel et votre sous-réseau. Ajoutez ensuite les détails du domaine : nom de domaine complet, unité d'organisation, nom de compte Citrix DaaS et informations d'identification.
   - **Région :** (disponible uniquement pour **Aucune connectivité**.) Sélectionnez la région où vous souhaitez créer la machine contenant l'image.

- **Informations d'identification de connexion pour la machine à images :** vous utiliserez ces informations d'identification ultérieurement lorsque vous vous connecterez (RDP) à la machine contenant la nouvelle image, afin de pouvoir installer des applications et d'autres logiciels.
- **Performances de la machine :** il s'agit des informations relatives à l'unité centrale, à la RAM et au stockage de la machine qui exécute l'image. Sélectionnez une performance machine qui répond aux exigences de vos applications.
- **Accès IP restreint :** si vous souhaitez restreindre l'accès à des adresses spécifiques, sélectionnez **Ajouter des adresses IP**, puis saisissez une ou plusieurs adresses. Après avoir ajouté les adresses, sélectionnez **Terminé** pour revenir à la carte **Créer image**.
- **Remarques :** vous pouvez ajouter jusqu'à 1 024 caractères de notes. Une fois l'image créée, vous pouvez mettre à jour les notes à partir de l'affichage des détails de l'image.
- **Jointure de domaine local :** indiquez si vous souhaitez rejoindre le domaine Active Directory local.
  - Si vous sélectionnez **Oui**, saisissez le nom de domaine complet, l'unité d'organisation, le nom du compte Citrix DaaS et les informations d'identification.
  - Si vous sélectionnez **Non**, saisissez les informations d'identification de la machine hôte.

4. Lorsque vous avez terminé, sélectionnez **Créer image**.

La création d'une image peut prendre jusqu'à 30 minutes. Dans **Gérer > Déploiement rapide**, développez **Images principales** sur la droite pour voir l'état actuel (tel que `Building image` ou `Ready to customize`).

Que faire ensuite : connectez-vous à une nouvelle image et personnalisez-la.

Se connecter à une nouvelle image et la personnaliser

Une fois qu'une nouvelle image a été créée, son nom est ajouté à la liste des images, avec un statut `Ready to customize` (ou un libellé similaire). Pour personnaliser cette image, vous devez d'abord télécharger un fichier RDP. Lorsque vous utilisez ce fichier pour vous connecter à l'image, vous pouvez ensuite ajouter des applications et d'autres logiciels à l'image.

1. Dans **Gérer > Déploiement rapide**, développez **Images principales** sur la droite. Sélectionnez l'image à laquelle vous souhaitez vous connecter.
2. Sélectionnez **Télécharger le fichier RDP**. Un client RDP est téléchargé.

   La machine d'images peut s'éteindre si vous n'y ajoutez pas de fichier RDP peu de temps après sa création. Cela permet de réduire les coûts. Lorsque cela se produit, sélectionnez la **Mise sous tension**.

3. Démarrez le client RDP téléchargé. Il tente automatiquement de se connecter à l'adresse de la machine contenant la nouvelle image. Lorsque vous y êtes invité, saisissez les informations d'identification indiquées lors de la création de l'image.
4. Une fois que vous êtes connecté à la machine, ajoutez ou supprimez des applications, installez des mises à jour et terminez tout autre travail de personnalisation.

   N'effectuez **pas** de Sysprep de l'image.
5. Lorsque vous avez fini de personnaliser la nouvelle image, revenez à la zone **Images principales** et sélectionnez **Terminer la création**. La nouvelle image subit automatiquement des tests de validation.

Plus tard, lorsque vous créez un catalogue, la nouvelle image est incluse dans la liste des images que vous pouvez sélectionner.

Dans **Gérer > Déploiement rapide**, l'affichage de l'image sur la droite indique le nombre de catalogues et de machines qui utilisent chaque image.

> **Remarque :**
>
> Une fois que vous avez finalisé une image, vous ne pouvez pas la modifier. Vous devez créer une image (éventuellement en utilisant l'image précédente comme point de départ), puis mettre à jour la nouvelle image.

Importer une image depuis Azure

Lorsque vous importez une image depuis Azure qui possède un VDA Citrix et des applications dont vos utilisateurs ont besoin, vous pouvez l'utiliser pour créer un catalogue ou remplacer l'image dans un catalogue existant.

Exigences relatives à l'image

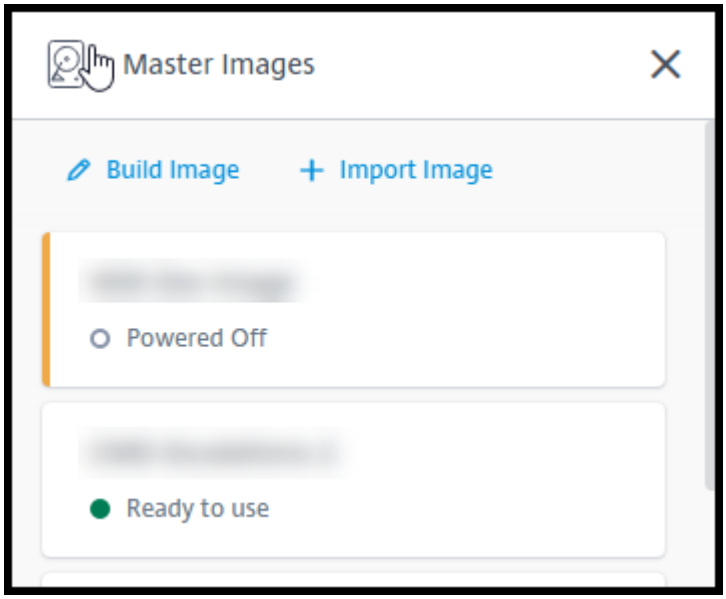
Citrix exécute des tests de validation sur l'image importée. Assurez-vous que les exigences suivantes sont satisfaites lorsque vous préparez l'image que vous allez importer dans Citrix DaaS.

- **Système d'exploitation pris en charge :** l'image doit être un système d'exploitation pris en charge. Pour vérifier une version du système d'exploitation Windows, exécutez `Get-WmiObject Win32_OperatingSystem`.
- **Génération prise en charge :** les machines virtuelles de génération 1 prennent en charge la plupart des systèmes d'exploitation invités. Les machines virtuelles de génération 2 prennent en charge la plupart des versions 64 bits de Windows et les versions les plus récentes des systèmes d'exploitation Linux.

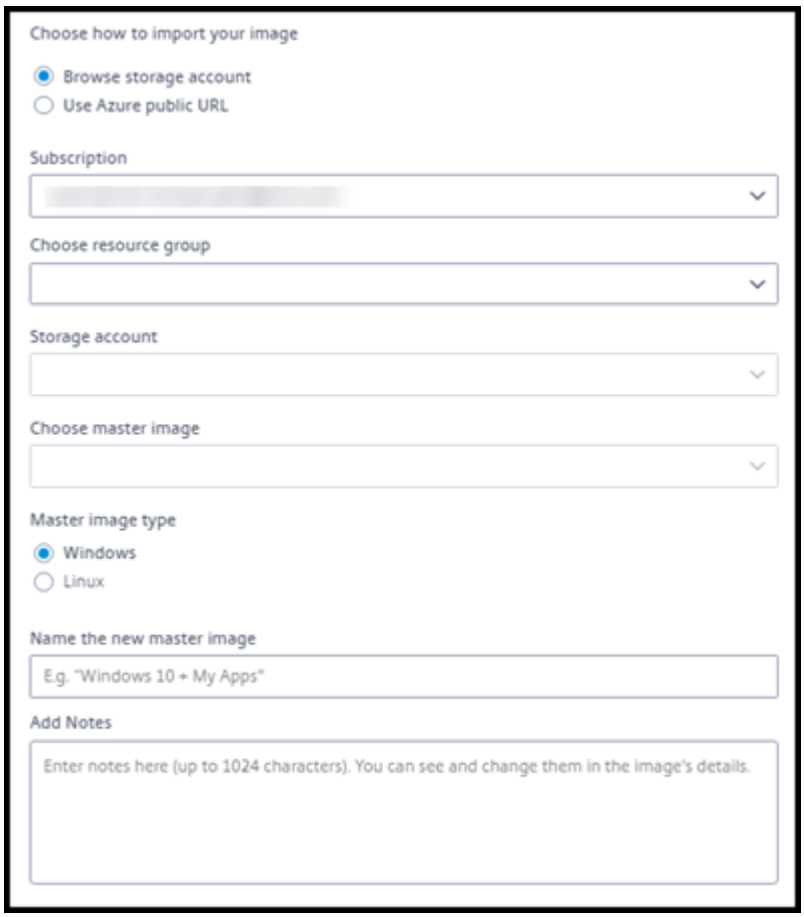
- **Non généralisée :** l'image ne doit pas être généralisée.
- **Aucun Delivery Controller configuré :** assurez-vous qu'aucun Citrix Delivery Controller n'est configuré dans l'image. Assurez-vous que les clés de registre suivantes sont effacées.
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **Fichier Personality.ini :** le fichier `personality.ini` doit exister sur le lecteur système.
- **VDA valide :** un VDA Citrix plus récent que 7.11 doit être installé sur l'image.
  - Windows : pour vérifier, utilisez `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. Pour obtenir des instructions d'installation, reportez-vous à la section Installer un VDA Windows sur une image.
  - Red Hat Enterprise Linux et Ubuntu : pour obtenir des conseils d'installation, reportez-vous à la documentation produit.
- **Agent de machine virtuelle Azure :** avant d'importer une image, assurez-vous que l'agent de machine virtuelle Azure est installé sur l'image. Pour plus d'informations, consultez l'article Microsoft Vue d'ensemble d'agent de machine virtuelle Azure.

Importer l'image avec Déploiement rapide

1. Dans **Gérer > Déploiement rapide**, développez **Images principales** sur la droite.



2. Sélectionnez **Importer une image**.



3. Choisissez comment importer l'image.

   - Pour les disques gérés, utilisez la fonctionnalité d'exportation pour générer une URL Séquence d'avertissement sécurisée. Définissez le délai d'expiration à 7 200 secondes ou plus.
   - Pour les disques durs virtuels d'un compte de stockage, choisissez l'une des options suivantes :
     - Générez une URL Séquence d'avertissement sécurisée pour le fichier VHD.
     - Mettez à jour le niveau d'accès d'un conteneur de stockage par blocs en blob ou en conteneur. Ensuite, récupérez l'URL du fichier.

4. Si vous avez sélectionné **Parcourir le compte de stockage** :

   a) Sélectionnez séquentiellement un abonnement > groupe de ressources > compte de stockage > image.
   b) Nommez l'image.

5. Si vous avez sélectionné l'**URL publique Azure** :

a) Saisissez l'URL générée par Azure pour le disque dur virtuel. Pour obtenir des conseils, sélectionnez le lien vers le document Microsoft Télécharger un VHD Windows à partir d'Azure.
b) Sélectionnez un abonnement. (Une image Linux ne peut être importée que si vous sélectionnez un abonnement géré par le client.)
c) Nommez l'image.

6. Lorsque vous avez terminé, sélectionnez **Importer une image**.

Mettre à jour un catalogue de déploiement rapide avec une nouvelle image

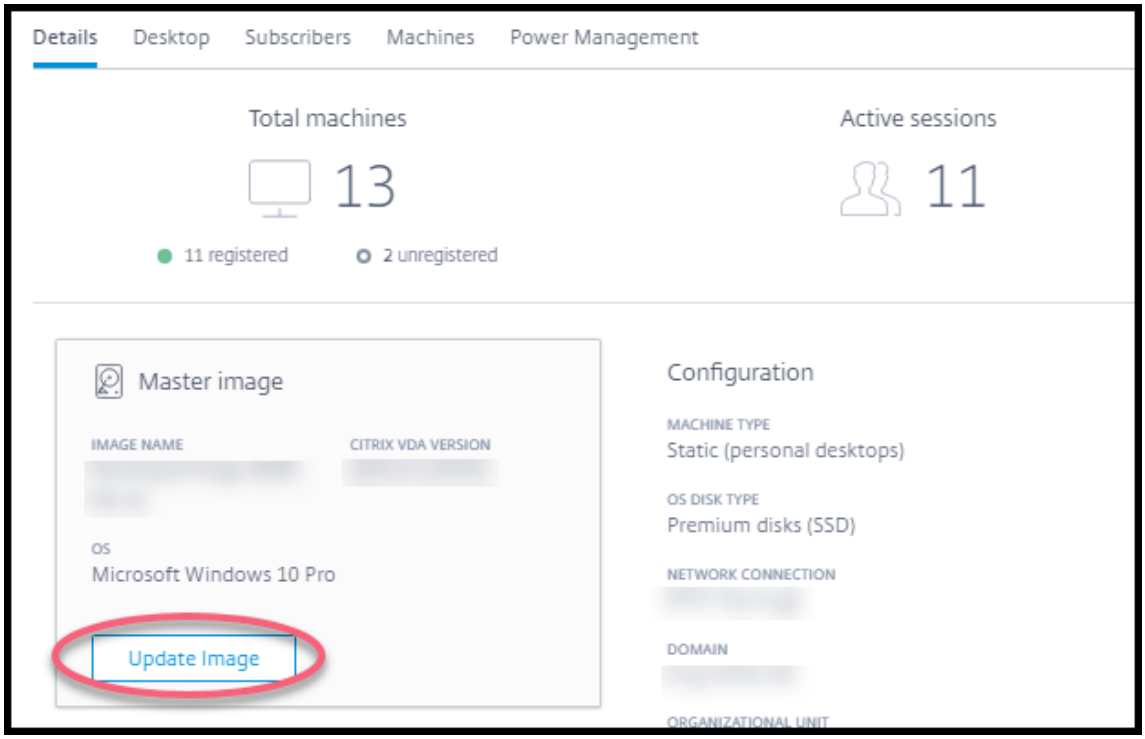
Le type de catalogue détermine quelles machines sont mises à jour lorsque vous mettez à jour le catalogue.

- Pour un catalogue aléatoire, toutes les machines actuellement dans le catalogue sont mises à jour avec la dernière image. Si vous ajoutez d'autres bureaux à ce catalogue, ceux-ci sont basés sur l'image la plus récente.
- Pour un catalogue statique, les machines actuellement dans le catalogue ne sont pas mises à jour avec la dernière image. Les machines actuellement dans le catalogue continuent d'utiliser l'image à partir de laquelle elles ont été créées. Toutefois, si vous ajoutez d'autres machines à ce catalogue, elles sont basées sur la dernière image.

Vous pouvez mettre à jour un catalogue contenant des machines avec des images de génération 1 avec une image de génération 2 si les machines du catalogue prennent en charge la génération 2. De même, vous pouvez mettre à jour un catalogue contenant des machines de génération 2 avec une image de génération 1 si les machines du catalogue prennent en charge la génération 1.

Pour mettre à jour un catalogue avec une nouvelle image :

1. Dans **Gérer > Déploiement rapide**, cliquez n'importe où dans l'entrée du catalogue.
2. Dans l'onglet **Détails**, sélectionnez **Mettre à jour l'image**.



3. Sélectionnez une image.
4. Pour les catalogues aléatoires ou à sessions multiples : sélectionnez un intervalle de fermeture de session. Une fois que Citrix DaaS a terminé le traitement initial de l'image, les abonnés reçoivent un avertissement pour enregistrer leur travail et se déconnecter de leurs bureaux. L'intervalle de fermeture de session indique le temps dont disposent les abonnés après la réception du message jusqu'à ce que la session se termine automatiquement.
5. Sélectionnez **Mettre à jour l'image**.

Supprimer une image de Déploiement rapide

1. Dans **Gérer > Déploiement rapide**, développez **Images principales** sur la droite.
2. Sélectionnez l'image que vous souhaitez supprimer.
3. Sélectionnez **Supprimer l'image** au bas de la carte. Confirmez la suppression.

Installer un VDA Windows sur une image

Suivez la procédure suivante lorsque vous préparez une image Windows que vous prévoyez d'importer dans Citrix DaaS.

Pour obtenir des instructions d'installation de Linux VDA, consultez la documentation produit du Linux VDA.

1. Dans votre environnement Azure, connectez-vous à la machine virtuelle d'image (si vous n'êtes pas déjà connecté).
2. Vous pouvez télécharger un VDA à l'aide du lien **Téléchargements** sur la barre de navigation de Citrix Cloud. Vous pouvez également utiliser un navigateur pour accéder à la page de téléchargement de Citrix DaaS.

   Téléchargez un VDA sur la machine virtuelle. Il existe des packages de téléchargement VDA distincts pour un système d'exploitation de bureau (à session unique) et un système d'exploitation serveur (à sessions multiples).
3. Lancez le programme d'installation de VDA en double-cliquant sur le fichier téléchargé. L'assistant d'installation démarre.
4. Sur la page **Environnement**, sélectionnez l'option permettant de créer une image à l'aide de MCS, puis sélectionnez **Suivant**.
5. Sur la page **Composants principaux**, sélectionnez **Suivant**.
6. Sur la page **Delivery Controller**, sélectionnez **Laisser Machine Creation Services effectuer ceci automatiquement**, puis sélectionnez **Suivant**. Confirmez votre sélection, si vous y êtes invité.
7. Laissez les paramètres par défaut sur les pages **Composants supplémentaires**, **Fonctionnalités** et **Pare-feu**, sauf avis contraire de Citrix. Sélectionnez **Suivant** à chaque page.
8. Sur la page **Résumé**, sélectionnez **Installer**. Les composants prérequis commencent à s'installer. Lorsque vous êtes invité à redémarrer, acceptez.
9. L'installation du VDA reprend automatiquement. L'installation des composants prérequis est terminée, puis les composants et les fonctionnalités sont installés. Sur la page **Call Home**, laissez le paramètre par défaut (sauf indication contraire de Citrix). Une fois que vous êtes connecté, sélectionnez **Suivant**.
10. Sélectionnez **Terminer**. La machine redémarre automatiquement.
11. Pour vous assurer que la configuration est correcte, lancez une ou plusieurs des applications que vous avez installées sur la machine virtuelle.
12. Arrêtez la machine virtuelle. N'effectuez pas de Sysprep de l'image.

Pour plus d'informations sur l'installation de VDA, reportez-vous à la section Installer des VDA.

Connexions réseau dans Déploiement rapide

June 12, 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.

Introduction

Cet article explique comment créer des connexions réseau à vos ressources d'entreprise lorsque vous utilisez un abonnement Azure géré par Citrix.

Lorsque vous utilisez votre propre abonnement Azure géré par le client, il n'est pas nécessaire de créer une connexion réseau.

Lorsque vous créez un catalogue de déploiement rapide, vous indiquez si et comment les utilisateurs peuvent accéder aux emplacements et aux ressources de leur réseau local d'entreprise à partir de leurs applications et bureaux Citrix. Lorsque vous utilisez une connexion, vous devez créer la connexion avant de créer le catalogue.

Lorsque vous utilisez un abonnement Azure géré par Citrix, les choix sont les suivants :

- Aucune connectivité
- Peering de réseau virtuel Azure
- SD-WAN

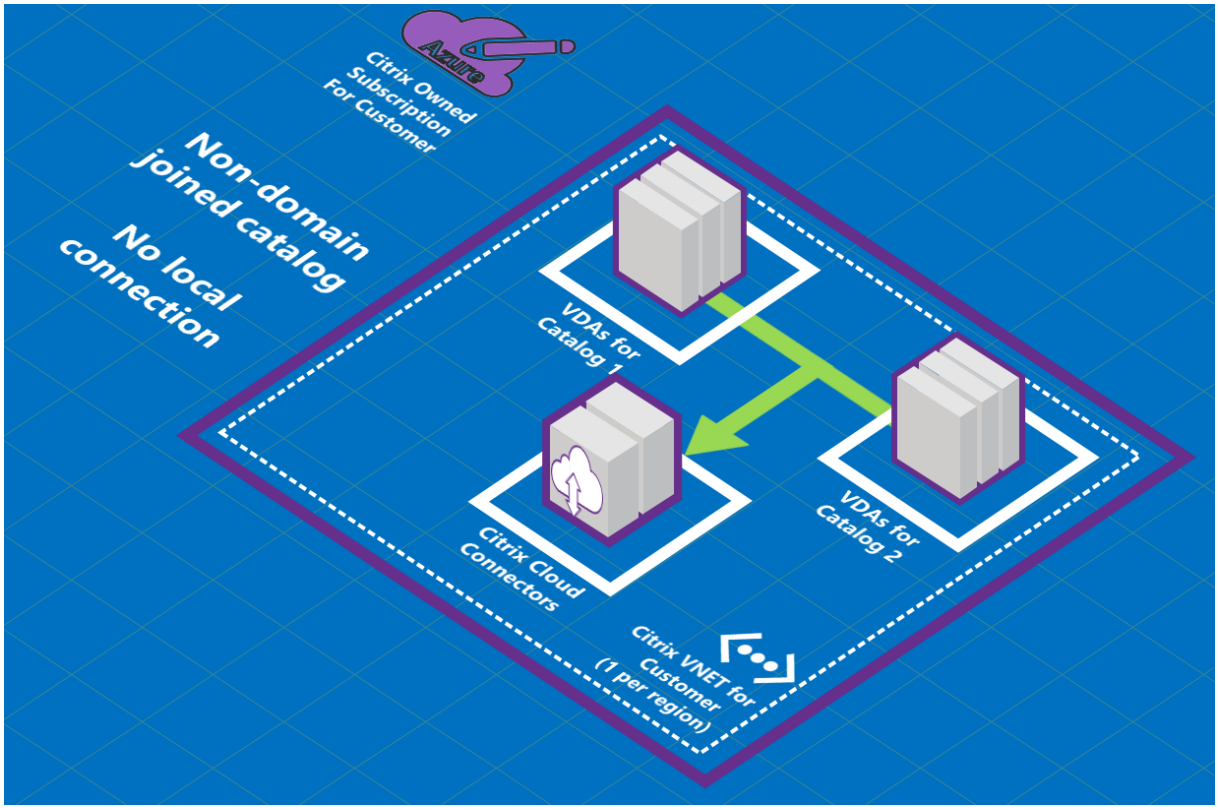
Vous ne pouvez pas modifier le type de connexion d'un catalogue une fois le catalogue créé.

Configuration requise pour toutes les connexions réseau

- Lors de la création d'une connexion, vous devez disposer d'entrées de serveur DNS valides.
- Lorsque vous utilisez Secure DNS ou un fournisseur DNS tiers, vous devez ajouter la plage d'adresses allouée pour être utilisée par Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) aux adresses IP du fournisseur DNS dans la liste verte. Cette plage d'adresses est spécifiée lorsque vous créez une connexion.
- Toutes les ressources de service qui utilisent la connexion (machines jointes à un domaine) doivent pouvoir atteindre votre serveur Network Time Protocol (NTP), afin d'assurer la synchronisation de l'heure.

Aucune connectivité

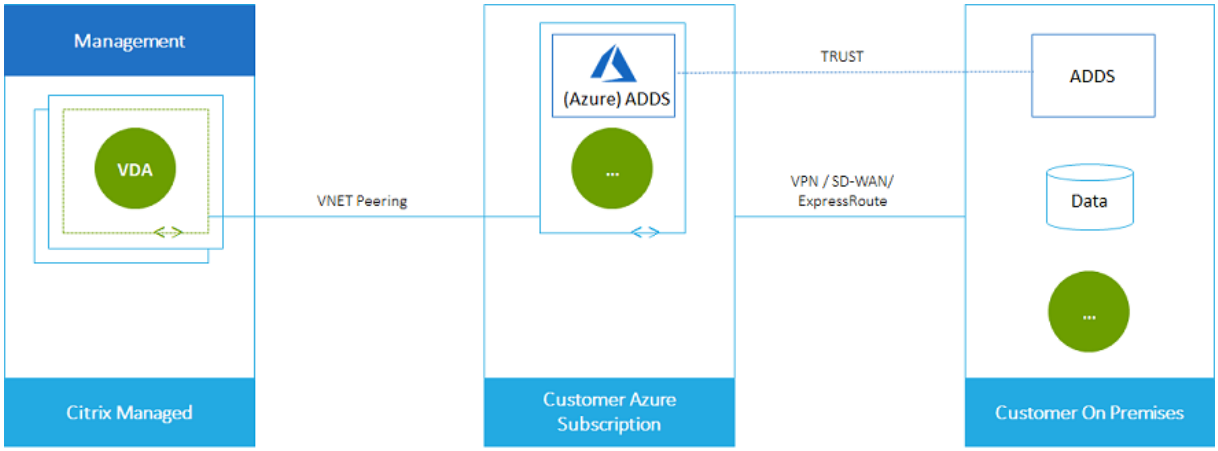
Lorsqu'un catalogue est configuré avec **Aucune connectivité**, l'utilisateur ne peut pas accéder aux ressources sur son réseau local ni sur d'autres réseaux. Il s'agit du seul choix lors de la création d'un catalogue à l'aide de la création rapide.



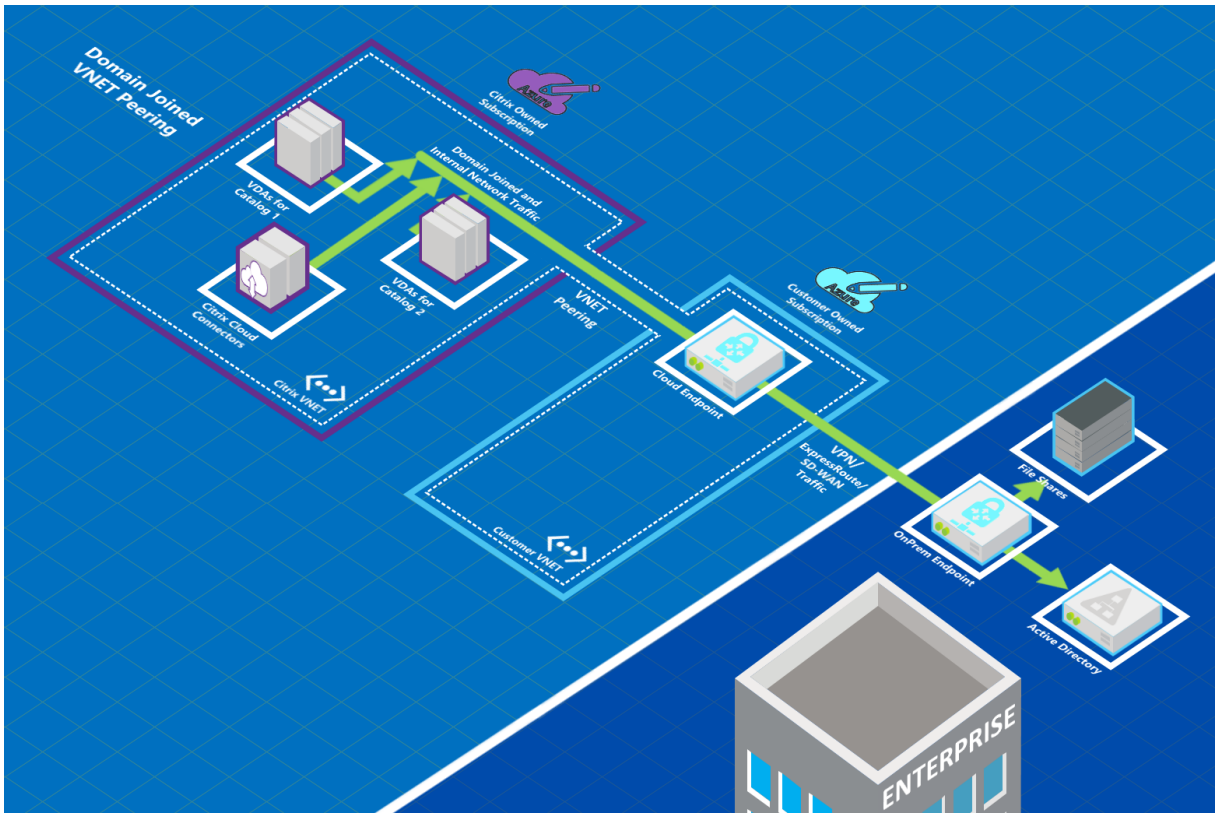
À propos des connexions de peering de réseau virtuel Azure

Le peering de réseau virtuel connecte de manière transparente deux réseaux virtuels Azure : le vôtre et le réseau virtuel Citrix DaaS. Le peering permet également aux utilisateurs d'accéder à des fichiers et autres éléments à partir de vos réseaux locaux.

Comme le montre le graphique suivant, vous créez une connexion à l'aide du peering de réseau virtuel Azure depuis l'abonnement Azure géré par Citrix vers le réseau virtuel dans l'abonnement Azure de votre entreprise.



Voici une autre illustration du peering de réseau virtuel.



Les utilisateurs peuvent accéder à leurs ressources réseau (telles que les serveurs de fichiers) en rejoignant le domaine local lorsque vous créez un catalogue. (C'est-à-dire que vous rejoignez le domaine AD qui contient les partages de fichiers et les autres ressources nécessaires.) Votre abonnement Azure se connecte à ces ressources (dans les graphiques, à l'aide d'un VPN ou d'Azure ExpressRoute). Lorsque vous créez le catalogue, vous fournissez les informations d'identification du domaine, de l'unité d'organisation et du compte.

> **Important :**
>
> - Découvrez le peering de réseau virtuel Azure avant de l'utiliser dans ce service.
> - Créez une connexion de peering de réseau virtuel avant de créer un catalogue qui l'utilise.

Itinéraires personnalisés de peering de réseau virtuel Azure

Les itinéraires personnalisés ou définis par l'utilisateur remplacent les itinéraires système par défaut d'Azure pour diriger le trafic entre les machines virtuelles dans un peering de réseau virtuel, les réseaux locaux et sur Internet. Vous pouvez utiliser des itinéraires personnalisés s'il existe des réseaux auxquels les ressources de Citrix DaaS sont censées accéder, mais ne sont pas directement connectés via le peering de réseau virtuel. Par exemple, vous pouvez créer un itinéraire personnalisé qui force le trafic via une appliance réseau vers Internet ou vers un sous-réseau local.

Pour utiliser des itinéraires personnalisés :

- Vous devez disposer d'une passerelle réseau virtuel Azure ou d'une appliance réseau telle que Citrix SD-WAN dans votre environnement Citrix DaaS.
- Lorsque vous ajoutez des itinéraires personnalisés, vous devez mettre à jour les tables de routage de votre entreprise avec les informations du réseau virtuel de destination de Citrix DaaS pour garantir une connectivité de bout en bout.
- Les itinéraires personnalisés sont affichés dans Citrix DaaS dans l'ordre dans lequel ils sont saisis. Cet ordre d'affichage n'affecte pas l'ordre dans lequel Azure sélectionne les itinéraires.

Avant d'utiliser des itinéraires personnalisés, consultez l'article Microsoft Routage du trafic de réseau virtuel pour en savoir plus sur l'utilisation d'itinéraires personnalisés, les types de sauts suivants et la façon dont Azure sélectionne les itinéraires pour le trafic sortant.

Vous pouvez ajouter des itinéraires personnalisés lorsque vous créez une connexion de peering de réseau virtuel Azure ou à des connexions existantes dans votre environnement Citrix DaaS. Lorsque vous êtes prêt à utiliser des itinéraires personnalisés avec votre peering de réseau virtuel, reportez-vous aux sections suivantes de cet article :

- Pour les itinéraires personnalisés avec de nouveaux peerings de réseaux virtuels Azure : créez une connexion de peering de réseau virtuel Azure
- Pour les itinéraires personnalisés avec des peerings de réseaux virtuels Azure existants : gérez des itinéraires personnalisés pour les connexions de peerings de réseaux virtuels Azure existantes

Configuration requise et préparation du peering de réseau virtuel Azure

- Informations d'identification d'un propriétaire d'abonnement Azure. Il doit s'agir d'un compte Azure Active Directory. Ce service ne prend pas en charge les autres types de comptes, tels que live.com ou les comptes Azure AD externes (dans un autre locataire).
- Un abonnement Azure, un groupe de ressources et un réseau virtuel (VNet).
- Configurez les itinéraires réseau Azure afin que les VDA de l'abonnement Azure géré par Citrix puissent communiquer avec vos emplacements réseau.
- Ouvrez les groupes de sécurité réseau Azure depuis votre réseau virtuel vers la plage IP spécifiée.
- **Active Directory :** dans les scénarios dans lesquels vous êtes joints à un domaine, nous vous recommandons d'utiliser un type de services Active Directory dans le réseau virtuel associé. Cela tire parti des caractéristiques de faible latence de la technologie de peering de réseau virtuel Azure.

  Par exemple, la configuration peut inclure Azure Active Directory Domain Services (AADDS), une machine virtuelle de contrôleur de domaine dans le réseau virtuel ou Azure AD Connect à votre

Active Directory local.

Après avoir activé AADDS, vous ne pouvez pas déplacer votre domaine géré vers un autre réseau virtuel sans supprimer le domaine géré. Il est donc important de sélectionner le réseau virtuel approprié pour activer votre domaine géré. Avant de continuer, consultez l'article Microsoft Considérations relatives à la conception du réseau virtuel et options de configuration pour Azure Active Directory Domain Services.

- **Plage IP du réseau virtuel :** lors de la création de la connexion, vous devez fournir un espace d'adressage de routage CIDR disponible (adresse IP et préfixe réseau) unique parmi les ressources réseau et les réseaux virtuels Azure connectés. Il s'agit de la plage IP attribuée aux machines virtuelles au sein du réseau virtuel appairé de Citrix DaaS.

  Assurez-vous de spécifier une plage IP qui ne chevauche aucune adresse que vous utilisez dans vos réseaux Azure et locaux.

  - Par exemple, si votre réseau virtuel Azure dispose d'un espace d'adressage de 10.0.0.0 /16, créez la connexion de peering de réseau virtuel dans Citrix DaaS sous une forme comme 192.168.0.0 /24.
  - Dans cet exemple, la création d'une connexion de peering avec une plage IP 10.0.0.0 /24 serait considérée comme une plage d'adresses qui se chevauchent.

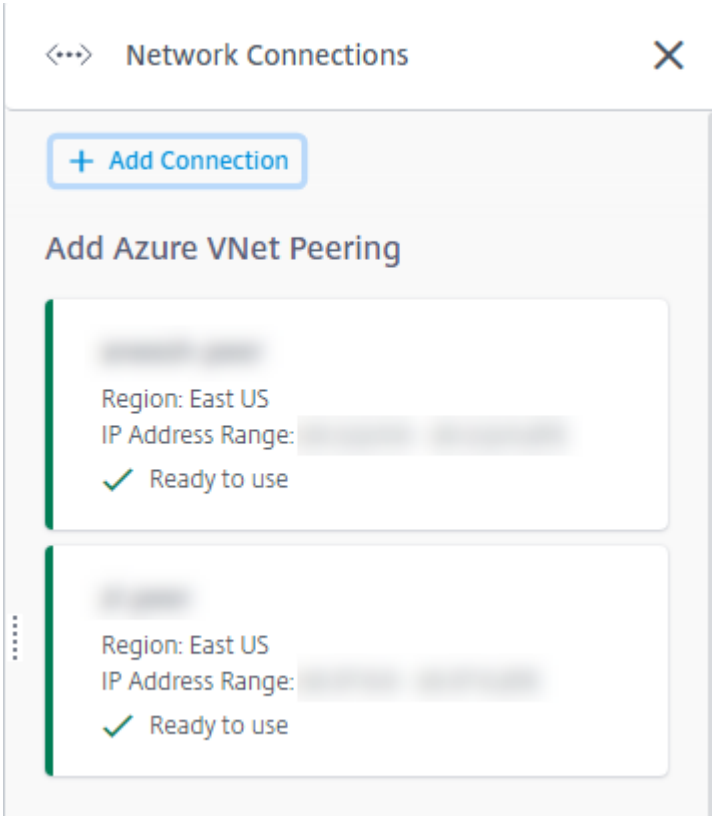
  Si les adresses se chevauchent, la connexion de peering de réseau virtuel est susceptible de ne pas être créée correctement. Cela ne fonctionne pas non plus correctement pour les tâches d'administration de site.

Pour en savoir plus sur le peering de réseau virtuel, consultez les articles Microsoft suivants.

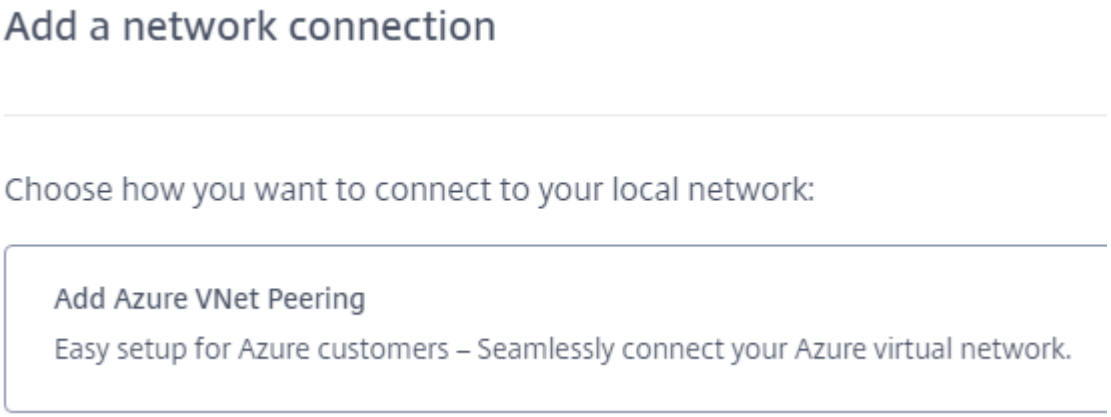
- Peering de réseau virtuel
- Passerelle VPN Azure
- Créer une connexion de site à site dans le portail Azure
- FAQ sur la passerelle VPN (recherchez « chevauchement »)

Création d'une connexion de peering de réseau virtuel Azure

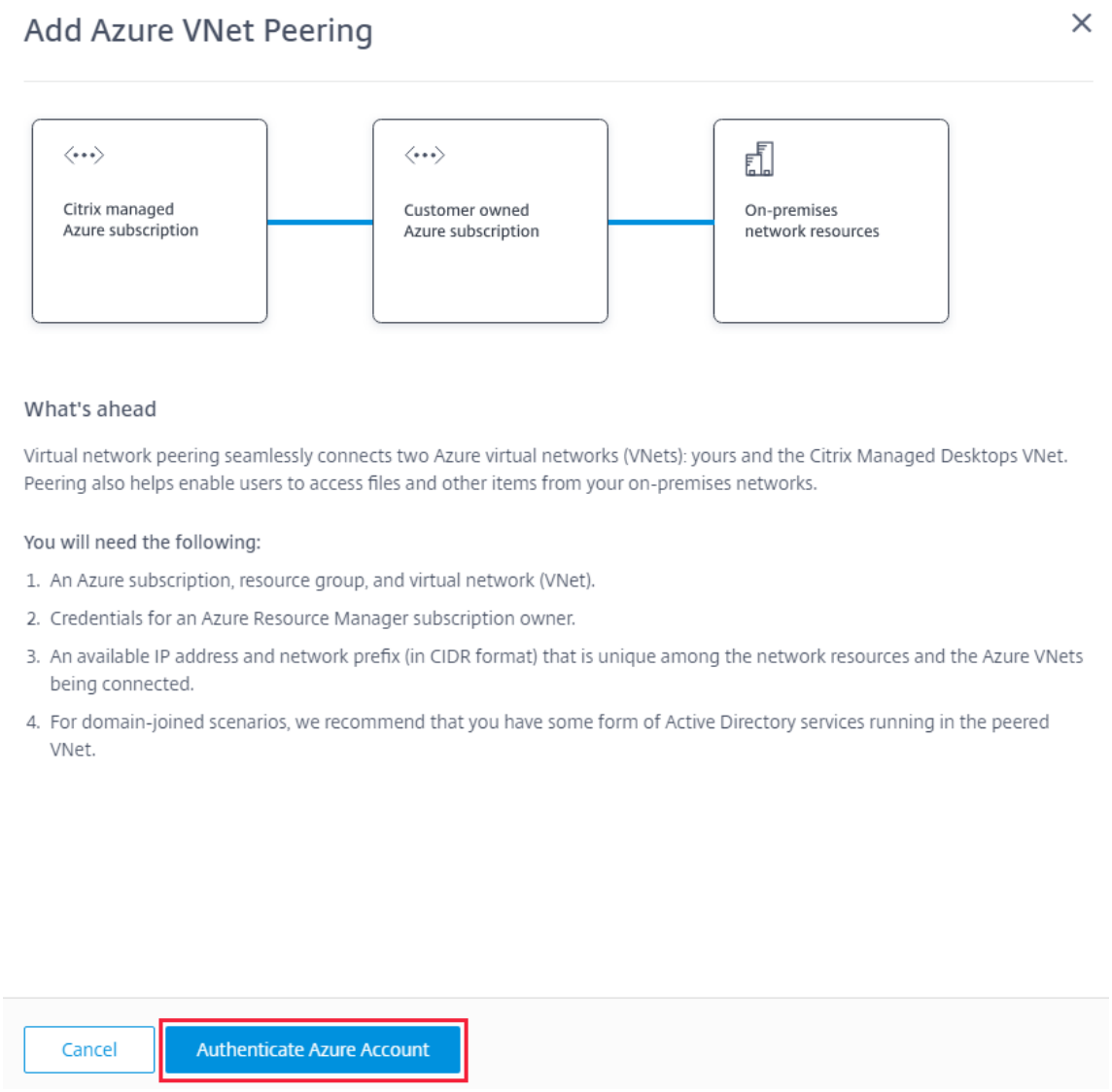
1. Dans **Gérer > Déploiement rapide**, développez **Connexions réseau** sur la droite. Si vous avez déjà configuré des connexions, elles sont répertoriées.



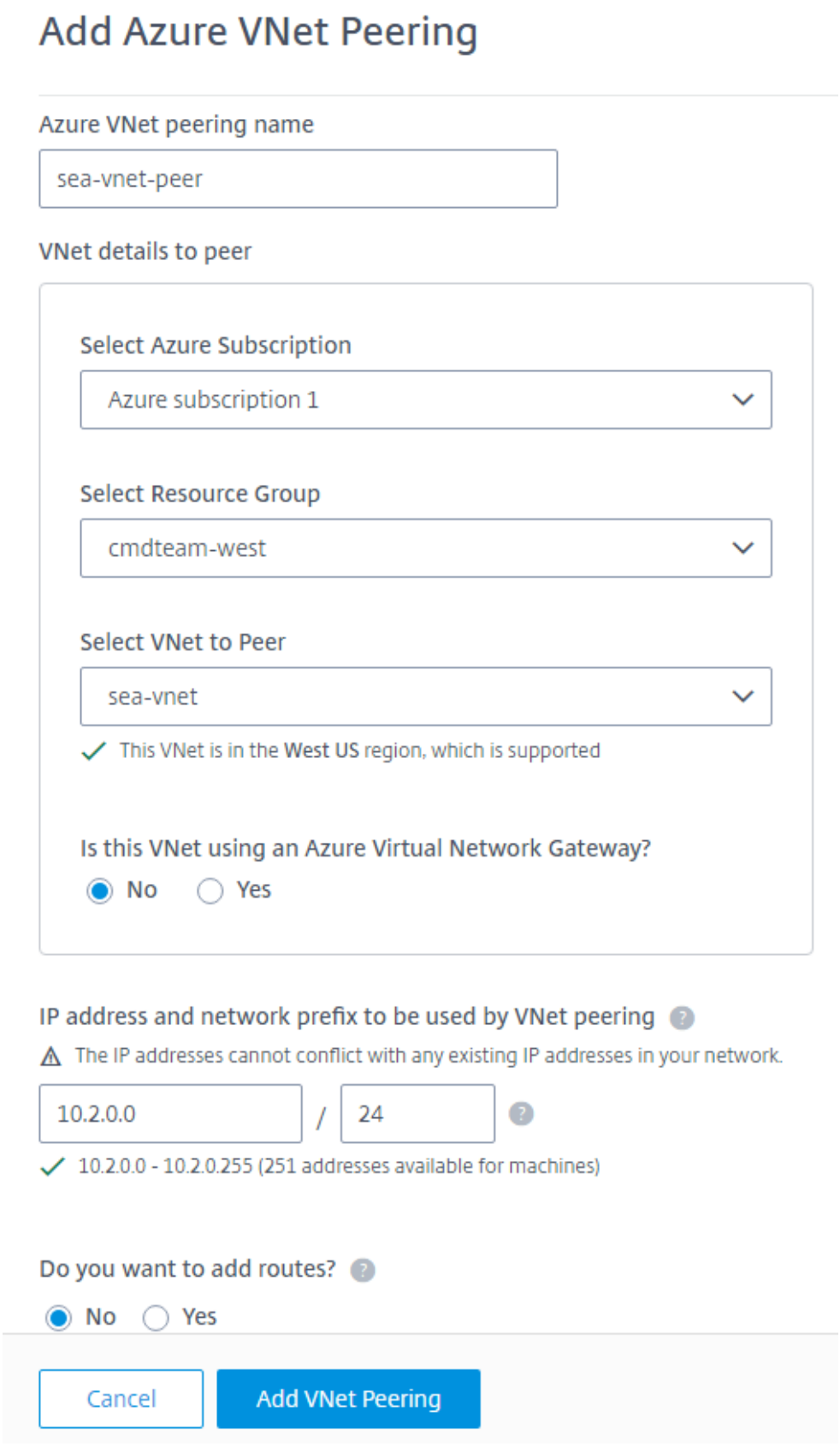
2. Sélectionnez **Ajouter une connexion**.
3. Cliquez n'importe où dans la zone **Ajouter peering de réseau virtuel Azure**.



4. Sélectionnez **Authentifier le compte Azure**.



5. Citrix DaaS vous amène automatiquement à la page de connexion Azure pour authentifier vos abonnements Azure. Une fois que vous êtes connecté à Azure (avec les informations d'identification du compte administrateur général) et que vous avez accepté les termes, vous revenez à la boîte de dialogue des détails de création de connexion.



6. Saisissez un nom pour l'homologue de réseau virtuel Azure.
7. Sélectionnez l'abonnement Azure, le groupe de ressources et le réseau virtuel à homologue.
8. Indiquez si le réseau virtuel sélectionné utilise une passerelle réseau virtuel Azure. Pour plus d'informations, consultez l'article Microsoft Passerelle VPN Azure.
9. Si vous avez répondu **Oui** à l'étape précédente (le réseau virtuel utilise une passerelle réseau virtuel Azure), indiquez si vous souhaitez activer la propagation de routage de la passerelle réseau virtuelle. Lorsque cette option est activée, Azure apprend (ajoute) automatiquement tous les itinéraires via la passerelle.

   Vous pouvez modifier ce paramètre ultérieurement sur la page **Détails** de la connexion. Toutefois, sa modification peut entraîner des changements de modèle de routage et des interruptions de trafic VDA. De plus, si vous le désactivez ultérieurement, vous devez ajouter manuellement des itinéraires aux réseaux que les VDA utiliseront.
10. Saisissez une adresse IP et sélectionnez un masque réseau. La plage d'adresses à utiliser est affichée, ainsi que le nombre d'adresses prises en charge par la plage. Assurez-vous que la plage IP ne chevauche aucune adresse que vous utilisez dans vos réseaux Azure et locaux.

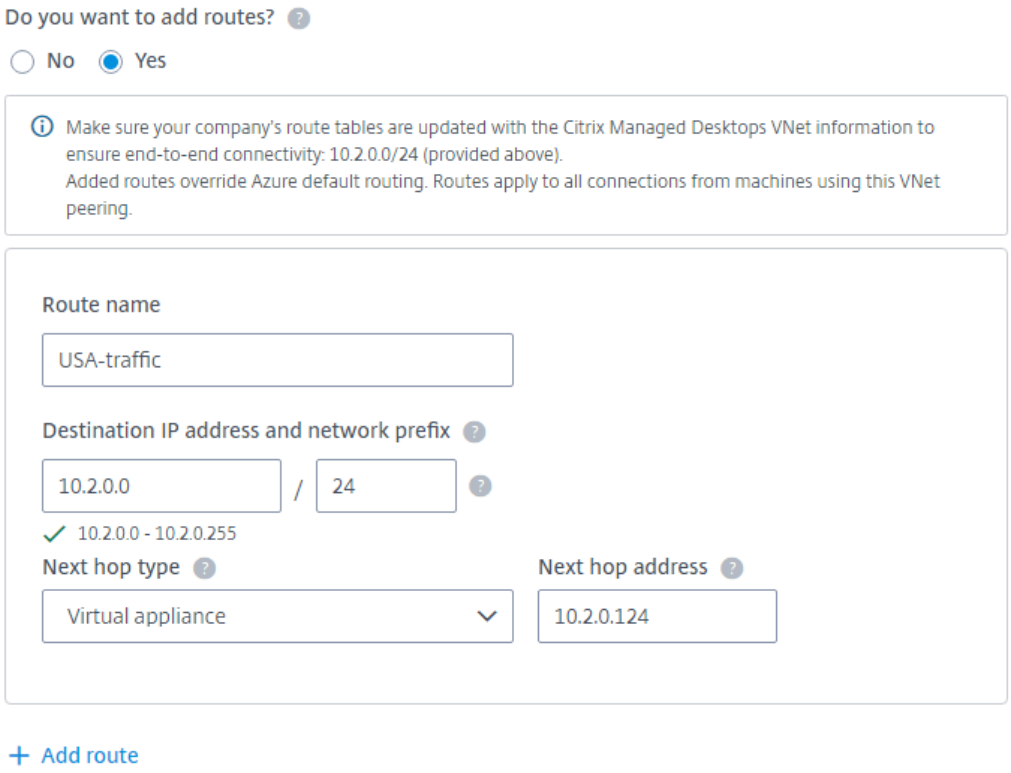
    - Par exemple, si votre réseau virtuel Azure dispose d'un espace d'adressage de 10.0.0.0 /16, créez la connexion de peering de réseau virtuel dans Citrix DaaS sous une forme comme 192.168.0.0 /24.
    - Dans cet exemple, la création d'une connexion de peering de réseau virtuel avec une plage d'adresses IP 10.0.0.0 /24 est considérée comme une plage d'adresses qui se chevauche.

    Si les adresses se chevauchent, la connexion de peering de réseau virtuel est susceptible de ne pas être créée correctement. Cela ne fonctionnera pas non plus correctement pour les tâches d'administration de site.
11. Indiquez si vous souhaitez ajouter des itinéraires personnalisés à la connexion de peering de réseau virtuel. Si vous sélectionnez **Oui**, saisissez les informations suivantes :

    a) Saisissez un nom convivial pour l'itinéraire personnalisé.

    b) Saisissez l'adresse IP de destination et le préfixe réseau. Le préfixe réseau doit être compris entre 16 et 24.

    c) Sélectionnez un type de saut suivant pour l'endroit où vous souhaitez acheminer le trafic. Si vous sélectionnez **Appliance virtuelle**, saisissez l'adresse IP interne de l'appliance.



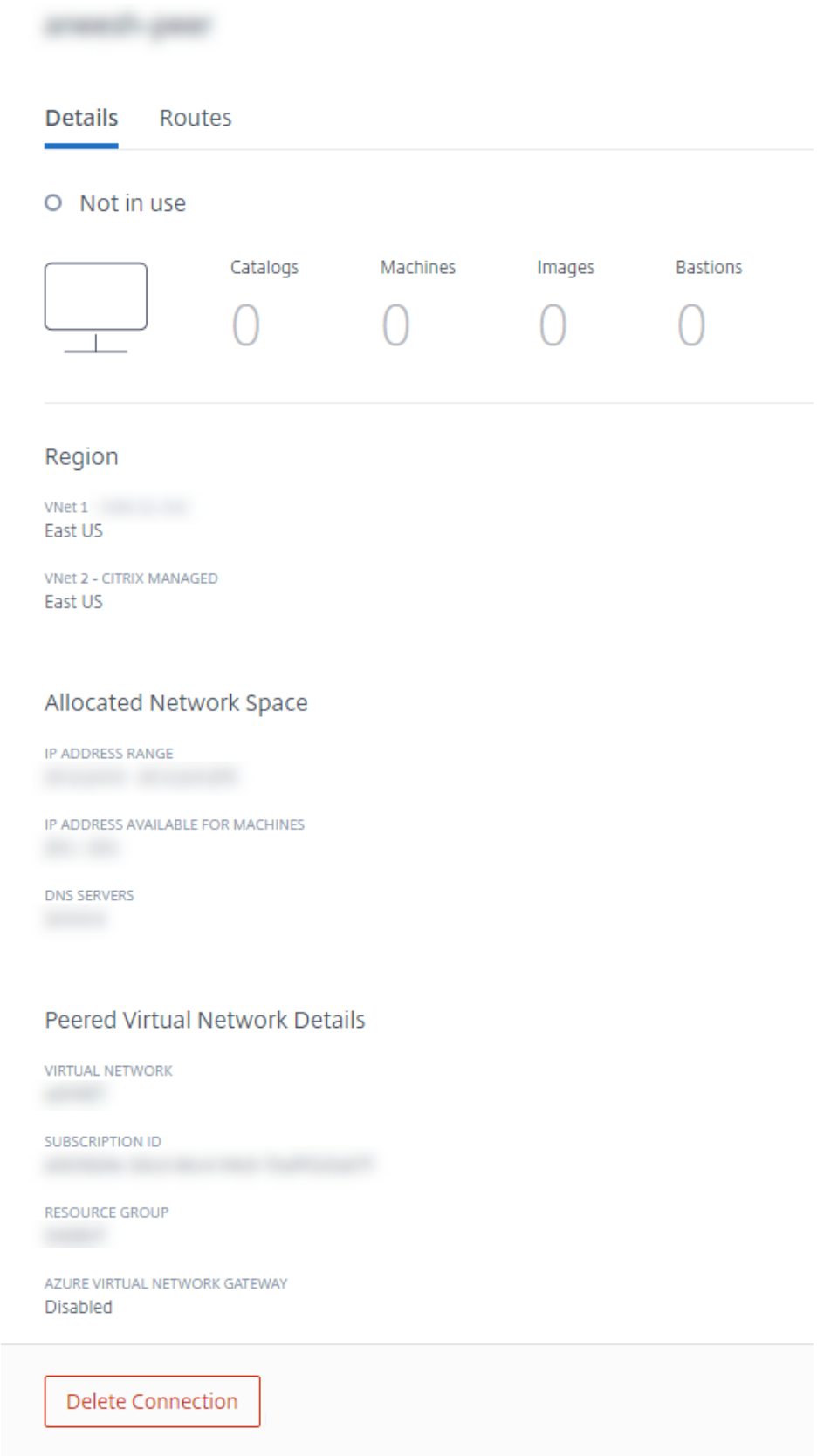
Pour plus d'informations sur les types de sauts suivants, reportez-vous à la section Itinéraires personnalisés de l'article Microsoft *Routage du trafic de réseau virtuel*.

d) Pour créer un autre itinéraire personnalisé pour la connexion, sélectionnez **Ajouter un itinéraire**.

12. Sélectionnez **Ajouter peering de réseau virtuel**.

Une fois la connexion créée, elle est répertoriée sous **Connexions réseau > Homologues de réseau virtuel Azure** sur le côté droit du tableau de bord **Gérer > Déploiement rapide**. Lorsque vous créez un catalogue, cette connexion est incluse dans la liste des connexions réseau disponibles.

Afficher les détails de la connexion de peering de réseau virtuel Azure



1. Dans **Gérer > Déploiement rapide**, développez **Connexions réseau** sur la droite.
2. Sélectionnez la connexion de peering de réseau virtuel Azure que vous souhaitez afficher.

Les détails incluent :

- le nombre de catalogues, de machines, d'images et de bastions utilisant cette connexion ;
- la région, l'espace réseau alloué et les réseaux virtuels appairés ;
- les itinéraires actuellement configurés pour la connexion de peering de réseau virtuel.

Gérer les itinéraires personnalisés pour les connexions homologues de réseau virtuel Azure existantes

Vous pouvez ajouter de nouveaux itinéraires personnalisés à une connexion existante ou modifier des itinéraires personnalisés existants, y compris la désactivation ou la suppression d'itinéraires personnalisés.

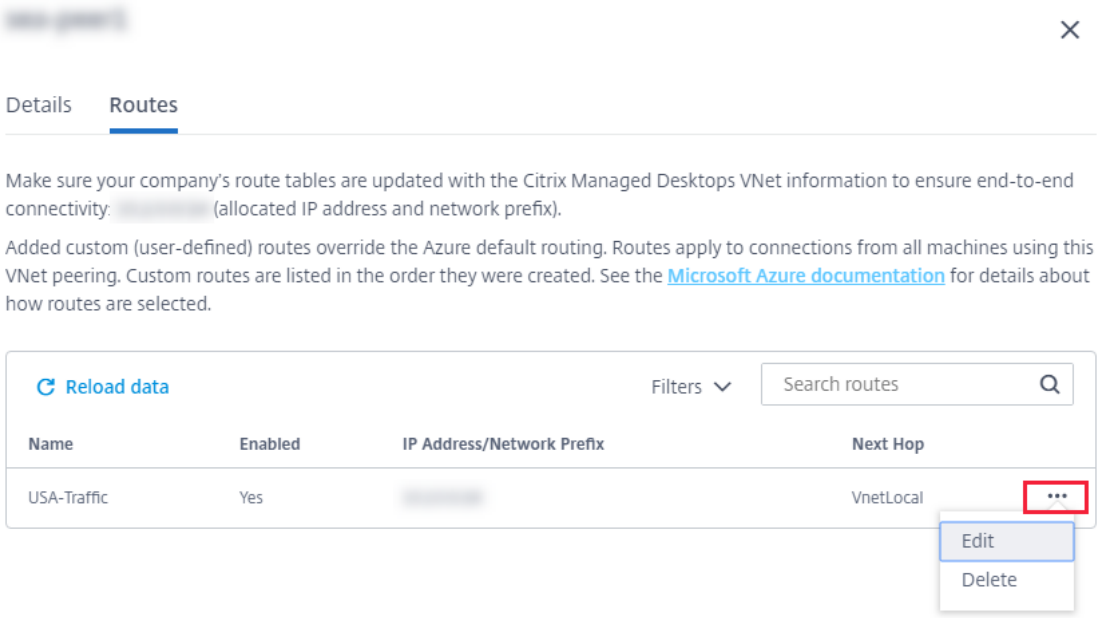
> **Important :**
>
> La modification, la désactivation ou la suppression d'itinéraires personnalisés modifient le flux de trafic de la connexion et peuvent perturber toutes les sessions utilisateur susceptibles d'être actives.

Pour ajouter un itinéraire personnalisé, procédez comme suit :

1. Dans **Gérer > Déploiement rapide**, développez **Connexions réseau** sur la droite.
2. Sélectionnez la connexion que vous souhaitez supprimer.
3. Dans les détails de la connexion, sélectionnez **Itinéraires**, puis **Ajouter un itinéraire**.
4. Saisissez un nom convivial, l'adresse IP de destination et le préfixe, ainsi que le type de saut suivant que vous souhaitez utiliser. Si vous sélectionnez **Appliance virtuelle** comme type de saut suivant, saisissez l'adresse IP interne de l'appliance.
5. Indiquez si vous souhaitez activer l'itinéraire personnalisé. Par défaut, l'itinéraire personnalisé est activé.
6. Sélectionnez **Ajouter un itinéraire**.

Pour modifier ou désactiver un itinéraire personnalisé, procédez comme suit :

1. Dans **Gérer > Déploiement rapide**, développez **Connexions réseau** sur la droite.
2. Sélectionnez la connexion que vous souhaitez supprimer.
3. Dans les détails de la connexion, sélectionnez **Itinéraires**, puis localisez l'itinéraire personnalisé que vous souhaitez gérer.
4. Dans le menu des points de suspension, sélectionnez **Modifier**.



5. Apportez les modifications nécessaires à l'adresse IP de destination et au préfixe ou au type de saut suivant, le cas échéant.
6. Pour activer ou désactiver un itinéraire personnalisé, dans **Activer cet itinéraire ?**, sélectionnez **Oui** ou **Non**.
7. Sélectionnez **Save**.

Pour supprimer un itinéraire personnalisé, procédez comme suit :

1. Dans **Gérer > Déploiement rapide**, développez **Connexions réseau** sur la droite.
2. Sélectionnez la connexion que vous souhaitez supprimer.
3. Dans les détails de la connexion, sélectionnez **Itinéraires**, puis localisez l'itinéraire personnalisé que vous souhaitez gérer.
4. Dans le menu des points de suspension, sélectionnez **Supprimer**.
5. Sélectionnez **Supprimer un itinéraire peut perturber les sessions actives** pour reconnaître l'impact de la suppression de l'itinéraire personnalisé.
6. Sélectionnez **Supprimer l'itinéraire**.

Supprimer une connexion de peering de réseau virtuel Azure

Avant de pouvoir supprimer une connexion de peering de réseau virtuel Azure, supprimez tous les catalogues qui y sont associés. Consultez la section Supprimer un catalogue.

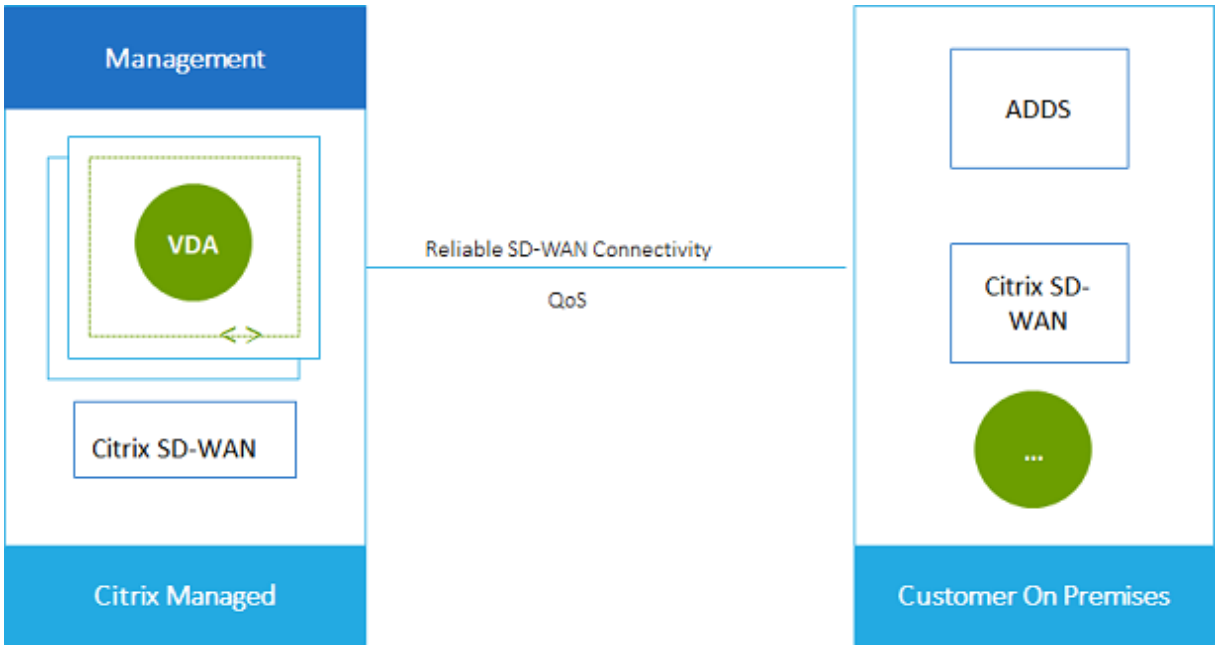
1. Dans **Gérer > Déploiement rapide**, développez **Connexions réseau** sur la droite.
2. Sélectionnez la connexion que vous souhaitez supprimer.
3. Dans les détails de la connexion, sélectionnez **Supprimer la connexion**.

À propos des connexions SD-WAN

Citrix SD-WAN optimise toutes les connexions réseau nécessaires à Citrix DaaS. Travaillant de concert avec les technologies HDX, Citrix SD-WAN offre une qualité de service et une fiabilité de connexion pour le trafic ICA et Citrix DaaS hors bande. Citrix SD-WAN prend en charge les connexions réseau suivantes :

- connexion ICA Multi-Stream entre les utilisateurs et leurs bureaux virtuels ;
- accès Internet depuis le bureau virtuel aux sites Web, aux applications SaaS et à d'autres propriétés Cloud :
- accès depuis le bureau virtuel à des ressources locales telles qu'Active Directory, serveurs de fichiers et serveurs de bases de données ;
- trafic interactif et en temps réel transporté par RTP depuis le moteur multimédia de l'application Workspace vers des services de communications unifiées hébergés dans le Cloud tels que Microsoft Teams ;
- récupération de vidéos côté client à partir de sites tels que YouTube et Vimeo.

Comme le montre le graphique suivant, vous créez une connexion SD-WAN à vos sites à partir de l'abonnement Azure géré par Citrix. Lors de la création de la connexion, les appliances VPX SD-WAN sont créées dans l'abonnement Azure géré par Citrix. Du point de vue du SD-WAN, cet emplacement est traité comme une succursale.



Configuration requise et préparation de la connexion SD-WAN

- Si les exigences suivantes ne sont pas satisfaites, l'option de connexion réseau SD-WAN n'est pas disponible.

  - Droits de service Citrix Cloud : Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) et SD-WAN Orchestrator.
  - Un déploiement SD-WAN installé et configuré. Le déploiement doit inclure un nœud de contrôle maître (MCN), que ce soit dans le Cloud ou local, et être géré avec SD-WAN Orchestrator.

- Plage IP de réseau virtuel : fournissez un espace d'adressage de routage CIDR disponible (adresse IP et préfixe réseau) unique parmi les ressources réseau connectées. Il s'agit de la plage IP attribuée aux machines virtuelles au sein du réseau virtuel de Citrix DaaS.

  Assurez-vous d'indiquer une plage IP qui ne chevauche aucune adresse que vous utilisez dans votre Cloud et vos réseaux locaux.

  - Par exemple, si votre réseau dispose d'un espace d'adressage de 10.0.0.0 /16, créez la connexion dans Citrix DaaS en utilisant par exemple 192.168.0.0 /24.
  - Dans cet exemple, la création d'une connexion avec une plage IP 10.0.0.0 /24 serait considérée comme une plage d'adresses qui se chevauche.

  Si les adresses se chevauchent, la connexion est susceptible de ne pas être créée correctement. Cela ne fonctionne pas non plus correctement pour les tâches d'administration de site.

- Le processus de configuration de la connexion inclut les tâches que vous (l'administrateur Citrix DaaS) et l'administrateur SD-WAN Orchestrator doivent effectuer. De plus, pour effectuer vos tâches, vous avez besoin d'informations fournies par l'administrateur SD-WAN Orchestrator.

  Avant de créer une connexion, nous vous recommandons de consulter à la fois les conseils de ce document, ainsi que la documentation SD-WAN.

Créer une connexion SD-WAN

> **Important :**
>
> Pour plus d'informations sur la configuration SD-WAN, consultez Configuration SD-WAN pour l'intégration de Citrix DaaS.

1. Dans **Gérer > Déploiement rapide**, développez **Connexions réseau** sur la droite.
2. Sélectionnez **Ajouter une connexion**.
3. Sur la page **Ajouter une connexion réseau**, cliquez n'importe où dans la zone SD-WAN.
4. La page suivante résume la suite. Lorsque vous avez terminé la lecture, sélectionnez **Démarrer la configuration du SD-WAN**.
5. Sur la page **Configurer SD-WAN**, saisissez les informations fournies par votre administrateur SD-WAN Orchestrator.

- **Mode de déploiement :** si vous sélectionnez **Haute disponibilité**, deux appliances VPX sont créées (recommandé pour les environnements de production). Si vous sélectionnez **Autonome**, une appliance est créée. Vous ne pouvez pas modifier ce paramètre ultérieurement. Pour passer au mode de déploiement, vous devez supprimer et recréer la succursale et tous les catalogues associés.
- **Nom :** saisissez un nom pour le site SD-WAN.
- **Débit et nombre de bureaux :** ces informations sont fournies par votre administrateur SD-WAN Orchestrator.
- **Région :** région dans laquelle les appliances VPX seront créées.
- **Sous-réseau VDA et sous-réseau SD-WAN :** ces informations sont fournies par votre administrateur SD-WAN Orchestrator. Consultez Configuration requise et préparation de la connexion SD-WAN pour savoir comment éviter les conflits.

6. Lorsque vous avez terminé, sélectionnez **Créer une succursale**.
7. La page suivante résume les éléments à rechercher dans le tableau de bord **Gérer > Déploiement rapide**. Lorsque vous avez terminé la lecture, sélectionnez **OK**.
8. Dans **Gérer > Déploiement rapide**, la nouvelle entrée SD-WAN sous **Connexions réseau** indique la progression du processus de configuration. Lorsque l'entrée devient orange avec le message `Awaiting activation by SD-WAN administrator`, informez votre administrateur SD-WAN Orchestrator.
9. Pour connaître les tâches d'administrateur SD-WAN Orchestrator, consultez la documentation produit SD-WAN Orchestrator.
10. Lorsque l'administrateur SD-WAN Orchestrator a terminé, l'entrée SD-WAN sous **Connexions réseau** devient verte, avec le message `You can create catalogs using this connection`.

Afficher les détails de la connexion SD-WAN

1. Dans **Gérer > Déploiement rapide**, développez **Connexions réseau** sur la droite.
2. Sélectionnez **SD-WAN** s'il ne s'agit pas de la seule sélection.
3. Sélectionnez la connexion que vous souhaitez afficher.

L'écran comprend :

- **Onglet Détails :** les informations que vous avez indiquées lors de la configuration de la connexion.
- **Onglet Connectivité des succursales :** nom, connectivité Cloud, disponibilité, niveau de bande passante, rôle et emplacement pour chaque succursale et MCN.

Supprimer une connexion SD-WAN

Avant de pouvoir supprimer une connexion SD-WAN, supprimez tous les catalogues qui y sont associés. Consultez la section Supprimer un catalogue.

1. Dans **Gérer > Déploiement rapide**, développez **Connexions réseau** sur la droite.
2. Sélectionnez SD-WAN s'il ne s'agit pas de la seule sélection.
3. Sélectionnez la connexion que vous souhaitez supprimer pour développer ses détails.
4. Dans l'onglet **Détails**, sélectionnez **Supprimer la connexion**.
5. Confirmez la suppression.

Utilisateurs et authentification dans Déploiement rapide

May 17, 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.

Méthodes d'authentification utilisateur

Les utilisateurs doivent s'authentifier lorsqu'ils se connectent à Citrix Workspace pour démarrer leur bureau ou leurs applications.

Déploiement rapide prend en charge les méthodes d'authentification utilisateur suivantes :

- **Azure AD géré :** Azure AD géré est un Azure Active Directory (AAD) fourni et géré par Citrix. Vous n'avez pas besoin de fournir votre propre structure Active Directory. Il suffit d'ajouter vos utilisateurs au répertoire.
- **Votre fournisseur d'identité :** vous pouvez utiliser n'importe quelle méthode d'authentification disponible dans Citrix Cloud.

> **Remarque :**
>
> - Les déploiements Remote PC Access utilisent uniquement Active Directory. Pour plus d'informations, consultez la section Remote PC Access.
> - Si vous utilisez Azure AD Domain Services : les noms UPN de connexion à Workspace doivent contenir le nom de domaine qui a été spécifié lors de l'activation de Azure AD

> Domain Services. Les connexions ne peuvent pas utiliser les noms UPN d'un domaine personnalisé que vous créez, même si ce domaine personnalisé est désigné comme le domaine principal.

La configuration de l'authentification utilisateur inclut les procédures suivantes :

1. Configurez la méthode d'authentification utilisateur dans la configuration de l'espace de travail dans Citrix Cloud.
2. Si vous utilisez Azure géré par Citrix AD pour l'authentification de vos utilisateurs, ajoutez des utilisateurs à l'annuaire.
3. Ajoutez des utilisateurs à un catalogue.

Configurer l'authentification des utilisateurs dans Citrix Cloud

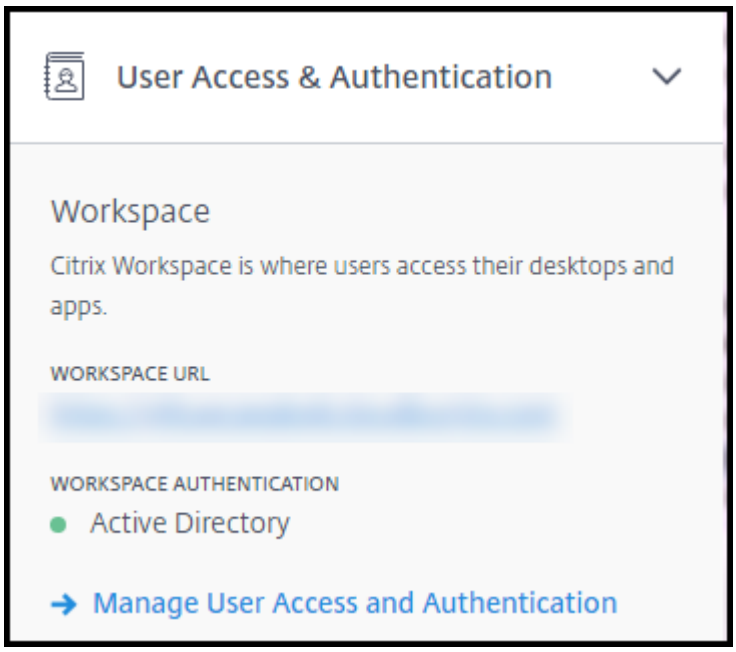
Pour configurer l'authentification des utilisateurs dans Citrix Cloud :

- Connectez-vous à la méthode d'authentification utilisateur que vous souhaitez utiliser. (Dans Citrix Cloud, vous vous « connectez » à une méthode d'authentification ou vous vous en « déconnectez ».)
- Dans Citrix Cloud, définissez l'authentification Workspace pour utiliser la méthode connectée.

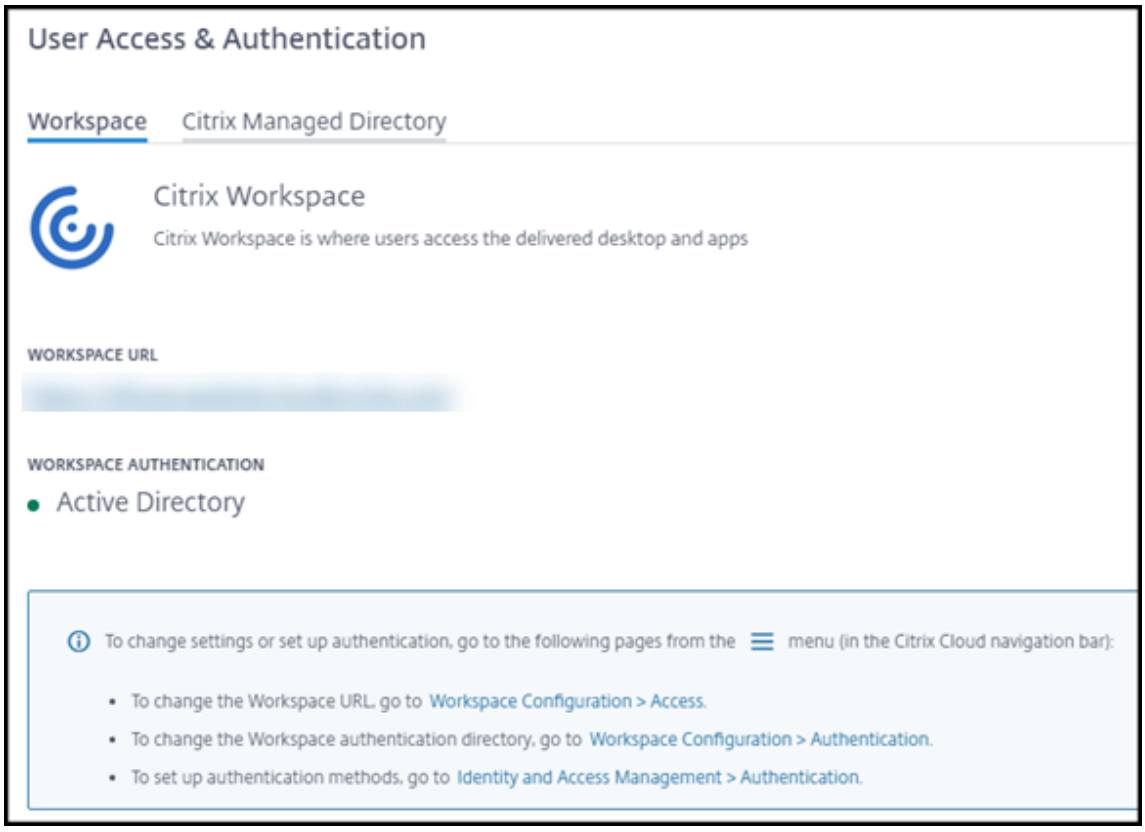
> **Remarque :**
>
> La méthode d'authentification Azure AD géré est configurée par défaut. C'est-à-dire qu'il est automatiquement connecté dans Citrix Cloud et que l'authentification Workspace est automatiquement définie pour utiliser Azure AD géré pour Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Si vous souhaitez utiliser cette méthode (et que vous n'avez pas configuré d'autre méthode auparavant), continuez avec Ajouter et supprimer des utilisateurs dans Azure AD géré.
> Si Azure AD géré est déconnecté, l'authentification Workspace basculera vers Active Directory. Si vous souhaitez utiliser une autre méthode d'authentification, suivez les étapes ci-dessous.

Pour modifier la méthode d'authentification :

1. Dans **Gérer > Déploiement rapide**, sélectionnez **Accès utilisateur et authentification** sur la droite.



2. Sélectionnez **Gérer l'accès utilisateur et l'authentification**. Sélectionnez l'onglet **Workspace**, si ce n'est pas déjà fait. (L'autre onglet indique quelle méthode d'authentification utilisateur est actuellement configurée.)



3. Suivez le lien **Pour configurer les méthodes d'authentification**. Ce lien vous redirige vers

Citrix Cloud. Sélectionnez **Connecter** dans le menu des points de suspension correspondant à la méthode souhaitée.

4. Lorsque vous êtes encore dans Citrix Cloud, sélectionnez **Configuration de l'espace de travail** dans le menu supérieur gauche. Dans l'onglet **Authentification**, sélectionnez la méthode souhaitée.

Que faire ensuite :

- Si vous utilisez Azure géré par Citrix AD, ajoutez des utilisateurs à l'annuaire.
- Pour toutes les méthodes d'authentification, ajoutez des utilisateurs au catalogue.

Ajouter et supprimer des utilisateurs dans Azure AD géré

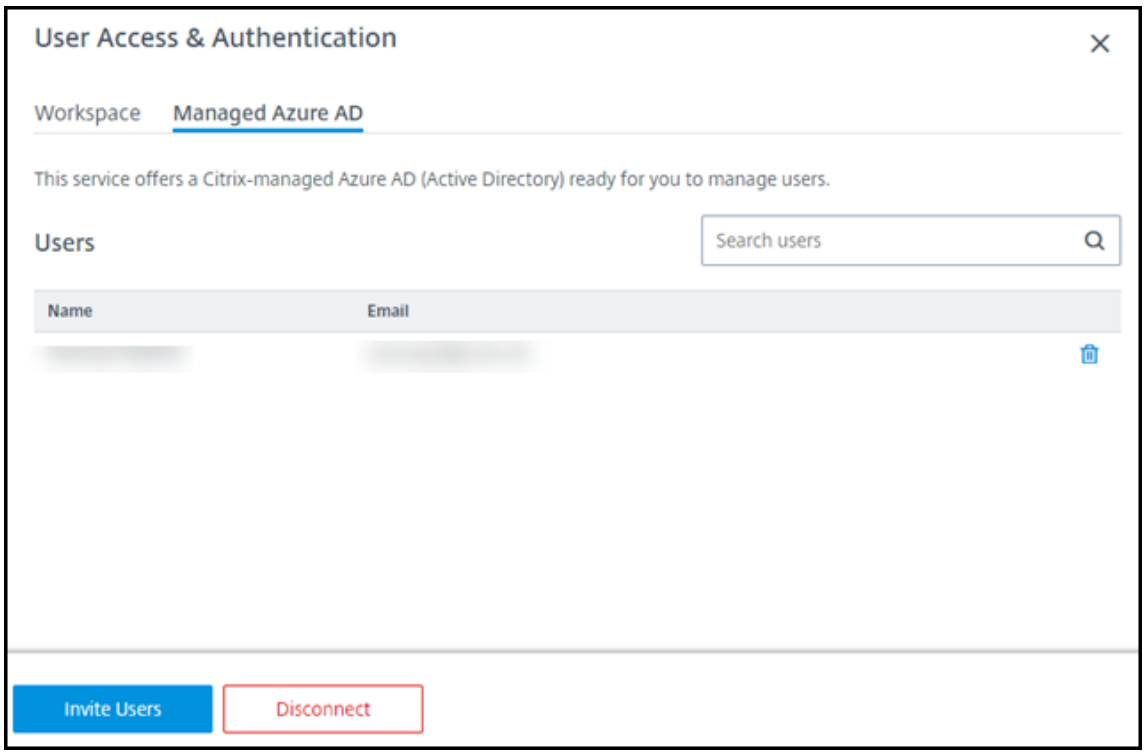
Effectuez cette procédure uniquement si vous utilisez Azure AD géré pour l'authentification des utilisateurs dans Citrix Workspace.

Vous indiquez le nom et les adresses e-mail de vos utilisateurs. Citrix leur envoie ensuite une invitation par e-mail. L'e-mail indique aux utilisateurs de sélectionner un lien qui leur permet de rejoindre Azure AD géré par Citrix.

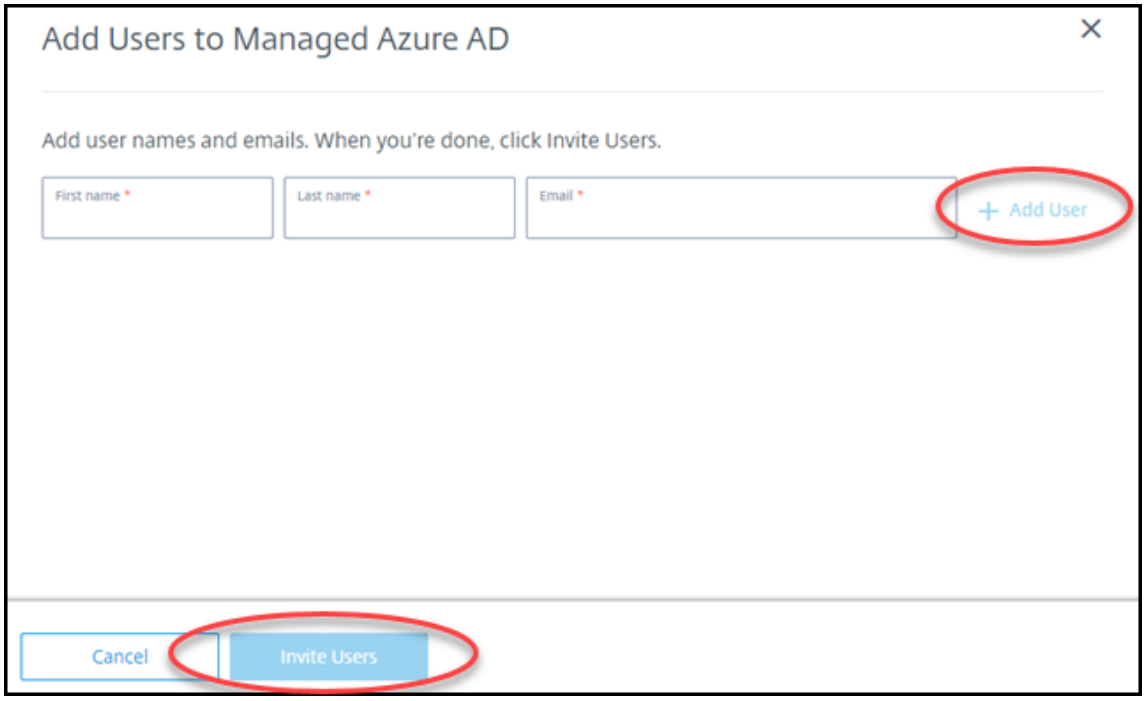
- Si l'utilisateur possède déjà un compte Microsoft associé à l'adresse e-mail que vous avez fournie, ce compte est utilisé.
- Si l'utilisateur ne possède pas de compte Microsoft avec cette adresse e-mail, Microsoft crée un compte.

Pour ajouter et inviter des utilisateurs à Azure AD géré, procédez comme suit :

1. Dans **Gérer > Déploiement rapide**, développez **Accès utilisateur et authentification** sur la droite. Sélectionnez **Gérer l'accès utilisateur et l'authentification**.
2. Sélectionnez l'onglet **Azure AD géré**.
3. Sélectionnez **Inviter des utilisateurs**.



4. Saisissez le nom et l'adresse e-mail d'un utilisateur, puis sélectionnez **Ajouter un utilisateur**.



5. Répétez l'étape précédente pour ajouter d'autres utilisateurs.
6. Lorsque vous avez fini d'ajouter des informations utilisateur, sélectionnez **Inviter des utilisateurs** au bas de la carte.

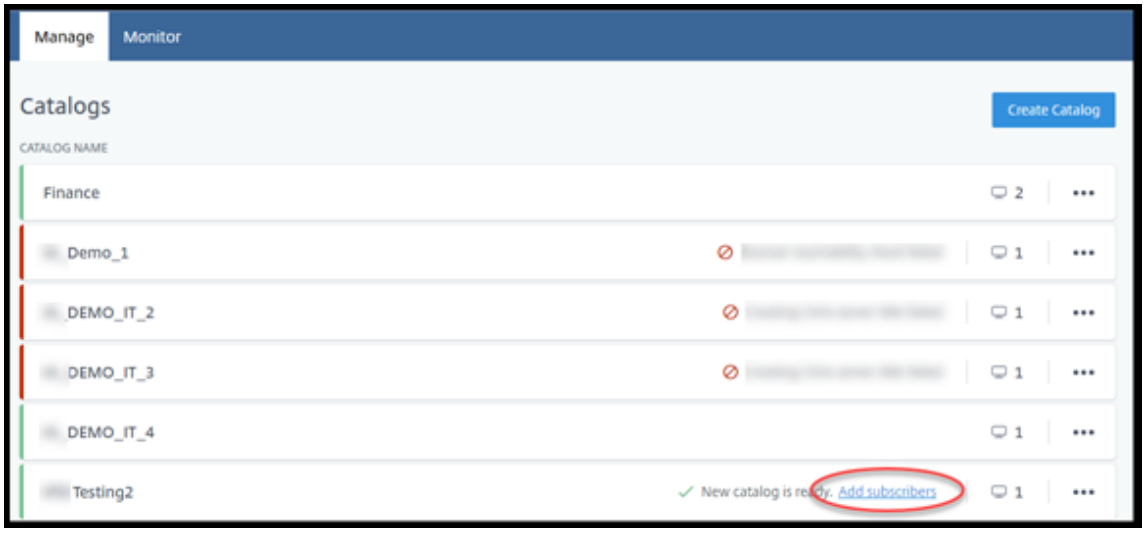
Pour supprimer un utilisateur de Azure AD géré, sélectionnez l'icône de corbeille en regard du nom de l'utilisateur que vous souhaitez supprimer du répertoire. Confirmez la suppression.

Que faire ensuite : Ajouter des utilisateurs au catalogue

Ajouter ou supprimer des utilisateurs dans un catalogue

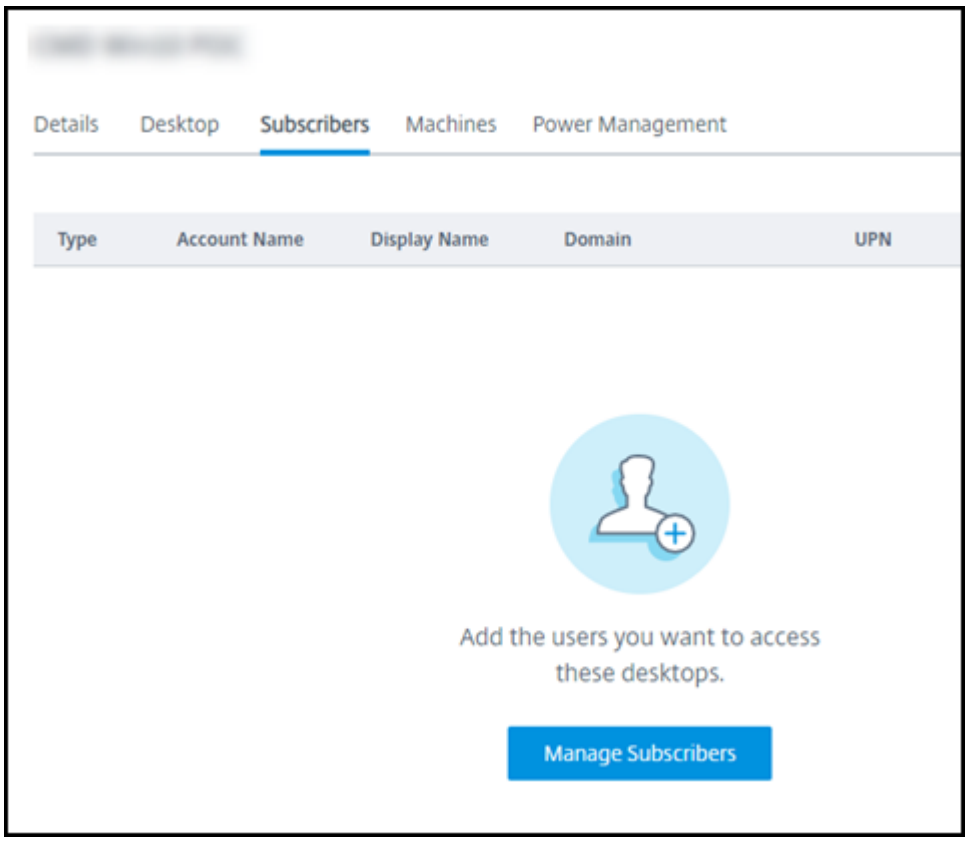
Effectuez cette procédure quelle que soit la méthode d'authentification que vous utilisez.

1. Dans **Gérer > Déploiement rapide**, si vous n'avez ajouté aucun utilisateur à un catalogue, sélectionnez **Ajouter des abonnés**.

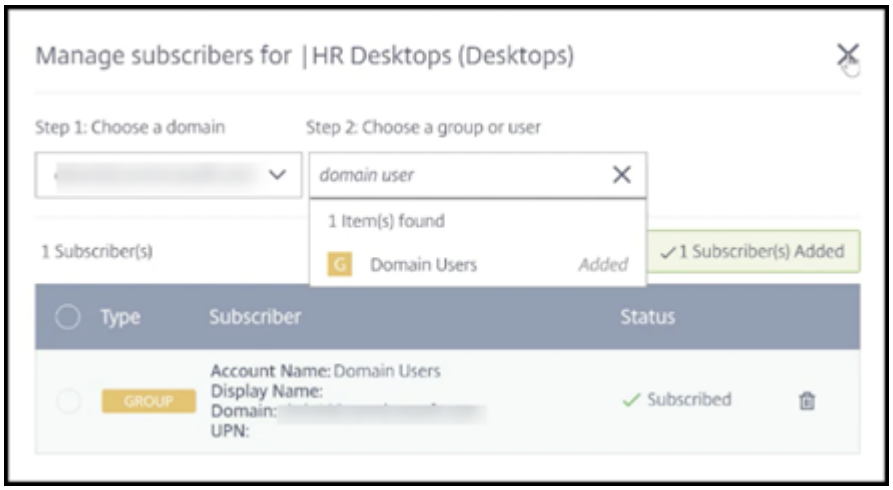


   Pour ajouter des utilisateurs à un catalogue qui compte déjà des utilisateurs, cliquez n'importe où dans l'entrée du catalogue.

2. Dans l'onglet **Abonnés**, sélectionnez **Gérer les abonnés**.



3. Sélectionnez un domaine. (Si vous utilisez Azure AD géré pour l'authentification des utilisateurs, il n'y a qu'une seule entrée dans le champ de domaine.) Sélectionnez ensuite un utilisateur.



4. Sélectionnez d'autres utilisateurs, le cas échéant. Lorsque vous avez terminé, sélectionnez le **X** dans le coin supérieur droit.

Pour supprimer des utilisateurs d'un catalogue, suivez les étapes 1 et 2. À l'étape 3, sélectionnez l'icône de corbeille en regard du nom que vous souhaitez supprimer (au lieu de sélectionner un domaine et un groupe/utilisateur). Cette action supprime l'utilisateur du catalogue, et non de la source

(par exemple Azure AD géré ou votre propre AD ou AAD).

Que faire ensuite :

- Pour un catalogue avec des machines à sessions multiples, ajoutez des applications, si ce n'est déjà fait.
- Pour tous les catalogues, envoyez l'URL Citrix Workspace à vos utilisateurs.

Informations supplémentaires

Pour plus d'informations sur l'authentification dans Citrix Cloud, consultez Gestion des identités et des accès.

Remote PC Access dans Déploiement rapide

February 21, 2023

Introduction

Citrix Remote PC Access permet aux utilisateurs d'utiliser à distance des machines physiques Windows ou Linux situées au bureau. Les utilisateurs bénéficient d'une meilleure expérience utilisateur lorsque Citrix HDX est utilisé pour fournir leur session PC de bureau.

Remote PC Access prend en charge les machines jointes à un domaine.

Cet article explique comment créer un déploiement Remote PC Access à l'aide de l'interface Déploiement rapide. Pour créer un déploiement Remote PC Access à l'aide de l'interface Configuration complète, reportez-vous à la section Remote PC Access.

Différences par rapport à la fourniture de bureaux et d'applications virtuels

La fonctionnalité Remote PC Access présente plusieurs différences avec la fourniture de bureaux et d'applications virtuels :

- Un catalogue Remote PC Access contient généralement des machines physiques existantes. Il n'est donc pas nécessaire de préparer une image ou de provisionner des machines pour utiliser Remote PC Access. La fourniture de bureaux et d'applications passe généralement par des machines virtuelles (MV), et une image est utilisée comme modèle pour provisionner les machines virtuelles.

- Lorsqu'une machine d'un catalogue de pool aléatoire Remote PC Access est mise hors tension, elle n'est pas réinitialisée à l'état d'origine de l'image.
- Pour les catalogues d'attribution d'utilisateur statiques Remote PC Access, l'attribution se produit après la connexion d'un utilisateur (soit sur la machine, soit via RDP). Lors de la livraison de bureaux et d'applications, un utilisateur est attribué si une machine est disponible.

Résumé de l'installation et de la configuration

Consultez cette section avant de commencer les tâches.

1. Avant de commencer :
   a) Consultez la configuration requise et les considérations.
   b) Effectuez les tâches de préparation.
2. À partir de Citrix Cloud :
   a) Configurez un compte Citrix Cloud et abonnez-vous à Citrix DaaS.
   b) Configurez un emplacement des ressources qui peut accéder à vos ressources Active Directory. Installez au moins deux Cloud Connectors dans l'emplacement des ressources. Les Cloud Connectors communiquent avec Citrix Cloud.

      Suivez les instructions pour créer un emplacement de ressources et y installer des Cloud Connector. Ces informations incluent la configuration système requise, la préparation et les procédures.
   c) Connectez Active Directory à Citrix Cloud.
3. Installez un Citrix Virtual Delivery Agent (VDA) sur chaque machine à laquelle les utilisateurs accèderont à distance. Les VDA communiquent avec Citrix Cloud via les Cloud Connectors dans l'emplacement des ressources.
4. Dans **Gérer > Déploiement rapide** :
   a) Créez un catalogue Remote PC Access. Dans cette procédure, vous indiquez l'emplacement de votre emplacement de ressources et sélectionnez la méthode d'attribution de l'utilisateur.
   b) Ajoutez des abonnés (utilisateurs) au catalogue, si nécessaire. Ajoutez des utilisateurs à un catalogue si le catalogue utilise la méthode d'attribution d'utilisateurs automatique statique ou de pool aléatoire. Il n'est pas nécessaire d'ajouter des utilisateurs à un catalogue préattribué statique.
5. Envoyez l'URL de l'espace de travail aux utilisateurs. À partir de leur espace de travail, les utilisateurs peuvent se connecter à leurs machines au bureau.

Configuration requise et considérations

Les références aux machines dans cette section font référence aux machines auxquelles les utilisateurs accèdent à distance.

Général

- Les machines doivent exécuter un système d'exploitation à session unique Windows 10 ou Linux (Red Hat Enterprise Linux et Ubuntu).
- La machine doit être jointe à un domaine des services de domaine Active Directory.
- Si vous connaissez bien l'utilisation de Remote PC Access avec Citrix Virtual Apps and Desktops, la fonctionnalité de veille sur le réseau local (Wake-on-LAN) n'est pas disponible dans Citrix DaaS.

Réseau

- La machine 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 :
  - Définissez les paramètres d'alimentation pour laisser la carte sans fil allumée.
  - 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. La machine n'est pas disponible pour un accès à distance tant qu'un utilisateur ne se connecte pas.
  - Assurez-vous que les Cloud Connectors sont accessibles depuis le réseau Wi-Fi.

Appareils et périphériques

- Les appareils 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.
- Connectez le clavier et la souris directement à la machine. 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.

- Pour les ordinateurs portables et les appareils Surface Pro : assurez-vous que l'ordinateur portable est connecté à une source d'alimentation au lieu de fonctionner sur batterie. Configurez les options d'alimentation de l'ordinateur portable pour qu'elles correspondent à un ordinateur de bureau. Par exemple :

  - Désactivez la fonctionnalité de veille prolongée.
  - Désactivez la fonctionnalité de veille.
  - Définissez l'action de fermeture de l'écran sur **Ne rien faire**.
  - Définissez l'action d'**appui sur le bouton d'alimentation** sur **Arrêter**.
  - Désactivez les fonctionnalités d'économie d'énergie de la carte vidéo et de la carte réseau.

  Lorsque vous utilisez une station d'accueil, vous pouvez retirer et reconnecter les ordinateurs portables. Lorsque vous retirez l'ordinateur portable, le VDA se réenregistre auprès des Cloud Connectors 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. D'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 :

  - Dans **Démarrer > Paramètres > Système > Alimentation et veille**, réglez **Veille** sur **Jamais**.
  - Dans **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 sélectionnée.

Linux VDA

- 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.
- Les catalogues avec des machines Linux doivent utiliser la méthode d'attribution des utilisateurs préattribuée statique. Les catalogues avec des machines Linux ne peuvent pas utiliser les méthodes d'attribution automatique statique ou de pool aléatoire.

Considérations relatives à Workspace

- Plusieurs utilisateurs avec l'accès au même PC de bureau voient la même icône dans Citrix Workspace. Lorsqu'un utilisateur se connecte à Citrix Workspace, cette machine apparaît indisponible si elle est déjà utilisée par un autre utilisateur.

Préparer

- Décidez comment installer le VDA sur les machines. Plusieurs méthodes sont possibles :
  - Installer manuellement le VDA sur chaque machine.
  - Pousser l'installation du VDA à l'aide de la stratégie de groupe en utilisant un script.
  - Pousser l'installation du VDA à l'aide d'un outil de distribution électronique de logiciels (ESD) tel que Microsoft System Center Configuration Manager (SCCM). Pour de plus amples informations, consultez Installer les VDA à l'aide de SCCM.
- Découvrez les méthodes d'attribution des utilisateurs et décidez de la méthode que vous allez utiliser. Vous spécifiez la méthode lors de la création d'un catalogue Remote PC Access.
- Décidez comment les machines (il s'agit en fait des VDA que vous installez sur les machines) vont s'enregistrer auprès de Citrix Cloud. Un VDA doit s'enregistrer pour établir des communications avec le session broker dans Citrix Cloud.

  Les VDA s'inscrivent via les Cloud Connectors dans l'emplacement des ressources. Vous pouvez spécifier des adresses Cloud Connector lorsque vous installez un VDA ou le faire ultérieurement.

  Pour le premier enregistrement (initial) d'un VDA, Citrix recommande d'utiliser un objet de stratégie de groupe ou LGPO basé sur des règles. Après l'enregistrement initial, Citrix recommande d'utiliser la mise à jour automatique, qui est activée par défaut. En savoir plus sur l'enregistrement VDA.

Installer un VDA

Téléchargez et installez un VDA sur chaque machine physique à laquelle les utilisateurs auront accès à distance.

Télécharger un VDA

- Pour télécharger un VDA Windows :
  1. À l'aide des informations d'identification de votre compte Citrix Cloud, accédez à la page de téléchargement Citrix DaaS.

2. Téléchargez la dernière version du VDA. Deux types de packages d'installation sont disponibles. Les valeurs de l'année et du mois dans le titre VDA varient.

- Pour télécharger un VDA Linux pour Remote PC Access, suivez les instructions de la documentation du Linux VDA.

Types de packages d'installation VDA Windows Le site de téléchargement Citrix fournit deux types de package d'installation VDA Windows pouvant être utilisés pour les machines Remote PC Access :

- Installateur VDA principal à session unique (la*version* est au format *aamm*) : `VDAWorkstationCoreSetup.exe`

  Le programme d'installation VDA principal à session unique est spécialement conçu pour Remote PC Access. Il est léger et plus facile à déployer (que les autres installateurs de VDA) sur toutes les machines du réseau. Il n'inclut pas les composants qui ne sont généralement pas nécessaires dans ces déploiements, tels que Citrix Profile Management, Machine Identity Service et la couche de personnalisation des utilisateurs.

  Toutefois, si Citrix Profile Management n'est pas installé, les affichages de Citrix Analytics for Performance et certains détails de Surveiller ne sont pas disponibles. Pour plus d'informations sur ces limitations, consultez l'article de blog Surveillance et dépannage des machines Remote PC Access.

  Si vous souhaitez des écrans d'analyse et de surveillance complets, utilisez le programme d'installation VDA complet à session unique.

- Installateur VDA complet à session unique (*version* au format *aamm*) : `VDAWorkstationSetup_release.exe`

  Bien que le programme d'installation VDA complet à session unique soit un package plus volumineux que le programme d'installation VDA principal à session unique, vous pouvez l'adapter pour installer uniquement les composants dont vous avez besoin. Par exemple, vous pouvez installer les composants prenant en charge Profile Management.

Installer un VDA Windows pour Remote PC Access de manière interactive

1. Double-cliquez sur le fichier d'installation du VDA que vous avez téléchargé.
2. Sur la page **Environnement**, sélectionnez **Activer Remote PC Access**, puis cliquez sur **Suivant**.
3. Sur la page **Delivery Controller**, sélectionnez l'une des options suivantes :

   - Si vous connaissez les adresses de vos Cloud Connectors, sélectionnez **Effectuer manuellement**. Saisissez le nom de domaine complet d'un Cloud Connector, puis

cliquez sur **Ajouter**. Répétez cette opération pour les autres Cloud Connectors de votre emplacement des ressources.

- Si vous savez où vous avez installé les Cloud Connectors dans votre structure Active Directory, sélectionnez **Choisir les emplacements d'Active Directory**, puis accédez à cet emplacement. Répétez cette opération pour les autres Cloud Connectors.
- Si vous souhaitez spécifier les adresses Cloud Connector dans la stratégie de groupe Citrix, sélectionnez **Le faire plus tard (Avancé)**, puis confirmez cette sélection lorsque vous y êtes invité.

Lorsque vous avez terminé, cliquez sur **Suivant**.

4. Si vous utilisez le programme d'installation VDA complet à session unique, sur la page **Composants supplémentaires**, sélectionnez les composants que vous souhaitez installer, tels que Profile Management. (Cette page n'apparaît pas si vous utilisez le programme d'installation VDA principal à session unique.)
5. Sur la page **Fonctionnalités**, cliquez sur **Suivant**.
6. Sur la page **Pare-feu**, sélectionnez **Automatiquement** (si ce n'est pas déjà le cas). Cliquez ensuite sur **Suivant**.
7. Sur la page **Résumé**, cliquez sur **Installer**.
8. Sur la page **Diagnostiquer**, cliquez sur **Connexion**. Assurez-vous que la case à cocher est sélectionnée. Lorsque vous y êtes invité, saisissez vos informations d'identification de compte Citrix. Une fois vos informations d'identification validées, cliquez sur **Suivant**.
9. Sur la page **Terminer**, cliquez sur **Terminer**.

Pour plus d'informations sur l'installation, consultez la section Installer des VDA.

Installer un VDA Windows pour Remote PC Access à l'aide d'une ligne de commandes

- Si vous utilisez le programme d'installation VDA principal à session unique : exécutez `VDAWorkstationCoreSetup.exe` et incluez les options `/quiet`, `/enable_hdx_ports` et `/enable_hdx_udp_ports`. Pour spécifier des adresses Cloud Connector, utilisez l'option `/controllers`.

  Par exemple, la commande suivante installe un VDA principal à session unique. L'application Citrix Workspace et les autres services non fondamentaux ne sont pas installés. Les noms de domaine complets de deux Cloud Connectors sont spécifiés, et les ports du Service de pare-feu Windows seront automatiquement ouverts. L'administrateur doit gérer les redémarrages.

  ```
  VDAWorkstationCoreSetup .exe /quiet /controllers "Connector-East.domain.com"“Connector-East2.domain.com” /enable_hdx_ports /noreboot
  ```


- Si vous utilisez le programme d'installation VDA complet à session unique et que vous souhaitez inclure Profile Management (ou d'autres composants facultatifs) : exécutez `VDAWorkstationSetup.exe` et incluez les options `/remotepc` et `/includeadditional`. L'option `/remotepc` empêche l'installation de la plupart des composants supplémentaires. L'option `/includeadditional` spécifie exactement les composants supplémentaires que vous souhaitez installer.

  Par exemple, la commande suivante empêche l'installation de tous les composants supplémentaires facultatifs, à l'exception de Profile Management.

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /includeadditional "Citrix User Profile Manager","Citrix User Profile Manager WMI Plugin" /controllers "connector.domain.com" "connector2.domain.com" /enable_hdx_ports /noresume /noreboot
  ```

Pour plus d'informations, consultez les options de ligne de commande pour installer un VDA.

Installer un VDA Linux

Suivez les instructions de la documentation Linux pour installer un VDA Linux de manière interactive ou en utilisant la ligne de commandes.

Créez un catalogue Remote PC Access

Un emplacement des ressources contenant au moins deux Cloud Connectors doit exister avant de pouvoir créer un catalogue.

> **Important :**
>
> Une machine ne peut appartenir qu'à un seul catalogue à la fois. Cette restriction n'est pas appliquée lorsque vous spécifiez les machines à ajouter à un catalogue. Toutefois, ignorer la restriction peut entraîner des problèmes ultérieurement.

1. Connectez-vous à Citrix Cloud.
2. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.
3. Si vous n'avez pas encore créé de catalogues, cliquez sur **Commencer** sur la page d'**accueil**.
4. Sélectionnez **Gérer > Déploiement rapide**.
5. Sélectionnez **Créer un catalogue**.
6. Dans l'onglet **Remote PC Access**, sélectionnez une méthode pour attribuer des utilisateurs à des machines.

7. Saisissez un nom pour le catalogue et sélectionnez l'emplacement des ressources que vous avez créé.
8. Ajoutez des machines.
9. Cliquez sur **Créer un catalogue**.
10. Sur la page **Votre catalogue Remote PC Access est en cours de création…**, cliquez sur **Terminé**.
11. Une entrée pour le nouveau catalogue apparaît dans le tableau de bord **Gérer > Déploiement rapide**.

    Une fois le catalogue créé, cliquez sur l'un des liens pour ajouter des abonnés (utilisateurs) au catalogue. Cette étape s'applique si le catalogue utilise la méthode d'attribution d'utilisateurs automatique statique ou de pool aléatoire sans attribution.

Après avoir créé un catalogue et ajouté des utilisateurs (si nécessaire), envoyez l'URL Workspace à vos utilisateurs.

Méthodes d'attribution d'utilisateurs

La méthode d'attribution d'utilisateurs que vous choisissez lors de la création d'un catalogue indique comment les utilisateurs sont affectés aux machines.

- Attribution **automatique statique :** l'attribution d'un utilisateur se produit lorsque celui-ci se connecte à la machine (sans utiliser Citrix, par exemple, en personne ou via RDP), après l'installation d'un VDA sur la machine. Plus tard, si d'autres utilisateurs se connectent à cette machine (sans Citrix), ils sont également attribués. Un seul utilisateur peut utiliser la machine à la fois. Il s'agit d'une configuration typique pour les employés de bureau ou les employés travaillant en équipe qui partagent un ordinateur.

  Cette méthode est prise en charge pour les machines Windows. Elle ne peut pas être utilisée avec des machines Linux.

- **Préattribué statique :** les utilisateurs sont préattribués aux machines. (Cela est généralement configuré en téléchargeant un fichier CSV contenant le mappage de l'utilisateur à la machine.) Il n'est pas nécessaire d'ouvrir une session utilisateur pour établir une attribution après l'installation du VDA. Il n'est pas non plus nécessaire d'attribuer des utilisateurs au catalogue une fois qu'il a été créé. C'est la meilleure option pour les employés de bureau.

  Cette méthode est prise en charge pour les machines Windows et Linux.

- **Pool aléatoire sans attribution :** les utilisateurs sont attribués de façon aléatoire à une machine disponible. Un seul utilisateur peut utiliser la machine à la fois. C'est idéal pour les laboratoires informatiques en milieu scolaire.

Cette méthode est prise en charge pour les machines Windows. Elle ne peut pas être utilisée avec des machines Linux.

Méthodes d'ajout de machines à un catalogue

N'oubliez pas : un VDA doit être installé sur chaque machine.

Lorsque vous créez ou modifiez un catalogue, vous pouvez ajouter des machines à un catalogue de trois manières :

- Sélectionnez des comptes de machines un par un.
- Sélectionnez des unités d'organisation.
- Ajoutez en vrac à l'aide d'un fichier CSV. Vous pouvez utiliser un modèle pour le fichier CSV.

Ajouter des noms de machines

Cette méthode ajoute des comptes de machines un par un.

1. Sélectionnez votre domaine.
2. Recherchez le compte de machine.
3. Cliquez sur **Ajouter**.
4. Répétez l'opération pour ajouter d'autres machines.
5. Lorsque vous avez fini d'ajouter des machines, cliquez sur **Terminé**.

Ajouter des unités d'organisation

Cette méthode ajoute des comptes de machine en fonction de l'unité d'organisation où ils se trouvent.
Lorsque vous sélectionnez des unités d'organisation, choisissez des unités d'organisation de niveau inférieur pour une plus grande granularité. Si une telle granularité n'est pas requise, vous pouvez choisir des unités d'organisation de plus haut niveau.

Par exemple, dans le cas de `Bank`/`Officers`/`Tellers`, sélectionnez `Tellers` pour une plus grande granularité. Sinon, vous pouvez sélectionner `Officers` ou `Bank` en fonction des besoins.

Le déplacement ou la suppression d'unités d'organisation après leur attribution à un catalogue Remote PC Access affecte les associations de VDA et entraîne des problèmes avec les attributions futures. Assurez-vous que votre plan de modification Active Directory tient compte des mises à jour des affectations d'unité d'organisation pour les catalogues.

Pour ajouter des unités d'organisation :

1. Sélectionnez votre domaine.

2. Sélectionnez les unités d'organisation qui contiennent les comptes de machines que vous souhaitez ajouter.
3. Indiquez à l'aide de la case à cocher si vous souhaitez inclure des sous-dossiers dans vos sélections.
4. Lorsque vous avez fini de sélectionner des unités d'organisation, cliquez sur **Terminé**.

Ajouter en vrac

1. Cliquez sur **Télécharger le modèle CSV**.
2. Dans le modèle, ajoutez les informations du compte de machine (jusqu'à 100 entrées). Le fichier CSV peut également contenir les noms des utilisateurs attribués à chaque machine.
3. Enregistrez le fichier.
4. Faites glisser le fichier sur la page **Ajouter des machines en vrac** ou accédez au fichier.
5. Un aperçu du contenu du fichier s'affiche. Si ce n'est pas le fichier souhaité, vous pouvez créer un autre fichier, puis le faire glisser ou y accéder.
6. Lorsque vous avez terminé, cliquez sur **Terminé**.

Gérer les catalogues Remote PC Access

Pour afficher ou modifier les informations de configuration d'un catalogue Remote PC Access, sélectionnez le catalogue dans le tableau de bord **Gérer > Déploiement rapide** (cliquez n'importe où dans l'entrée du catalogue).

- Dans l'onglet **Détails**, vous pouvez ajouter ou supprimer des machines.
- Dans l'onglet **Abonnés**, vous pouvez ajouter ou supprimer des utilisateurs.
- Dans l'onglet **Machines**, vous pouvez :
  - Ajouter ou supprimer des machines : bouton **Ajouter ou supprimer des machines**.
  - Modifier les attributions d'utilisateurs : icône de corbeille **Supprimer attribution**, **Modifier l'attribution de machine** dans le menu des points de suspension.
  - Vous voyez les machines enregistrées. Mettez les machines en mode de maintenance ou hors du mode de maintenance.

Surveillance dans Déploiement rapide

May 19, 2022

À partir du tableau de bord **Surveiller**, vous pouvez afficher l'utilisation des bureaux, les sessions et les machines dans votre déploiement Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Vous pouvez également contrôler les sessions, gérer l'alimentation des machines et mettre fin aux applications et aux processus en cours d'exécution.

Pour accéder au tableau de bord **Surveiller** :

1. Connectez-vous à Citrix Cloud si vous ne l'avez pas déjà fait. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.
2. Dans le tableau de bord **Gérer > Déploiement rapide**, sélectionnez l'onglet **Surveiller**.

Surveiller l'utilisation du bureau

Les affichages sur cette page sont actualisés toutes les cinq minutes.

- **Vue d'ensemble de la machine et des sessions :** vous pouvez adapter l'affichage pour afficher des informations sur tous les catalogues (par défaut) ou sur un catalogue sélectionné. Vous pouvez également adapter la période : le dernier jour, la dernière semaine, le dernier mois ou les trois derniers mois.

  Les chiffres en haut de l'écran indiquent le nombre total de machines, plus le nombre de machines sous tension et hors tension. Survolez une valeur pour afficher le nombre de machines en session unique et en sessions multiples.

  Le graphique situé sous les décomptes montre le nombre de machines sous tension et de sessions simultanées de pointe à intervalles réguliers pendant la période que vous avez sélectionnée. Survolez un point du graphique pour afficher les décompte à ce moment précis.

- **Top 10 :** pour personnaliser un affichage Top 10, sélectionnez une période : la dernière semaine (par défaut), le dernier mois ou les trois derniers mois. Vous pouvez également adapter l'af-

fichage pour afficher uniquement des informations sur l'activité impliquant des machines à session unique, à sessions multiples ou des applications.

- **Top 10 des utilisateurs actifs :** répertorie les utilisateurs qui ont démarré des bureaux le plus fréquemment pendant la période. Survoler une ligne affiche le nombre total de bureaux lancés.
- **Top 10 des catalogues actifs :** répertorie les catalogues dont la durée est la plus longue pendant la période sélectionnée. La durée est la somme de toutes les sessions utilisateur de ce catalogue.

Rapport sur l'utilisation du bureau

Pour télécharger un rapport contenant des informations sur les lancements de machines au cours du dernier mois, sélectionnez **Activités de lancement**. Un message indique que la demande est en cours de traitement. Le rapport est automatiquement téléchargé vers l'emplacement de téléchargement par défaut sur la machine locale.

Filtrer et rechercher pour surveiller les machines et les sessions

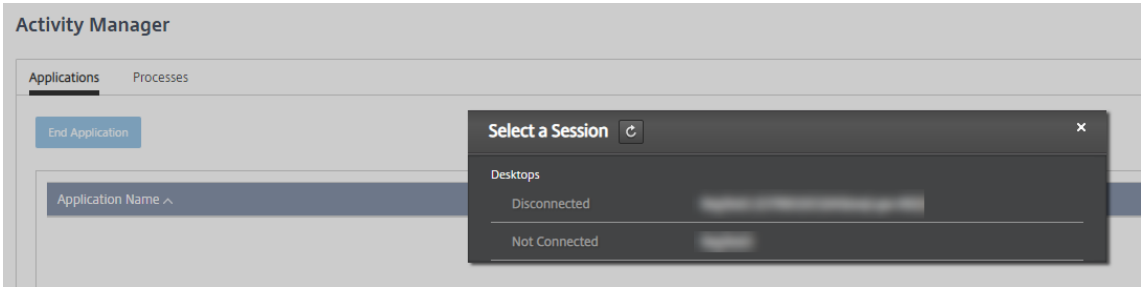
Lorsque vous surveillez les informations de session et de machine, toutes les machines ou sessions sont affichées par défaut. Vous pouvez :

- filtrer l'affichage par machines, sessions, connexions ou applications ;
- affiner l'affichage des sessions ou des machines en choisissant les critères souhaités, en créant un filtre à l'aide d'expressions ;
- enregistrer les filtres que vous créez pour les réutiliser.

Contrôler les applications d'un utilisateur

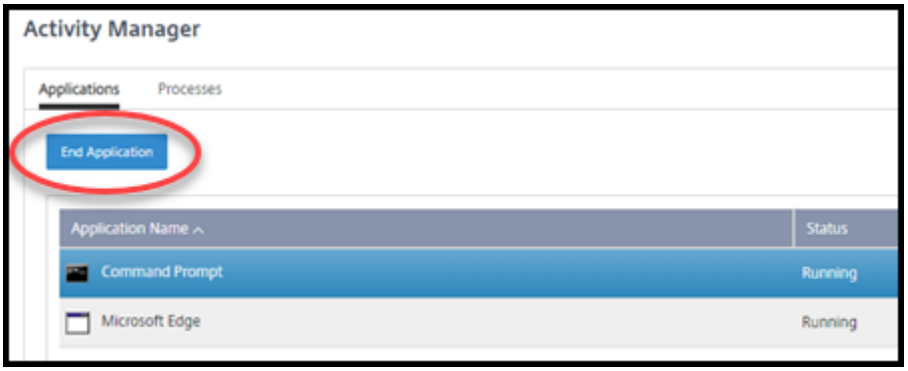
Vous pouvez afficher et gérer des applications et des processus pour un utilisateur disposant d'une session en cours d'exécution ou ayant un bureau attribué.

1. Dans le tableau de bord **Surveiller** de Citrix DaaS, sélectionnez **Rechercher** et saisissez le nom d'utilisateur (ou les premiers caractères du nom d'utilisateur), la machine ou le point de terminaison. Dans les résultats de la recherche, sélectionnez l'article que vous recherchez. (Pour réduire la zone de recherche sans effectuer de recherche, sélectionnez à nouveau **Rechercher**.)
2. Sélectionnez une session.



Le Gestionnaire d'activités répertorie les applications et les processus de la session de l'utilisateur.

3. Pour mettre fin à une application, sous l'onglet **Applications** du Gestionnaire d'activités, sélectionnez l'application dans la ligne correspondante, puis sélectionnez **Arrêter l'application**.



4. Pour terminer un processus, sous l'onglet **Processus** du Gestionnaire d'activités, sélectionnez le processus dans la ligne correspondante, puis sélectionnez **Arrêter le processus**.
5. Pour afficher les détails de la session, sélectionnez **Détails** en haut à droite. Pour revenir à l'affichage des applications et des processus, sélectionnez Gestionnaire d'activités en haut à droite.
6. Pour contrôler la session, sélectionnez **Contrôle de session > Fermer la session** ou **Contrôle de session > Déconnecter**.

Observer les utilisateurs

Utilisez la fonction d'observation pour afficher ou travailler directement sur la machine virtuelle ou la session d'un utilisateur. Vous pouvez observer des VDA Windows et Linux. L'utilisateur doit être connecté à la machine que vous souhaitez observer. Pour vérifier cette connexion, vérifiez le nom de la machine indiqué dans la barre de titre `User`.

L'observation se lance dans un nouvel onglet de navigateur. Assurez-vous que votre navigateur autorise les fenêtres contextuelles à partir de l'URL Citrix Cloud.

L'observation est prise en charge uniquement pour les utilisateurs sur des machines jointes à un domaine. Pour observer une machine non jointe à un domaine, vous devez configurer une machine bastion. Pour plus de détails, voir Accéder au Bastion.

L'observation doit être initiée à partir d'une machine sur le même réseau virtuel que les machines jointes au domaine, et répondre à toutes les exigences de port.

Activer l'observation

1. Dans **Gérer > Déploiement rapide > Surveiller**, accédez à la vue **Détails de l'utilisateur**.
2. Sélectionnez la session utilisateur, puis cliquez sur **Observer** dans la vue **Gestionnaire d'activités** ou dans le panneau **Détails de la session**.

Observer les 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.

Surveiller utilise le nom de domaine complet pour se connecter au VDA Linux cible. Assurez-vous que le client du service de surveillance peut résoudre le nom de domaine complet du VDA Linux.

- Les paquets `python-websockify` et `x11vnc` doivent être installés sur le VDA.
- La connexion `noVNC` au VDA utilise le protocole WebSocket. Par défaut, le protocole WebSocket `ws://` est utilisé. Pour des raisons de sécurité, Citrix recommande que vous utilisiez le protocole `wss://` sécurisé. Installez des certificats SSL sur chaque client du service de surveillance et VDA Linux.

Suivez les instructions dans Observation de session pour configurer votre VDA Linux pour l'observation.

1. Une fois que vous avez activé l'observation, la connexion de l'observation démarre et une invite de confirmation s'affiche sur la machine utilisateur.
2. Demandez à l'utilisateur de sélectionner **Oui** pour démarrer la machine ou le partage de session.
3. L'administrateur peut afficher uniquement la session observée.

Observer des VDA Windows

Les sessions de VDA Windows sont observées à l'aide de l'Assistance à distance Windows. Activez la fonctionnalité `Use Windows Remote Assistance` lors de l'installation du VDA.

1. Une fois que vous avez activé l'observation, la connexion d'observation démarre et une boîte de dialogue vous invite à ouvrir ou à enregistrer le fichier `.msrc incident`.
2. Ouvrez le fichier d'incident avec la visionneuse d'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 sélectionner **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.

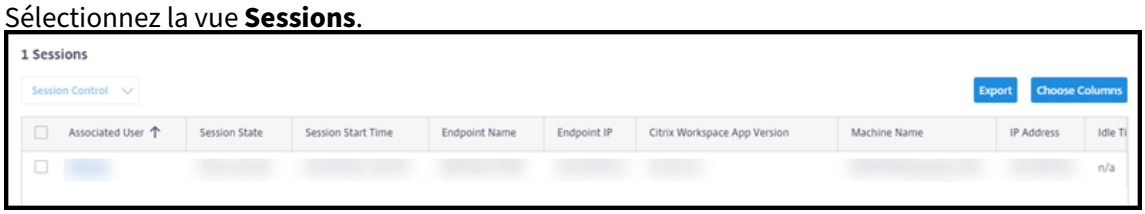
Surveillance et contrôle des sessions

Les écrans de session sont mis à jour chaque minute.

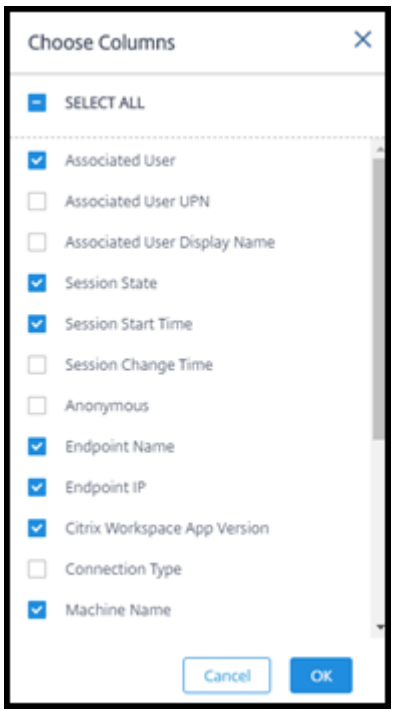
En plus de visualiser les sessions, vous pouvez déconnecter une ou plusieurs sessions ou déconnecter des utilisateurs des sessions.

1. Dans **Gérer > Déploiement rapide > Surveiller**, sélectionnez **Filtres**.

2. Sélectionnez la vue **Sessions**.



3. Pour personnaliser l'affichage, sélectionnez **Choisir des colonnes** et cochez les cases des éléments que vous souhaitez afficher. Lorsque vous avez terminé, sélectionnez **OK**. L'affichage des sessions est automatiquement actualisé.



4. Sélectionnez la case à cocher située à gauche de chaque session que vous souhaitez contrôler.
5. Pour fermer ou déconnecter la session, sélectionnez **Contrôle de session > Fermer la session** ou **Contrôle de session > Déconnecter**.

N'oubliez pas que le programme de gestion de l'alimentation du catalogue peut également contrôler la déconnexion des sessions et la déconnexion des utilisateurs des sessions déconnectées.

Au lieu de suivre la procédure ci-dessus, vous pouvez également **rechercher** un utilisateur, sélectionner la session que vous souhaitez contrôler, puis afficher les détails de la session. Les options de fermeture de session et de déconnexion y sont également disponibles.

Rapport d'informations sur la session

Pour télécharger les informations de session, sélectionnez **Exporter** sur l'écran des sessions. Un message indique que la demande est en cours de traitement. Le rapport est automatiquement téléchargé vers l'emplacement de téléchargement par défaut sur la machine locale.

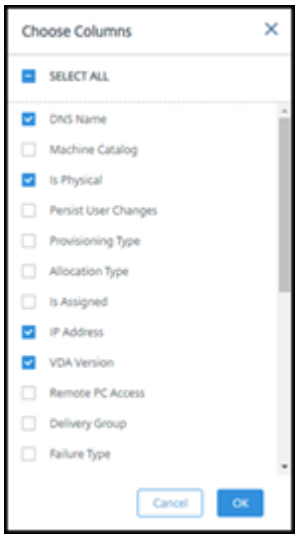
Surveiller et contrôler l'alimentation des machines

Les écrans des machines sont mis à jour chaque minute

1. Dans **Gérer > Déploiement rapide > Surveiller**, sélectionnez **Filtres**.
2. Sélectionnez la vue **Machines**.

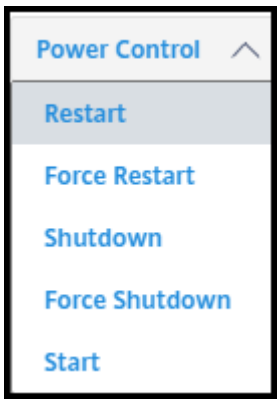
Par défaut, l'affichage répertorie les machines avec OS mono-session. Vous pouvez également afficher des machines à sessions multiples.

3. Pour personnaliser l'affichage, sélectionnez **Choisir des colonnes** et cochez les cases des éléments que vous souhaitez afficher. Lorsque vous avez terminé, sélectionnez **OK**. L'écran des machines est automatiquement actualisé.



4. Pour contrôler l'alimentation des machines ou les placer en mode de maintenance ou hors du mode de maintenance, cochez la case située à gauche de chaque machine que vous souhaitez contrôler.

5. Pour contrôler l'alimentation des machines sélectionnées, sélectionnez **Contrôle de l'alimentation** et sélectionnez une action.



6. Pour placer les machines sélectionnées en mode de maintenance ou hors du mode de maintenance, sélectionnez **Mode de maintenance > ON** ou **Mode Maintenance > OFF**.

Lorsque vous utilisez la fonction de recherche pour rechercher et sélectionner une machine, vous voyez les détails de la machine, son utilisation, son historique d'utilisation (au cours des sept derniers jours) et la moyenne des IOPS.

Rapport d'informations sur la machine

Pour télécharger les informations de session, sélectionnez **Exporter** sur l'écran des machines. Un message indique que la demande est en cours de traitement. Le rapport est automatiquement téléchargé vers l'emplacement de téléchargement par défaut sur la machine locale.

Vérification de l'état des applications et du bureau

La vérification de l'intégrité automatise le processus de vérification de l'état des applications et des bureaux publiés. Les résultats de la vérification de l'intégrité sont disponibles via le tableau de bord **Surveiller**. Pour plus de détails, consultez :

- Analyse d'application.
- Analyse de bureaux

Dépannage dans Déploiement rapide

September 16, 2022

Introduction

Les emplacements de ressources contiennent les machines qui fournissent des bureaux et des applications. Ces machines sont créées dans des catalogues, de sorte que les catalogues sont considérés comme faisant partie de l'emplacement des ressources. Chaque emplacement de ressources contient également des Cloud Connectors. Les Cloud Connectors permettent à Citrix Cloud de communiquer avec l'emplacement des ressources. En général, Citrix installe et met à jour les Cloud Connectors.

Vous avez également la possibilité de lancer plusieurs actions Cloud Connector et d'emplacement des ressources. Voir :

- Actions d'emplacement des ressources
- Paramètres d'emplacement des ressources lors de la création d'un catalogue

Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) dispose d'outils de dépannage et de prise en charge qui peuvent aider à résoudre les problèmes de configuration et de communication avec les machines qui fournissent des bureaux et des applications (VDA). Par exemple, la création d'un catalogue peut échouer ou les utilisateurs peuvent ne pas être en mesure de démarrer leur bureau ou leurs applications.

Ce dépannage inclut l'accès à votre abonnement Azure géré par Citrix via une machine bastion ou un RDP direct. Après avoir accédé à l'abonnement, vous pouvez utiliser les outils de prise en charge Citrix pour localiser et résoudre les problèmes. Pour plus de détails, consultez :

- Dépannage VDA à l'aide d'un bastion ou d'un RDP direct
- Accéder au bastion
- Accès direct à RDP

Dépannage VDA à l'aide d'un bastion ou d'un RDP direct

Les fonctionnalités de prise en charge s'adressent aux personnes expérimentées dans le dépannage des problèmes Citrix. Parmi lesquelles :

- Les Citrix Service Providers (CSP) et d'autres personnes possédant les connaissances techniques et l'expérience de dépannage avec les produits Citrix DaaS.
- Les services de support technique Citrix.

Si vous ne connaissez pas ou n'êtes pas à l'aise avec le dépannage des composants Citrix, vous pouvez demander de l'aide au service de support Citrix. Les techniciens du support Citrix peuvent vous demander de configurer l'une des méthodes d'accès décrites dans cette section. Toutefois, ce sont les techniciens Citrix qui effectuent le dépannage à l'aide des outils et technologies Citrix.

> **Important :**
>
> Ces fonctionnalités de prise en charge ne concernent que les machines jointes à un domaine. Si les machines de vos catalogues ne sont pas jointes à un domaine, vous êtes guidé pour demander de l'aide au dépannage auprès du support Citrix.

Méthodes d'accès

Ces méthodes d'accès concernent uniquement l'abonnement Azure géré par Citrix. Pour plus d'informations, consultez Abonnements Azure.

Deux méthodes d'accès à la prise en charge sont fournies.

- Accédez à vos ressources via une machine bastion dans l'abonnement Azure géré par Citrix dédié du client. Le bastion est un point d'entrée unique qui permet d'accéder aux machines

de l'abonnement. Il fournit une connexion sécurisée à ces ressources en autorisant le trafic distant à partir d'adresses IP dans une plage spécifiée.

Les étapes de cette méthode sont les suivantes :

- création de la machine bastion ;
- téléchargement d'un agent RDP ;
- RDP vers la machine bastion ;
- établissement d'une connexion entre la machine bastion et les autres machines Citrix de votre abonnement.

La machine bastion est destinée à une utilisation à court terme. Cette méthode est destinée aux problèmes liés à la création de catalogues ou de machines d'images.

- Accès RDP direct aux machines de l'abonnement Azure géré par Citrix dédié du client. Pour autoriser le trafic RDP, le port 3389 doit être défini dans le groupe de sécurité réseau.

  Cette méthode est destinée aux problèmes de catalogue autres que la création, tels que les utilisateurs qui ne peuvent pas démarrer leur bureau.

N'oubliez pas : pour remplacer ces deux méthodes d'accès, contactez le support Citrix pour obtenir de l'aide.

Accéder au bastion

1. Dans **Gérer > Déploiement rapide**, développez **Dépannage et support** sur la droite.
2. Cliquez sur **Afficher les options de dépannage**.
3. Sur la page **Dépannage**, sélectionnez l'un des deux premiers types de problèmes, puis cliquez sur **Utiliser notre machine de dépannage**.
4. Sur la page **Dépannage avec machine bastion**, sélectionnez le catalogue.

   - Si les machines du catalogue sélectionné ne sont pas jointes au domaine, vous êtes invité à contacter le support Citrix.
   - Si une machine bastion a déjà été créée avec un accès RDP à la connexion réseau du catalogue sélectionné, passez à l'étape 8.

5. La plage d'accès RDP s'affiche. Si vous souhaitez limiter l'accès RDP à une plage inférieure à celle autorisée par la connexion réseau, sélectionnez la case à cocher **Restreindre l'accès RDP aux ordinateurs dans la plage d'adresses IP**, puis saisissez la plage souhaitée.
6. Saisissez un nom d'utilisateur et un mot de passe que vous utiliserez pour vous connecter lorsque vous effectuerez un RDP sur la machine bastion. Exigences de mot de passe.

   N'utilisez pas de caractères Unicode dans le nom d'utilisateur.

7. Cliquez sur **Créer une machine bastion**.

   Lorsque la machine bastion a été créée, le titre de la page devient **Bastion** —***connexion***.

   Si la création de la machine bastion échoue (ou si elle échoue pendant le fonctionnement), cliquez sur **Supprimer** au bas de la page de notification d'échec. Faites une nouvelle tentative de création de la machine bastion.

   Vous pouvez modifier la restriction de plage RDP après la création de la machine bastion. Cliquez sur **Modifier**. Saisissez la nouvelle valeur, puis cliquez sur la coche pour enregistrer la modification. (Cliquez sur **X** pour annuler la modification.)

8. Cliquez sur **Télécharger le fichier RDP**.
9. RDP vers le bastion, en utilisant les informations d'identification que vous avez spécifiées lors de la création du bastion. (L'adresse de la machine bastion est intégrée au fichier RDP que vous avez téléchargé.)
10. Connectez-vous à partir de la machine bastion aux autres machines Citrix de l'abonnement. Vous pouvez ensuite collecter des journaux et exécuter des diagnostics.

Les machines bastion sont sous tension lorsqu'elles sont créées. Pour réduire les coûts, les machines sont automatiquement mises hors tension si elles restent inactives après le démarrage. Les machines sont supprimées automatiquement après plusieurs heures.

Vous pouvez gérer l'alimentation d'une machine bastion ou la supprimer à l'aide des boutons situés en bas de la page. Si vous choisissez de supprimer une machine bastion, vous devez reconnaître que toutes les sessions actives sur la machine se termineront automatiquement. De plus, toutes les données et les fichiers enregistrés sur la machine seront supprimés.

Accès direct à RDP

1. Dans **Gérer > Déploiement rapide**, développez **Dépannage et support** sur la droite.
2. Cliquez sur **Afficher les options de dépannage**.
3. Sur la page **Dépannage**, sélectionnez **Autre problème de catalogue**.
4. Sur la page **Dépanner l'accès RDP**, sélectionnez le catalogue.

   Si RDP a déjà été activé sur la connexion réseau du catalogue sélectionné, passez à l'étape 7.

5. La plage d'accès RDP s'affiche. Si vous souhaitez limiter l'accès RDP à une plage inférieure à celle autorisée par la connexion réseau, cochez la case **Restreindre l'accès RDP aux ordinateurs dans la plage d'adresses IP**, puis saisissez la plage souhaitée.
6. Cliquez sur **Activer l'accès RDP.**

   Lorsque l'accès RDP est activé, le titre de la page devient **Accès RDP** —***connexion***.

Si l'accès RDP n'est pas activé correctement, cliquez sur **Réessayer d'activer RDP** au bas de la page de notification d'échec.

7. Connectez-vous à des machines en utilisant vos informations d'identification d'administrateur Active Directory. Vous pouvez ensuite collecter des journaux et exécuter des diagnostics.

Obtenir de l'aide

Si vous rencontrez toujours des problèmes, ouvrez un ticket en suivant les instructions de la section Comment obtenir de l'aide.

Référence Déploiement rapide

August 3, 2022

Onglets Catalogue du tableau de bord Déploiement rapide

Dans le tableau de bord **Gérer > Déploiement rapide** de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), cliquez n'importe où dans l'entrée du catalogue. Les onglets suivants contiennent des informations au sujet du catalogue :

- **Détails :** répertorie les informations spécifiées lors de la création du catalogue (ou de sa dernière modification). Cet onglet contient également des informations sur l'image utilisée pour créer le catalogue.

  Dans cet onglet, vous pouvez :

  - modifier l'image utilisée dans le catalogue ;
  - supprimer le catalogue ;
  - accéder à la page contenant les détails de l'emplacement des ressources utilisé par le catalogue.

- **Bureau :** disponible uniquement pour les catalogues contenant des machines à session unique (statiques ou aléatoires). Dans cet onglet, vous pouvez modifier le nom et la description du catalogue.

- **Bureau et applications :** l'onglet **Bureau et applications** est disponible uniquement pour les catalogues contenant des machines à sessions multiples. Dans cet onglet, vous pouvez :

  - ajouter, modifier, ou supprimer des applications auxquelles les utilisateurs du catalogue peuvent accéder dans Citrix Workspace ;

  - modifier le nom et la description du catalogue.

- **Abonnés :** répertorie tous les utilisateurs, y compris leur type (utilisateur ou groupe), leur nom de compte, leur nom d'affichage, ainsi que leur domaine Active Directory et leur nom d'utilisateur principal.

  Dans cet onglet, vous pouvez ajouter ou supprimer des utilisateurs d'un catalogue.

- **Machines :** affiche le nombre total de machines dans le catalogue, ainsi que le nombre de machines enregistrées, de machines non enregistrées et de machines sur lesquelles le mode de maintenance est activé.

  Pour chaque machine du catalogue, l'affichage inclut le nom de chaque machine, l'état d'alimentation (marche/arrêt), l'état d'enregistrement (enregistré ou non enregistré), les utilisateurs attribués, le nombre de sessions (0/1) et l'état du mode de maintenance (icône marche/arrêt).

  Dans cet onglet, vous pouvez :

  - ajouter ou supprimer une machine ;
  - démarrer, redémarrer, forcer le redémarrage ou arrêter une machine ;
  - activer ou désactiver le mode de maintenance d'une machine.

  Pour plus d'informations, consultez la section Gérer les catalogues. La plupart des actions de la machine sont également disponibles dans l'onglet **Surveiller** du tableau de bord Déploiement rapide. Voir Surveiller et contrôler l'alimentation des machines.

- **Gestion de l'alimentation :** vous permet de gérer les moments où les machines du catalogue sont sous tension ou hors tension. Un programme d'alimentation indique également quand les machines inactives sont déconnectées.

  Vous pouvez configurer un programme d'alimentation lorsque vous créez un catalogue personnalisé ou ultérieurement. Si aucun programme d'alimentation n'est explicitement défini, une machine s'éteint à la fin d'une session.

  Lorsque vous créez un catalogue à l'aide de la création rapide, vous ne pouvez pas sélectionner ni configurer un programme d'alimentation. Par défaut, les catalogues créés à l'aide de la création rapide utilisent le calendrier prédéfini Économique. Toutefois, vous pouvez modifier ce catalogue ultérieurement et modifier la planification.

  Pour plus de détails, voir Gérer les calendriers de gestion de l'alimentation.

Serveurs DNS

Cette section s'applique à tous les déploiements contenant des machines jointes à un domaine. Vous pouvez ignorer cette section si vous utilisez uniquement des machines non jointes à un domaine.

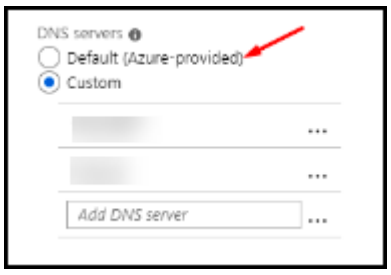
1. Avant de créer un catalogue joint à un domaine (ou une connexion, si vous utilisez un abonnement Azure géré par Citrix), vérifiez si des entrées de serveur DNS peuvent résoudre les noms de domaine publics et privés.

   Lorsque Citrix DaaS crée un catalogue ou une connexion, il recherche au moins une entrée de serveur DNS valide. Si aucune entrée valide n'est trouvée, l'opération de création échoue.

   Où vérifier :

   - Si vous utilisez votre propre abonnement Azure, vérifiez l'entrée des **serveurs DNS** dans votre Azure.
   - Si vous utilisez un abonnement Azure géré par Citrix et que vous créez une connexion de peering de réseau virtuel Azure, vérifiez l'entrée des **serveurs DNS** dans le réseau virtuel Azure que vous êtes en train d'appairer.
   - Si vous utilisez un abonnement Azure géré par Citrix et que vous créez une connexion SD-WAN, vérifiez les entrées DNS dans le SD-WAN Orchestrator.

2. Dans Azure, le paramètre **Personnalisé** doit comporter au moins une entrée valide. Ce service ne peut pas être utilisé avec le paramètre **Défaut (fourni par Azure)**.

   - Si **Défaut (fourni par Azure)** est activé, modifiez le paramètre sur **Personnalisé** et ajoutez au moins une entrée de serveur DNS.
   - Si vous avez déjà des entrées de serveur DNS sous **Personnalisé**, vérifiez que les entrées que vous souhaitez utiliser avec ce service peuvent résoudre les noms IP de domaine public et privé.
   - Si vous ne disposez d'aucun serveur DNS capable de résoudre les noms de domaine, Citrix recommande d'ajouter un serveur DNS fourni par Azure doté de ces fonctionnalités.

3. Si vous modifiez des entrées de serveur DNS, redémarrez toutes les machines connectées au réseau virtuel. Le redémarrage attribue les nouveaux paramètres du serveur DNS. (Les machines virtuelles continuent d'utiliser leurs paramètres DNS actuels jusqu'au redémarrage.)

   Si vous souhaitez modifier les adresses DNS ultérieurement, après la création d'une connexion :

- Lorsque vous utilisez votre propre abonnement Azure, vous pouvez les modifier dans Azure (comme décrit dans les étapes précédentes). Vous pouvez également les modifier dans ce service.

- Lorsque vous utilisez un abonnement Azure géré par Citrix, ce service ne synchronise pas les modifications d'adresse DNS que vous effectuez dans Azure. Toutefois, vous pouvez modifier les paramètres DNS de la connexion dans ce service.

N'oubliez pas que la modification des adresses des serveurs DNS peut potentiellement entraîner des problèmes de connectivité pour les machines des catalogues qui utilisent cette connexion.

Ajouter des serveurs DNS via ce service

Avant d'ajouter une adresse de serveur DNS à une connexion, assurez-vous que le serveur DNS peut résoudre les noms de domaine publics et internes. Citrix recommande de tester la connectivité à un serveur DNS avant de l'ajouter.

1. Pour ajouter, modifier ou supprimer une adresse de serveur DNS lorsque vous créez une connexion, sélectionnez **Modifier les serveurs DNS** sur la page **Ajouter** *un type de connexion*. Ou, si un message indique qu'aucune adresse de serveur DNS n'a été trouvée, sélectionnez **Ajouter des serveurs DNS**. Continuez avec l'étape 3.
2. Pour ajouter, modifier ou supprimer une adresse de serveur DNS pour une connexion existante, procédez comme suit :
    a) Dans **Gérer > Déploiement rapide**, développez **Connexions réseau** sur la droite.
    b) Sélectionnez la connexion que vous souhaitez modifier.
    c) Sélectionnez **Modifier les serveurs DNS**.
3. Ajoutez, modifiez ou supprimez des adresses.
    a) Pour ajouter une adresse, sélectionnez **Ajouter un serveur DNS**, puis saisissez l'adresse IP.
    b) Pour modifier une adresse, cliquez dans le champ d'adresse et modifiez les nombres.
    c) Pour supprimer une adresse, sélectionnez l'icône de corbeille en regard de l'entrée d'adresse. Vous ne pouvez pas supprimer toutes les adresses de serveur DNS. La connexion doit en avoir au moins une.
4. Lorsque vous avez terminé, sélectionnez **Confirmer les modifications** en bas de la page.
5. Redémarrez toutes les machines qui utilisent cette connexion. Le redémarrage attribue les nouveaux paramètres du serveur DNS. (Les machines virtuelles continuent d'utiliser leurs paramètres DNS actuels jusqu'au redémarrage.)

Stratégies

Définir des stratégies de groupe pour les machines non jointes à un domaine

1. RDP vers la machine utilisée pour l'image.

2. Installez Citrix Gestion des stratégies de groupe :

   a) Accédez à CTX220345. Téléchargez la pièce jointe.
   b) Double-cliquez sur le fichier téléchargé. Dans le dossier `Group Policy Templates 1912 > Group Policy Management`, double-cliquez sur `CitrixGroupPolicyManagement.msi`.

3. À l'aide de la commande **Exécuter**, lancez `gpedit.msc` pour ouvrir l'éditeur de stratégie de groupe.

4. Dans `User Configuration Citrix Policies > Unfiltered`, sélectionnez **Modifier la stratégie**.

   Si la console de gestion des stratégies de groupe échoue (comme décrit dans la section CTX225742), installez Microsoft Visual C++ 2015 Runtime (ou une version ultérieure de ce runtime).

5. Activez les paramètres de stratégie si nécessaire. Par exemple :

   - Lorsque vous travaillez dans **Configuration de l'ordinateur** ou **Configuration utilisateur** (en fonction de ce que vous souhaitez configurer) sous l'onglet **Paramètres** dans `Category > ICA / Printing`, sélectionnez **Créer automatiquement une imprimante universelle PDF** et définissez-la sur `Enabled`.
   - Si vous souhaitez que les utilisateurs connectés soient administrateurs de leur bureau, ajoutez le groupe **Utilisateurs interactifs** au groupe d'administrateurs intégré.

6. Lorsque vous avez terminé, enregistrez l'image.

7. Mettez à jour le catalogue existant ou créez un nouveau catalogue à l'aide de la nouvelle image.

Définir des stratégies de groupe pour les machines jointes à un domaine

1. Assurez-vous que la fonctionnalité de gestion des stratégies de groupe est installée.

   - Sur une machine Windows à sessions multiples, ajoutez la fonctionnalité de gestion des stratégies de groupe à l'aide de l'outil Windows pour ajouter des rôles et des fonctionnalités (tels que **Ajouter des rôles et fonctionnalités**).
   - Sur une machine Windows à session unique, installez les outils d'administration du serveur distant pour le système d'exploitation approprié. (Cette installation nécessite un compte administrateur de domaine.) Après cette installation, la console de gestion des stratégies de groupe est disponible dans le menu **Démarrer**.

2. Téléchargez et installez le package de gestion des stratégies de groupe Citrix à partir de la page de téléchargement Citrix, puis configurez les paramètres de stratégie si nécessaire. Suivez la

procédure décrite dans Définir des stratégies de groupe pour les machines non jointes à un domaine, étape 2 jusqu'à la fin.

Consultez les articles Référence des paramètres de stratégie pour en savoir plus sur ce qui est disponible. Toutes les fonctionnalités de stratégie sont disponibles à partir de l'interface Configuration complète de Citrix DaaS.

Actions d'emplacement des ressources

Citrix crée automatiquement un emplacement des ressources et deux Cloud Connectors lorsque vous créez le premier catalogue de publication de bureaux et d'applications. Vous pouvez spécifier certaines informations liées à l'emplacement des ressources lorsque vous créez un catalogue. Voir Paramètres d'emplacement des ressources lors de la création d'un catalogue.

Pour Remote PC Access, vous créez l'emplacement des ressources et les Cloud Connectors.

Cette section décrit les actions disponibles après la création d'un emplacement des ressources.

1. Dans **Gérer > Déploiement rapide**, développez **Abonnements Cloud** sur la droite.
2. Sélectionnez l'abonnement.
    - L'onglet **Détails** affiche le nombre et le nom des catalogues et des images de l'abonnement. Il indique également le nombre de machines pouvant fournir des bureaux ou des applications. Ce nombre ne tient pas compte des machines utilisées à d'autres fins, telles que les images, les Cloud Connectors ou les serveurs de licences RDS.
    - L'onglet **Emplacements des ressources** répertorie chaque emplacement des ressources. Chaque entrée d'emplacement des ressources inclut le statut et l'adresse de chaque Cloud Connector dans l'emplacement des ressources.

Le menu des points de suspension de l'entrée d'un emplacement des ressources contient les actions suivantes.

Exécuter vérification de l'intégrité

La sélection de **Exécuter vérification de l'intégrité** démarre immédiatement le contrôle de connectivité. Si la vérification échoue, l'état du Cloud Connector est inconnu, car il ne communique pas avec Citrix Cloud. Essayez de redémarrer le Cloud Connector.

Redémarrer des connecteurs

Citrix recommande de ne redémarrer qu'un seul Cloud Connector à la fois. Le redémarrage met Cloud Connector hors ligne et perturbe l'accès des utilisateurs et la connectivité de la machine.

Cochez la case correspondant au Cloud Connector que vous souhaitez redémarrer. Sélectionnez **Redémarrer**.

Ajouter des connecteurs

L'ajout d'un Cloud Connector prend généralement 20 minutes.

Fournissez les informations suivantes :

- le nombre de Cloud Connectors à ajouter ;
- les informations d'identification du compte de service de domaine, qui permettent de joindre les machines Cloud Connector au domaine ;
- les performances de la machine ;
- le groupe de ressources Azure. La valeur par défaut est le dernier groupe de ressources utilisé par l'emplacement de ressources ;
- l'unité d'organisation. La valeur par défaut est la dernière unité d'organisation utilisée par l'emplacement de ressources ;
- si votre réseau a besoin d'un serveur proxy pour la connectivité Internet. Si vous indiquez **Oui**, précisez le nom de domaine complet ou l'adresse IP du serveur proxy, ainsi que le numéro de port.

Lorsque vous avez terminé, sélectionnez **Ajouter des connecteurs**.

Supprimer des connecteurs

Si un Cloud Connector ne peut pas communiquer avec Citrix Cloud et qu'un redémarrage ne résout pas le problème, le support Citrix peut recommander de supprimer ce Cloud Connector.

Cochez la case correspondant au Cloud Connector que vous souhaitez supprimer. Sélectionnez ensuite **Supprimer**. Lorsque vous y êtes invité, confirmez la suppression.

Vous pouvez également supprimer un Cloud Connector disponible. Toutefois, si la suppression de ce Cloud Connector entraînait la mise à disposition de moins de deux Cloud Connector dans l'emplacement des ressources, vous ne seriez pas autorisé à supprimer le Cloud Connector sélectionné.

Sélectionner l'heure de mise à jour

Citrix fournit automatiquement des mises à jour logicielles pour les Cloud Connectors. Lors d'une mise à jour, un Cloud Connector est mis hors ligne et mis à jour, tandis que les autres Cloud Connectors restent en service. Lorsque la première mise à jour est terminée, un autre Cloud Connector est mis hors ligne et mis à jour. Ce processus se poursuit jusqu'à ce que tous les Cloud Connectors de l'

emplacement de ressources soient mis à jour. Le meilleur moment pour démarrer les mises à jour est généralement en dehors de vos heures de bureau habituelles.

Choisissez l'heure de début des mises à jour ou indiquez que vous souhaitez que les mises à jour démarrent lorsqu'une mise à jour est disponible. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

Renommer

Saisissez le nouveau nom de l'emplacement des ressources. Sélectionnez **Enregistrer**.

Configurer la connectivité

Indiquez si les utilisateurs peuvent accéder aux bureaux et aux applications via Citrix Gateway Service, ou uniquement depuis le réseau de votre entreprise.

Profile Management

Profile Management veille à ce que les paramètres personnels soient appliqués à leurs applications virtuelles, indépendamment de l'emplacement de la machine utilisateur.

La configuration de Profile Management est facultative.

Vous pouvez activer Profile Management avec le service d'optimisation de profil. Ce service constitue un moyen fiable de gérer ces paramètres sous Windows. La gestion des profils assure une expérience cohérente grâce à un profil unique qui suit l'utilisateur. Il se consolide automatiquement et optimise les profils utilisateur afin de minimiser les besoins en gestion et en stockage. Le service d'optimisation de profil ne nécessite pas beaucoup d'administration, de support et d'infrastructure. En outre, l'optimisation des profils offre aux utilisateurs une meilleure expérience en matière de connexion et de déconnexion.

Le service d'optimisation des profils nécessite un partage de fichiers dans lequel tous les paramètres personnels sont conservés. Vous gérez les serveurs de fichiers. Nous recommandons de configurer la connectivité réseau pour autoriser l'accès à ces serveurs de fichiers. Vous devez spécifier le partage de fichiers en tant que chemin UNC. Le chemin peut contenir des variables d'environnement système, des attributs d'utilisateur Active Directory ou des variables Profile Management. Pour en savoir plus sur le format de la chaîne de texte UNC, voir Pour spécifier le chemin d'accès au magasin de l'utilisateur.

Lorsque vous activez Profile Management, vous pouvez envisager d'optimiser davantage le profil de l'utilisateur en configurant la redirection de dossiers afin de minimiser les effets de la taille de ce dernier. L'application de la redirection de dossiers vient compléter la solution Profile Management. Pour plus d'informations, consultez Redirection de dossiers Microsoft).

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

Ce service 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). La machine Windows sur laquelle le VDA Citrix est installé 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 Citrix DaaS 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 sur l'une des VM disponibles. La VM doit toujours être disponible. Les charges de travail Citrix DaaS 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.

Utilisation de l'engagement de consommation

> **Remarque :**
>
> Cette fonctionnalité est disponible dans la Tech Preview.

Dans **Gérer > Déploiement rapide**, sélectionnez la carte **Général**. La valeur de **consommation** indique la consommation utilisée au cours du mois civil en cours. Cette valeur inclut les engagements mensuels et annuels.

Lorsque vous sélectionnez **Général**, l'onglet **Notifications** inclut :

- la consommation totale utilisée pour le mois (mensuelle et annuelle) ;

- le nombre d'unités d'engagement de consommation mensuel ;
- le pourcentage de l'engagement de consommation annuel.

Les valeurs et les barres de progression peuvent vous alerter en cas de dépassements d'utilisation potentiels ou réels.

Les données réelles peuvent prendre 24 heures avant d'apparaître. Les données d'utilisation et de facturation sont considérées comme définitives 72 heures après la fin d'un mois civil.

Pour plus d'informations sur l'utilisation, consultez la section Surveiller les licences et l'utilisation active.

Vous pouvez éventuellement demander que des notifications apparaissent dans le tableau de bord **Gérer > Déploiement rapide** lorsque l'utilisation de la consommation (pour les engagements mensuels, annuels ou les deux) atteint un niveau spécifié. Par défaut, les notifications sont désactivées.

1. Dans l'onglet **Notifications**, sélectionnez **Modifier les préférences de notification**.
2. Pour activer les notifications, cliquez sur le curseur pour que la coche apparaisse.
3. Saisissez une valeur. Répétez l'opération pour l'autre type de consommation, si nécessaire.
4. Sélectionnez **Enregistrer**.

Pour désactiver les notifications, cliquez sur le curseur afin que la coche n'apparaisse plus, puis sélectionnez **Enregistrer**.

Surveiller l'utilisation des licences Citrix

Pour afficher les informations d'utilisation de vos licences Citrix, suivez les instructions de la section Surveiller les licences et l'utilisation active. Vous pouvez consulter les éléments suivants :

- Résumé de l'option Système de licences
- Rapports d'utilisation
- Tendances d'utilisation et activité des licences
- Utilisateurs sous licence

Vous pouvez également libérer des licences.

Équilibrage de charge

L'équilibrage de charge s'applique aux machines à sessions multiples, et non aux machines à session unique.

> **Important :**
>
> La modification de la méthode d'équilibrage de charge affecte tous les catalogues de votre dé-

> ploiement. Cela inclut tous les catalogues créés à l'aide de n'importe quel type d'hôte pris en charge, basé sur le Cloud et local, quelle que soit l'interface utilisée pour les créer (telle que Déploiement complet ou Déploiement rapide).
>
> Assurez-vous que les limites de session maximales sont configurées pour tous les catalogues avant de continuer.
>
> - Dans Déploiement rapide, ce paramètre se trouve dans l'onglet **Détails** de chaque catalogue.
> - Dans Configuration complète, reportez-vous à la section Équilibrer la charge des machines.

L'équilibrage de charge mesure la charge de la machine et détermine la machine à sessions multiples à sélectionner pour une session utilisateur entrante dans les conditions actuelles. Cette sélection est basée sur la méthode d'équilibrage de charge configurée.

Vous pouvez configurer l'une des deux méthodes d'équilibrage de charge : horizontale ou verticale. La méthode s'applique à tous les catalogues à sessions multiples (et donc à toutes les machines à sessions multiples) de votre déploiement Citrix DaaS.

- **Équilibrage de charge horizontal :** une session utilisateur entrante est attribuée à la machine sous tension la moins chargée disponible.

  Exemple simple : deux machines sont configurées pour 10 sessions chacune. La première machine gère cinq sessions simultanées. La deuxième machine en gère cinq.

  L'équilibrage de charge horizontal offre des performances utilisateur élevées, mais il peut augmenter les coûts à mesure que davantage de machines sont mises sous tension et utilisées.

  Cette méthode est activée par défaut.

- **Équilibrage de charge vertical :** une session utilisateur entrante est attribuée à la machine sous tension avec l'indice de charge le plus élevé. Citrix DaaS calcule puis attribue un indice de charge à chaque machine à sessions multiples. Le calcul prend en compte des facteurs tels que l'unité centrale, la mémoire et la concurrence.

  Cette méthode sature les machines existantes avant de passer à de nouvelles machines. Lorsque les utilisateurs se déconnectent et libèrent de la capacité sur les machines existantes, une nouvelle charge est attribuée à ces machines.

  Exemple simple : 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.

  Avec l'équilibrage de charge vertical, les sessions maximisent la capacité de la machine sous tension, ce qui peut réduire les coûts de la machine.

Pour configurer la méthode d'équilibrage de charge :

1. Dans **Gérer > Déploiement rapide**, développez **Général** sur la droite.
2. Sous **Paramètres généraux**, sélectionnez **Afficher tout**.
3. Sur la page **Paramètres généraux**, sous **Équilibrage de charge de catalogues multi-session**, choisissez la méthode d'équilibrage de charge.
4. Sélectionnez **Confirmer**.

Créer un catalogue dans un réseau utilisant un serveur proxy

Suivez cette procédure si votre réseau nécessite un serveur proxy pour la connectivité Internet et que vous utilisez votre propre abonnement Azure. (L'utilisation d'un abonnement Azure géré par Citrix avec un réseau nécessitant un serveur proxy n'est pas prise en charge.)

1. Dans **Gérer > Déploiement rapide**, commencez le processus de création de catalogue en fournissant les informations requises, puis sélectionnez **Créer un catalogue** en bas de la page.
2. La création du catalogue échoue en raison de l'exigence de proxy. Toutefois, un emplacement de ressources est créé. Le nom de cet emplacement de ressources commence par « DAS », sauf si vous avez fourni un nom d'emplacement de ressources lors de la création du catalogue. Sur le tableau de bord **Gérer > Déploiement rapide**, développez **Abonnements Cloud** sur la droite. Dans l'onglet **Emplacements de ressources**, vérifiez si le nouvel emplacement des ressources créé contient des Cloud Connectors. Si c'est le cas, supprimez-les.
3. Dans Azure, créez deux machines virtuelles (voir Configuration système requise pour Cloud Connector). Joignez ces machines au domaine.
4. À partir de la console Citrix Cloud, installez un Cloud Connector sur chaque machine virtuelle. Assurez-vous que les Cloud Connectors se trouvent dans le même emplacement des ressources que celui créé précédemment. Suivez les instructions décrites dans la section :
   - Configuration du pare-feu et du proxy d'un Cloud Connector
   - Configuration requise pour le système et la connectivité
5. Dans **Gérer > Déploiement rapide**, répétez le processus de création du catalogue. Lorsque le catalogue est créé, il utilise l'emplacement des ressources et les Cloud Connectors que vous avez créés lors des étapes précédentes.

Obtenir de l'aide

- Consultez la section Dépannage.
- Si vous avez besoin d'aide supplémentaire pour Citrix DaaS, ouvrez un ticket en suivant les instructions de la section Comment obtenir de l'aide.

Créer des groupes de mise à disposition

June 12, 2024

Introduction

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 peut également indiquer les utilisateurs autorisés à utiliser ces machines ainsi que les applications et bureaux auxquels les utilisateurs peuvent accéder.

La création d'un groupe de mise à disposition est la prochaine étape de configuration de votre déploiement après 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 pas lors de sa création.

Avant de créer un groupe de mise à disposition :

- 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 ou aux autres ressources qui hébergent vos machines.
- Assurez-vous que vous avez créé un catalogue de machines contenant des machines virtuelles ou physiques.

Pour lancer l'assistant de création de groupe de mise à disposition :

1. Connectez-vous à Citrix Cloud. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**.
2. Sélectionnez **Gérer**.
3. S'il s'agit du premier groupe de mise à disposition que vous créez, la console vous indique quelle option choisir (telle que « Configurez des groupes de mise à disposition à afficher en tant que services »). L'assistant de création de groupe de mise à disposition s'ouvre et vous guide tout au long du processus.
4. Si vous avez déjà créé un groupe de mise à disposition et que vous souhaitez en créer un autre, procédez comme suit :

    a) Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.

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 de groupe.
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.

L'assistant vous guide à travers les pages décrites dans les sections suivantes. Les pages de l'assistant qui s'affichent peuvent varier selon les sélections que vous effectuez.

Étape 1. Machines

Sélectionnez un catalogue de machines et sélectionnez le nombre de machines que vous souhaitez utiliser dans ce catalogue.

À savoir :

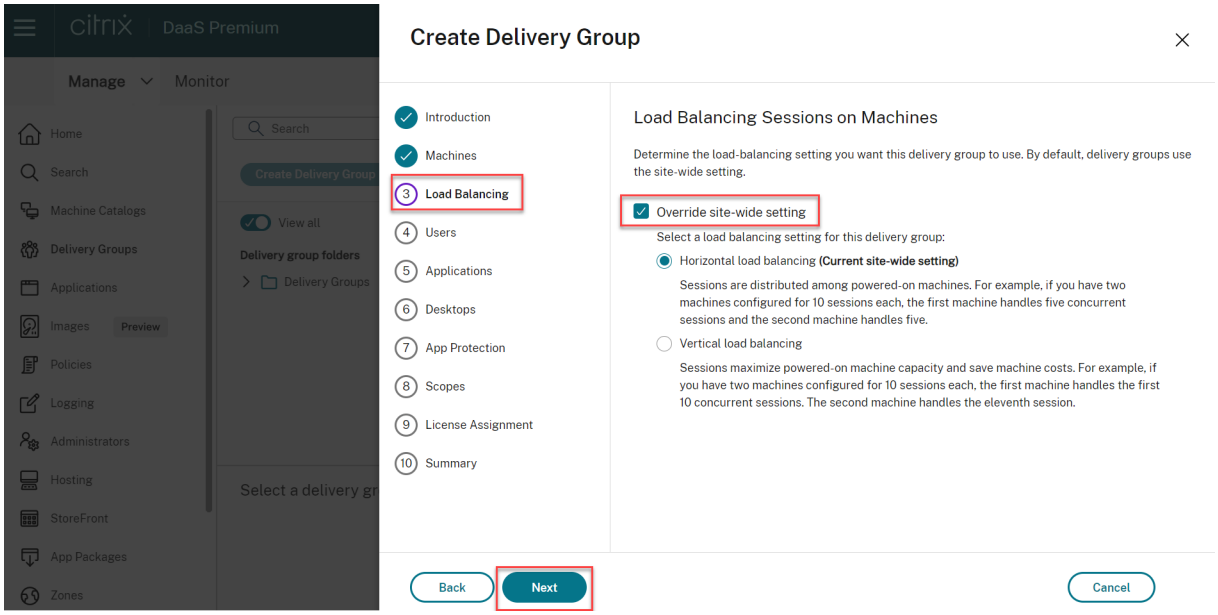
- Au moins une machine doit rester non utilisée dans un catalogue sélectionné.
- Un catalogue peut être spécifié dans plusieurs groupes de mise à disposition. Toutefois, une machine ne peut être utilisée que dans un seul groupe de mise à disposition.
- Un groupe de mise à disposition peut utiliser des machines de plusieurs catalogues. Cependant ces catalogues doivent contenir les mêmes types de machines (OS multisession, OS monosession 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.
- Un groupe de mise à disposition MCS peut uniquement ajouter un catalogue de type MCS.
- Citrix vous recommande d'installer ou de mettre à niveau tous les VDA vers la dernière version, et d'effectuer une **modification du niveau fonctionnel** pour les catalogues de machines et les groupes de mise à disposition le cas échéant. 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 sera compatible avec la version de VDA la plus ancienne Par exemple, si l'une des machines que vous sélectionnez dispose d'un VDA version 7.1 et que d'autres machines ont une version plus récente, toutes les machines du groupe peuvent uniquement utiliser les fonctionnalités prises en charge dans le VDA 7.1. Cela signifie que certaines fonctionnalités qui nécessitent des versions de VDA plus récentes risquent de ne pas être disponibles dans ce groupe de mise à disposition.
- 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
- Vérification associée à AppDisk

Étape 2. Équilibrage de charge (Technical Preview)

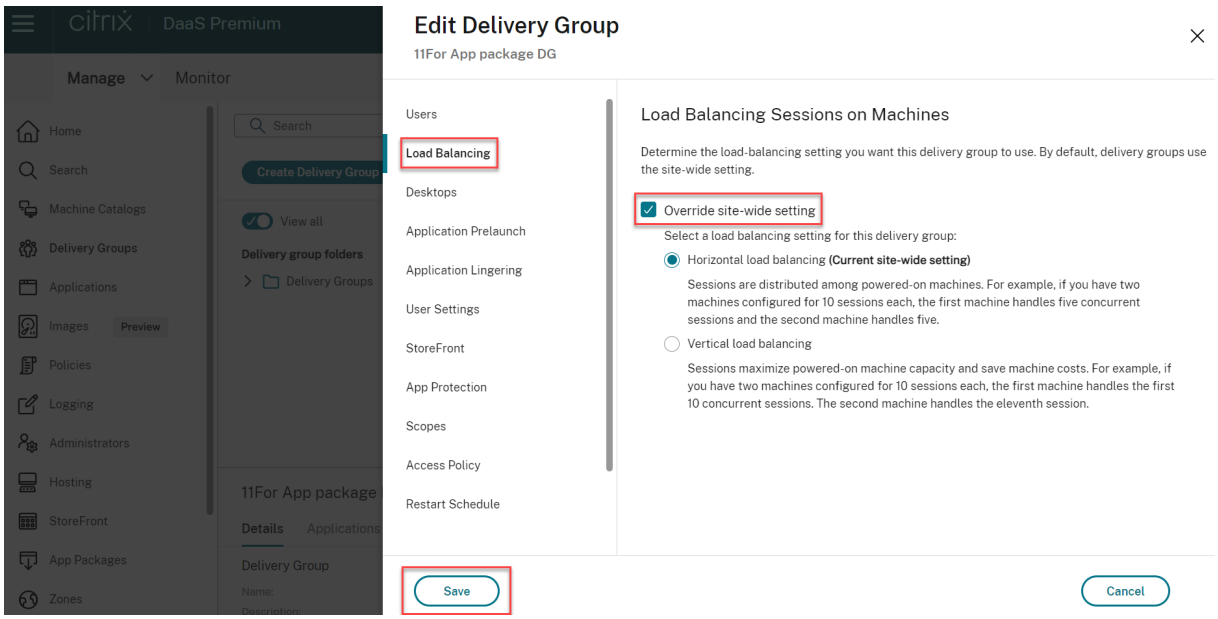
Pour configurer les paramètres d'équilibrage de charge lors de la création d'un groupe de mise à disposition :

1. Connectez-vous à DaaS Premium.
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 **Équilibrage de charge vertical** selon vos besoins et cliquez sur **Suivant**.

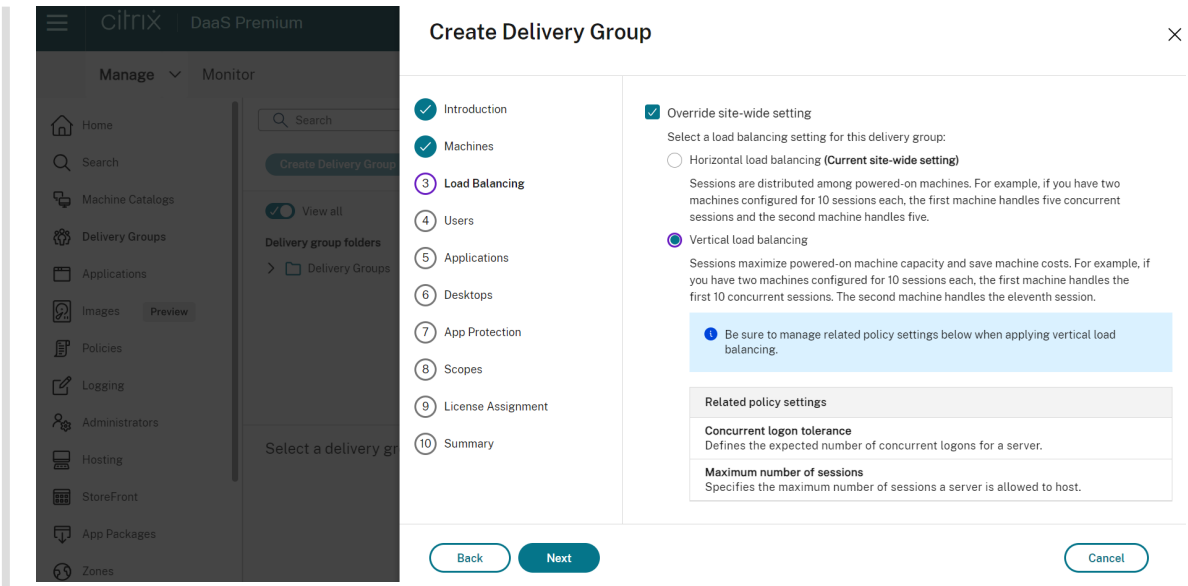


Pour configurer les paramètres d'équilibrage de charge lors de la modification d'un groupe de mise à disposition existant :

1. Connectez-vous à DaaS Premium.
2. Dans le menu de navigation 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 plus d'informations sur l'équilibrage de charge au niveau du site et au niveau du groupe de mise à disposition, voir 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 monosession statiques (attribuées). 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. AppDisks

Ignorez cette page. Sélectionnez **Suivant**.

Étape 5. 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 sont spécifiées lorsque vous créez ou modifiez les informations suivantes :

- La liste d'accès utilisateur d'un déploiement, qui n'est pas configurée dans cette console. 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.
- Groupes de mise à disposition.
- Applications.

> **Remarque :**
>
> Lorsque vous spécifiez une liste d'utilisateurs, vous pouvez sélectionner des comptes utilisateur parmi les fournisseurs d'identité suivants auxquels votre compte Citrix Cloud est connecté : Active Directory, Azure Active Directory (Microsoft Entra ID) ou Okta.

La liste des utilisateurs qui peuvent accéder à une application est formée par l'intersection des listes utilisateur ci-dessus.

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 multi-session 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 AnonXYZ, 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 ?	Activer la case à cocher « 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

Restreindre l'accès aux utilisateurs ou groupes

Vous pouvez également restreindre l'utilisation d'un groupe de mise à disposition en ajoutant des utilisateurs ou des groupes d'utilisateurs à la **liste verte**. Seuls les utilisateurs figurant sur la **liste verte** peuvent accéder aux applications et aux bureaux du groupe de mise à disposition. Vous pouvez également ajouter des utilisateurs et des groupes d'utilisateurs à une liste rouge en cliquant sur **Ajouter une liste rouge**, ce qui empêche les utilisateurs d'utiliser les applications et les bureaux du groupe de mise à disposition sélectionné. Une liste rouge n'a de sens que lorsqu'elle est utilisée pour bloquer des utilisateurs figurant dans la liste verte.

Étape 6. Applications

À savoir :

- Vous pouvez ajouter des applications packagées aux groupes de mise à disposition de type *statique monosession* et *Remote PC Access*. Les packages contenant ces applications sont automatiquement montés chaque fois que les utilisateurs se connectent à leur bureau ou à des PC distants.
- 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 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 Applications.
- Si vous essayez d'ajouter une application et qu'une application avec le même nom existe déjà 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 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). Sinon, des noms en double s'affichent dans l'application Citrix Workspace.

Sélectionnez le menu **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 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 sélectionnez **OK**.
- **Manuellement définies :** applications qui se trouvent dans le déploiement 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 saisi ces informations, sélectionnez **OK**.
- **Existantes :** applications déjà ajoutées au site, peut-être dans un autre groupe de mise à disposition. Lorsque vous sélectionnez cette source, une nouvelle page s'ouvre avec une liste d'applications découvertes ; sélectionnez les applications que vous souhaitez ajouter, puis sélectionnez **OK**.
- **Packages d'applications :** applications dans App-V, MSIX, packagées vis l'attachement d'application MSIX ou des packages d'applications FlexApp. Lorsque vous sélectionnez cette source, la page **Ajouter des applications à partir de packages** s'ouvre. Sélectionnez une source de package d'applications, puis les applications que vous souhaitez ajouter dans la liste qui s'affiche, puis sélectionnez **OK**

  > **Remarque :**
  >
  > Pour publier des applications MSIX ou packagées via l'attachement d'application MSIX, le niveau fonctionnel du groupe de mise à disposition doit être 2106 ou supérieur. Pour

> les applications FlexApp, le niveau fonctionnel doit être 2206 ou supérieur. Lorsqu'une exigence de niveau fonctionnel n'est pas satisfaite, les options correspondantes de la liste déroulante des **sources de package d'application** sont grisées.

- **Groupe d'applications :** groupes d'applications qui existent dans le déploiement.

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 déploiement. Ou une application peut ne pas être compatible avec les types de session pris en charge sur des machines du catalogue de machines sélectionné.

Étape 7. App Protection

Les informations suivantes complètent l'article sur la protection des applications dans la documentation de Citrix Virtual Apps and Desktops. Pour utiliser la protection des applications dans un déploiement Citrix DaaS, suivez les instructions générales de cet article, et plus particulièrement les informations suivantes.

- Vous devez disposer d'un abonnement Citrix Cloud valide et de droits de protection des applications valides. Pour acheter la fonctionnalité de protection des applications, vous pouvez contacter votre représentant commercial Citrix.
- La protection des applications 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 protection des applications est active lorsqu'une fenêtre protégée n'est pas réduite.
  - Sur Linux, l'intégralité de la capture est vide. La protection des applications est active, qu'une fenêtre protégée soit réduite ou non.

Étape 8. Bureaux (ou règles d'attribution de bureau)

Le titre de cette page dépend du catalogue de machines que vous avez choisi précédemment dans l'assistant :

- 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 **Règles d'attribution de 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 **Applications**.

Sélectionnez **Add**. 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 le menu.
- À l'aide des boutons radio, vous pouvez :
  - **Autoriser tous les utilisateurs ayant accès à ce groupe de mise à disposition à utiliser un bureau.** Tous les utilisateurs du groupe de mise à disposition peuvent lancer un bureau (pour les groupes avec machines regroupées) ou se voir attribuer une machine lorsqu'ils lancent le bureau (pour les groupes avec machines attribuées).
  - **Limiter l'utilisation de bureau** en ajoutant des utilisateurs et des groupes d'utilisateurs à la **liste verte**. Seuls les utilisateurs figurant sur la **liste verte** peuvent accéder à un bureau. Vous pouvez également ajouter des utilisateurs et des groupes d'utilisateurs à une liste rouge en cliquant sur **Ajouter une liste rouge**, ce qui empêche les utilisateurs d'utiliser les bureaux du groupe de mise à disposition sélectionné. Une liste rouge n'a de sens que lorsqu'elle est utilisée pour bloquer des utilisateurs figurant dans la liste verte.
- 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, sélectionnez **OK**.

Étape 9 –Attribution de licence

Déterminez quelle licence vous souhaitez que le groupe de mise à disposition utilise. Par défaut, le groupe de mise à disposition utilise la licence de site. Pour plus d'informations, consultez la section Licences multitypes.

Étape 10. Paramètre Cache d'hôte local

Ce paramètre n'est visible que pour les groupes de mise à disposition contenant des machines mono-session regroupées à alimentation gérée.

Par défaut, ces machines ne sont pas disponibles en mode de cache d'hôte local (LHC, Local Host Cache) en raison des risques d'exposition des données. Pour modifier le comportement par défaut et les rendre disponibles pour les nouvelles connexions utilisateur en mode LHC, sélectionnez **Garder les ressources disponibles**.

Vous pouvez également modifier le comportement par défaut à l'aide des commandes PowerShell. Pour plus d'informations, consultez la section Prise en charge des applications et des bureaux.

> **Important :**
>
> L'activation de l'accès à des machines monosession regroupées à alimentation gérée peut entraîner la présence de données et de modifications issues de sessions utilisateur précédentes dans les sessions suivantes.

Étape 11. Résumé

Entrez un nom pour le groupe de mise à disposition. Vous pouvez également entrer une description (facultatif), qui s'affiche dans l'application Workspace et dans l'interface de gestion Configuration complète.

Consultez les informations récapitulatives, puis sélectionnez **Terminer**. Si vous n'avez pas sélectionné d'applications ou spécifié de bureaux à mettre à disposition, vous êtes invité à indiquer si vous voulez continuer.

Informations supplémentaires

- Gérer des groupes de mise à disposition
- Applications

Gérer des groupes de mise à disposition

June 12, 2024

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 procédures sont organisées par catégories : 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. Par conséquent, 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
- Modifier la licence d'un groupe de mise à disposition
- Organiser les groupes de mise à disposition sous forme de dossiers
- Gérer la protection des applications

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.

Colonne	Description
Nombre alloué	Nombre de machines du catalogue attribuées à un groupe de mise à disposition.
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 remplacer un type **applications** par le type **bureaux**, supprimez toutes les applications du groupe.

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **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. 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.

Modifier les adresses de StoreFront

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier** dans la barre d'actions.
3. Sur la page **StoreFront**, indiquez si vous allez spécifier une adresse de serveur StoreFront ultérieurement (**manuellement**) ou sélectionnez **Ajouter nouveau** pour spécifier les serveurs StoreFront que vous souhaitez utiliser (**automatiquement**).
4. 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.

Vous pouvez également spécifier les adresses du serveur StoreFront en sélectionnant **StoreFront** dans le volet de gauche de la console.

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 Citrix DaaS. Ce processus informe la console de la nature des éléments nécessitant une modification dans le groupe de mise à disposition.
- Si vous devez continuer à utiliser des versions antérieures du VDA, il se peut que des fonctionnalités plus récentes ne soient pas disponibles. Pour de plus amples informations, consultez la documentation de mise à niveau.

Pour modifier le niveau fonctionnel d'un groupe de mise à disposition :

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le niveau fonctionnel** 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 à un utilisateur, 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 à quel groupe de mise à disposition cette machine est attribuée 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. Cette association signifie que 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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe Remote PC Access.
3. Dans la section **Détails**, sélectionnez l'onglet **Catalogues de machines**, puis sélectionnez un catalogue Remote PC Access.
4. Pour ajouter ou restaurer une association, sélectionnez **Ajouter des bureaux**. Pour supprimer une association, sélectionnez **Supprimer l'association**.

Modifier la licence d'un groupe de mise à disposition

Pour modifier le droit de licence d'un groupe de mise à disposition, procédez comme suit :

1. Sélectionnez **Groupes de mise à disposition** dans le volet de navigation.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **Attribution de licences**, sélectionnez la licence que vous souhaitez que le groupe utilise.
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.

Pour plus d'informations sur les droits au niveau du groupe de mise à disposition, voir Licences multitypes.

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 de **Configuration complète** (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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet 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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet 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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet 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

Action	Autorisations requises
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 la protection des applications

Les informations suivantes complètent l'article sur la protection des applications dans la documentation de Citrix Virtual Apps and Desktops. Pour utiliser la protection des applications dans un déploiement Citrix DaaS, suivez les instructions générales de cet article, et plus particulièrement les informations suivantes.

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet 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**.

- Vous devez disposer d'un abonnement Citrix Cloud valide et de droits de protection des applications valides. Pour acheter la fonctionnalité de protection des applications, vous pouvez contacter votre représentant commercial Citrix.
- La protection des applications 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 protection des applications est active lorsqu'une fenêtre protégée n'est pas réduite.
  - Sur Linux, l'intégralité de la capture est vide. La protection des applications est active, qu'une fenêtre protégée soit réduite ou non.

Utilisateurs

> **Remarque :**
>
> L'option **Laissez Citrix Cloud se charger de la gestion des utilisateurs** a été supprimée. Pour gérer les attributions des utilisateurs pour les groupes de mise à disposition existants définis sur **Laisser la gestion des utilisateurs à Citrix Cloud**, vous avez deux options : Bibliothèque Citrix Cloud ou Configuration complète. Pour plus d'informations sur l'approche Configuration

> complète, consultez la section Gérer les attributions d'utilisateurs pour les groupes de mise à disposition gérés par la bibliothèque Citrix Cloud.

Cette rubrique couvre les sections suivantes :

- Modifier les paramètres utilisateur
- Ajouter ou supprimer des utilisateurs
- Gérer les attributions d'utilisateurs pour les groupes de mise à disposition gérés par la bibliothèque Citrix Cloud

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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier** dans la barre d'actions.
3. Sur la page **Paramètres utilisateur**, modifiez les paramètres dans le tableau suivant.
4. 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.

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.
Nbre maximal de bureaux par utilisateur	Le nombre de bureaux qu'un utilisateur peut avoir.

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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** dans la barre d'actions.
3. Sur la page **Utilisateurs** :
   - Pour ajouter des utilisateurs, sélectionnez **Ajouter**, puis spécifiez les utilisateurs que vous souhaitez ajouter.
   - Pour supprimer des utilisateurs, sélectionnez un ou plusieurs utilisateurs, puis sélectionnez **Supprimer**.
   - Cochez ou décochez la case pour autoriser l'accès aux utilisateurs non authentifiés.
4. 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.

Gérer les attributions d'utilisateurs Pour gérer les attributions d'utilisateurs :

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition**.
2. Sélectionnez un groupe, puis sélectionnez **Modifier** dans la barre d'actions.

3. Sur la page **Allocation de machines**, ajoutez ou supprimez des utilisateurs. Pour ajouter des utilisateurs, localisez-les ou entrez une liste de noms d'utilisateur séparés par des points-virgules.

Lorsque vous entrez des noms d'utilisateur, tenez compte des points suivants :

- Si les utilisateurs se trouvent dans Active Directory, entrez directement les noms. Si ce n'est pas le cas, entrez les noms au format suivant : `<identity provider>:<user name>`. Exemple : `AzureAD:username`.

Gérer les attributions d'utilisateurs pour les groupes de mise à disposition gérés par la bibliothèque Citrix Cloud

Pour gérer les attributions d'utilisateurs pour les groupes de mise à disposition gérés par la bibliothèque Citrix Cloud, utilisez Bibliothèque Citrix Cloud ou Configuration complète.

Pour effectuer cette tâche à l'aide de la fonctionnalité Configuration complète, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe de mise à disposition géré par Citrix Cloud, puis sélectionnez **Modifier** dans la barre d'actions.
3. Pour limiter l'utilisation d'un bureau à certains utilisateurs, procédez comme suit :
    a) Sur la page **Bureaux** ou **Règles d'attribution de bureau**, sélectionnez le bureau, puis cliquez sur **Modifier**. La page **Modifier le bureau** apparaît avec l'option **Limiter l'utilisation de bureau** sélectionnée.
    b) Cliquez sur **Ajouter**, sélectionnez un ou plusieurs utilisateurs selon vos besoins, puis cliquez sur **OK**.
    c) Cliquez sur **OK**.
4. Pour limiter l'utilisation des applications de ce groupe à certains utilisateurs, cliquez sur **Règle d'attribution d'application** dans le volet de gauche et suivez les étapes similaires décrites à l'étape 3 pour ajouter des utilisateurs.

Machines

- Modifier les attributions de machines des utilisateurs
- Activer le cache d'hôte local pour les VDA regroupés à session unique
- Mettre à jour une machine
- Ajouter, modifier ou retirer une restriction de balise pour un bureau

- Supprimer une machine
- Restreindre l'accès aux ressources
- 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
- Gérer le chargement des machines
- Gérer Autoscale

Outre les fonctionnalités décrites dans cet article, reportez-vous à Autoscale pour plus d'informations sur la gestion proactive de l'alimentation des machines.

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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier** dans la barre d'actions.
3. Sur la page **Allocation de machine**, spécifiez les nouveaux utilisateurs.
4. 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.

Activer le cache d'hôte local pour les VDA monosession regroupés

Par défaut, les machines monosession regroupées à alimentation gérée ne sont pas disponibles en mode de cache d'hôte local. Vous pouvez modifier le comportement par défaut pour chaque groupe de mise à disposition. Les étapes détaillées sont les suivantes :

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.

   Dans la liste des groupes, les groupes contenant des machines monosession regroupées provisionnées par MCS ou Citrix Provisioning affichent une icône d'avertissement.

2. Sélectionnez un groupe, puis sélectionnez **Modifier** dans la barre d'actions.
3. Sur la page **Cache d'hôte local**, sélectionnez **Garder les ressources disponibles**.
4. 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.

Vous pouvez également remplacer le comportement par défaut à l'aide des commandes PowerShell. Pour plus d'informations, consultez la section Prise en charge des applications et des bureaux.

> **Important :**
>
> L'activation de l'accès à des machines monosession regroupées à alimentation gérée peut entraîner la présence de données et de modifications issues de sessions utilisateur précédentes dans les sessions suivantes.

Mettre à jour une machine dans un groupe de mise à disposition

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans la barre d'actions.
3. Sélectionnez une machine, puis sélectionnez **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 : 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 recevront

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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet 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. 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. 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.

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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans la barre d'actions.
3. Vérifiez que la machine est arrêtée.
4. Sélectionnez la machine, puis sélectionnez **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 ressources dans un groupe de mise à disposition

Toute modification que vous apportez pour restreindre l'accès aux ressources 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 :** vous pouvez créer et allouer 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 :**vous pouvez configurer des règles de stratégie d'accès pour contrôler l'accès des utilisateurs à un groupe de mise à disposition spécifique. Exemples :

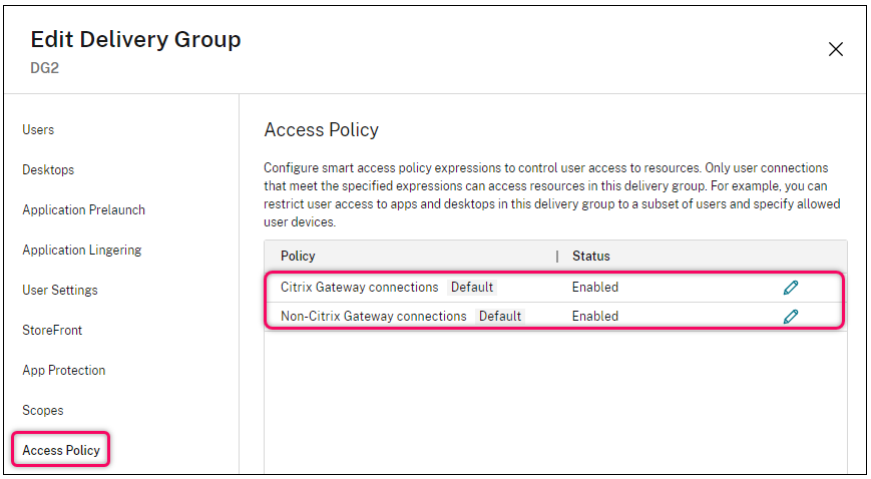
- Limiter l'accès à un sous-ensemble d'utilisateurs et indiquer les machines utilisateur autorisées.
- Limiter l'accès aux utilisateurs connectés via Workspace (plutôt que via StoreFront).
- Limiter l'accès aux utilisateurs connectés via une URL Workspace spécifique.

Cette section explique comment restreindre l'accès des utilisateurs aux groupes de mise à disposition par le biais de règles de stratégie d'accès :

- À propos des règles de stratégie d'accès
- Ajouter des règles de stratégie d'accès
- Gérer les règles de stratégie d'accès à l'aide de la fonctionnalité Configuration complète
- Ajouter et affiner des règles de stratégie avec PowerShell

À propos des règles de stratégie d'accès Vous pouvez configurer plusieurs règles de stratégie d'accès pour un groupe de mise à disposition. Les applications et les bureaux d'un groupe de mise à disposition apparaissent dans l'instance de StoreFront ou de Workspace d'un utilisateur lorsque la connexion de l'utilisateur correspond à une règle de stratégie d'accès que vous avez définie pour le groupe de mise à disposition, quel que soit l'ordre.

Chaque règle peut être activée ou désactivée individuellement. Une règle désactivée est ignorée lors de l'évaluation de la stratégie d'accès.



Dans Configuration complète, la liste des stratégies d'accès inclut les règles de stratégie SmartAccess par défaut suivantes. Vous pouvez en ajouter d'autres si nécessaire.

- **Connexions Citrix Gateway.** Cette stratégie autorise uniquement les connexions utilisateur établies via Citrix Gateway à accéder aux ressources du groupe de mise à disposition. Les connexions utilisateur établies via Workspace lorsque les fonctionnalités Posture de l'appareil ou Emplacement réseau sont activées sont également considérées comme des connexions via Citrix Gateway.

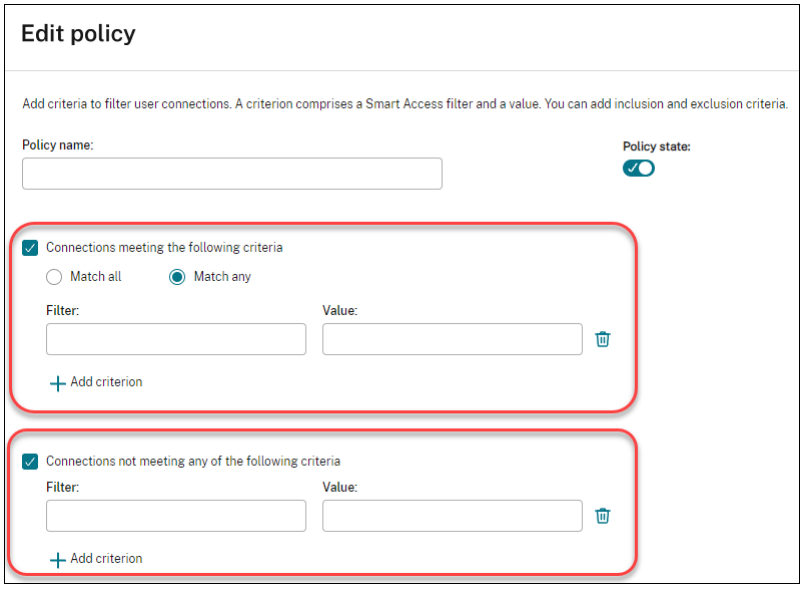
- **Connexions non-Citrix Gateway.** Cette stratégie autorise uniquement les connexions utilisateur non établies via Citrix Gateway à accéder aux ressources du groupe de mise à disposition.

> **Remarque :**
>
> - Pour éviter que les règles par défaut ne remplacent les règles nouvellement configurées, vous devez soit désactiver les règles par défaut, soit les affiner pour exclure les filtres utilisés dans la nouvelle stratégie.
> - Les stratégies par défaut ne peuvent pas être supprimées, mais elles peuvent être désactivées. Pour désactiver une stratégie, cliquez sur l'icône **Modifier**, puis redéfinissez l'**état de la stratégie** sur **Désactivé**.
> - La liste des stratégies affiche également les règles ajoutées à l'aide des commandes PowerShell. Ces stratégies peuvent être supprimées mais ne peuvent pas être modifiées dans Configuration complète.

Ajouter des règles de stratégie d'accès à l'aide de la fonctionnalité Configuration complète
Une règle de stratégie d'accès comprend un ensemble de filtres. Pour plus d'informations sur les filtres, consultez cet article. Lorsque vous ajoutez une règle de stratégie d'accès, vous ajoutez plusieurs filtres conditionnels à la règle selon les besoins.

Pour ajouter une stratégie pour un groupe de mise à disposition à l'aide de la fonctionnalité Configuration complète, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis cliquez sur **Modifier** dans la barre d'actions.
3. Sur la page **Stratégie d'accès**, cliquez sur **Ajouter**. La page **Ajouter une stratégie** apparaît.



4. Dans le champ **Nom de la stratégie**, saisissez un nom descriptif pour la stratégie. Le nom doit être unique dans votre déploiement.
5. Pour définir les critères relatifs aux connexions utilisateur autorisées, procédez comme suit :
   a) Sélectionnez **Connexions répondant aux critères suivants**.
   b) Cliquez sur **Ajouter un critère**.
   c) Dans le champ **Filtre**, saisissez le nom du filtre que vous souhaitez utiliser. Dans le champ **Valeur**, saisissez la valeur souhaitée pour le filtre. Par exemple, pour autoriser uniquement les utilisateurs connectés via Workspace (plutôt que via StoreFront) à accéder aux ressources de ce groupe de mise à disposition, saisissez `Citrix-Via-Workspace` pour **Filtre** et `True` pour **Valeur**.
   d) Pour ajouter d'autres critères, répétez les étapes b à c.
   e) Sélectionnez la relation entre les critères :
      - **Correspondance partielle**. Autorise l'accès uniquement lorsque la connexion utilisateur entrante répond à l'un des critères de filtre configurés.
      - **Correspondance exacte**. Autorise l'accès uniquement lorsque la connexion utilisateur entrante répond à tous les critères de filtre configurés.
6. Pour définir les critères relatifs aux connexions utilisateur interdites, procédez comme suit :
   a) Sélectionnez **Connexions ne répondant à aucun des critères suivants**.
   b) Cliquez sur **Ajouter un critère**.
   c) Dans le champ **Filtre**, saisissez le nom du filtre que vous souhaitez utiliser. Dans le champ **Valeur**, saisissez la valeur souhaitée pour le filtre. Par exemple, pour interdire aux utilisateurs connectés via l'URL Workspace `example.cloud.com` d'accéder aux ressources de ce groupe de mise à disposition. Saisissez `Citrix.Workspace.UsingDomain` pour **Filtre** et `example.cloud.com` pour **Valeur**.
   d) Pour ajouter d'autres critères, répétez les étapes b à c.

   > **Remarque :**
   >
   > Les connexions utilisateur répondant à l'un des critères configurés ne peuvent pas accéder aux ressources de ce groupe de mise à disposition.

7. Cliquez sur **Terminé**.

   La nouvelle stratégie s'affiche dans la liste des stratégies.
8. Passez en revue et affinez les règles de stratégie par défaut pour éviter les chevauchements involontaires avec les connexions couvertes par cette nouvelle stratégie. Pour affiner les stratégies existantes, utilisez les méthodes suivantes :

- Désactivez les règles de stratégie par défaut.
- Configurez les règles de stratégie par défaut pour exclure les filtres SmartAccess que vous avez ajoutés aux critères d'inclusion de la nouvelle stratégie. Pour plus d'informations, consultez Gérer les règles de stratégie à l'aide de la fonctionnalité Configuration complète et Ajouter et gérer des règles de stratégie d'accès à l'aide de PowerShell.

> **Important :**
>
> Comme expliqué dans À propos des règles de stratégie d'accès, lorsque la connexion d'un utilisateur correspond à une ou plusieurs règles de stratégie d'un groupe de mise à disposition, l'utilisateur accède à ses ressources. Par conséquent, après avoir créé une règle, vous devez examiner et affiner attentivement les règles existantes afin d'éviter tout chevauchement involontaire avec les connexions couvertes par la nouvelle règle.

Gérer les règles de stratégie d'accès à l'aide de la fonctionnalité Configuration complète Vous pouvez utiliser les critères d'inclusion et d'exclusion pour affiner les stratégies par défaut. Par exemple, pour limiter l'accès à un sous-ensemble de ces connexions, procédez comme suit :

1. Modifiez une stratégie par défaut.
2. Sélectionnez **Connexions répondant à l'un des critères suivants**.
3. Ajoutez, modifiez ou supprimez les expressions de stratégie SmartAccess pour les scénarios d'accès utilisateur autorisés.

Pour plus d'informations, consultez la documentation de Citrix Gateway.

Ajouter et gérer des règles de stratégie d'accès avec PowerShell Vous pouvez utiliser les applets de commande PowerShell suivants pour ajouter et gérer des règles de stratégie d'accès pour les groupes de mise à disposition :

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- Rename-BrokerAccessPolicyRule
- Remove-BrokerAccessPolicyRule

Pour plus d'informations, consultez les articles correspondants dans la documentation Citrix Developer.

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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe.
3. Pour activer le mode de maintenance pour toutes les machines dans le groupe de mise à disposition, sélectionnez **Activer le mode de maintenance** dans la barre d'actions.

   Pour activer le mode de maintenance pour une machine, sélectionnez **Afficher les machines** dans la barre d'actions. Sélectionnez une machine, puis sélectionnez **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, sélectionnez **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** et 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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans la barre d'actions.
3. Sélectionnez la machine, puis sélectionnez l'une des actions suivantes dans la barre d'actions :

   > **Remarque :**
   >
   > - Les actions suivantes s'appliquent uniquement aux machines dont l'alimentation est gérée.
   > - Certaines options peuvent ne pas être disponibles, en fonction de l'état de la machine.

   - **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.

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 (dans ce cas, les machines) 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. La durée peut être réglée sur « démarrer toutes les machines affectées en même temps » ou un intervalle nécessaire pour redémarrer toutes les machines affectées.

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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **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. 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.

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 (appliquée) 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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez le groupe contenant les machines qui seront contrôlées par le programme.
3. Sélectionnez **Afficher les machines**, puis sélectionnez les machines auxquelles vous souhaitez ajouter une balise.
4. Sélectionnez **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, sélectionnez **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. Sélectionnez **Enregistrer** dans la boîte de dialogue **Gérer les balises**.

Créer un programme de redémarrage

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier** dans la barre d'actions.
3. Sur la page **Programme de redémarrage**, sélectionnez **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 au 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 **Modifier le groupe de mise à disposition** ouverte. Ou cliquez sur **Enregistrer** pour appliquer les modifications et fermer la fenêtre.

Exécuter immédiatement un programme de redémarrage Un programme de redémarrage spécifie quand redémarrer périodiquement toutes les machines d'un groupe de mise à disposition. Vous pouvez également exécuter un programme de redémarrage immédiatement pour redémarrer les machines de ce programme.

Pour exécuter immédiatement un programme de redémarrage, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez le groupe de mise à disposition applicable, puis sélectionnez **Modifier** dans la barre d'actions.
3. Sur la page **Calendrier de redémarrage**, sélectionnez un programme que vous souhaitez exécuter, puis sélectionnez **Exécuter le programme**.

> **Remarque :**
>
> - Vous ne pouvez pas exécuter un programme immédiatement s'il est configuré avec le paramètre **Redémarrer toutes les machines après le vidage des sessions**.
> - Vous pouvez appliquer **Exécuter le programme** à un seul programme à la fois.
> - Une fois que vous avez modifié un programme, **Exécuter le programme** devient indisponible. Sélectionnez **Appliquer** pour le rendre disponible.

Modifier, supprimer, activer ou désactiver un programme de redémarrage

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier** dans la barre d'actions.
3. Sur la page **Programme de redémarrage**, cochez la case correspondant à un programme.
    - Pour modifier un programme, sélectionnez **Modifier**. Mettez à jour la configuration du programme en utilisant les instructions sous Créer un programme de redémarrage.
    - Pour activer ou désactiver un programme, sélectionnez **Modifier**. Sélectionnez ou désélectionnez la case **Activer calendrier de redémarrage**.
    - Pour supprimer un programme, sélectionnez **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. Cette action 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 3 heures du matin). Une panne de base de données de site se produit une heure avant le début d'un redémarrage programmé (2 heures du matin). La panne dure six heures (jusqu'à 8 heures du matin). Le programme de redémarrage commence lorsque la connexion entre le Delivery Controller et la base de données du site est restaurée. Les redémarrages du VDA commencent alors cinq heures après leur planification initiale. Cette action pourrait entraîner 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.

Redémarrages planifiés des machines en mode de maintenance 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 à la fois les machines qui sont en mode maintenance et les machines qui ne le sont pas.

```
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.

Gérer la charge des machines 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 actuellement indisponible lorsqu'ils lancent une session.

Vous pouvez surveiller l'index de charge dans Director (Monitor), une recherche de l'interface de gestion Configuration complète 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.

Gérer Autoscale

Par défaut, Autoscale est désactivé pour les groupes de mise à disposition. Pour gérer Autoscale pour un groupe de mise à disposition (le cas échéant), procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Gérer Autoscale** dans la barre d'actions. La fenêtre **Gérer Autoscale** s'affiche.
3. Configurez les paramètres selon vos besoins. Pour plus d'informations sur les paramètres de la fonctionnalité Autoscale, consultez la section Autoscale.
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.

Sessions

- Fermer ou déconnecter la session, ou envoyer un message aux utilisateurs
- Configurer le pré-lancement de session et la persistance de session
- Configurer l'itinérance de session
- Contrôler la reconnexion de session en cas de déconnexion d'une machine en mode de maintenance

Fermer ou déconnecter une session, ou envoyer un message aux utilisateurs d'un groupe de mise à disposition

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Afficher les machines** dans la barre d'actions.
3. Pour fermer la session d'un utilisateur, sélectionnez la session ou le bureau, puis sélectionnez **Fermer la session** dans la barre d'actions. La session se ferme et la machine devient disponible auprès des autres utilisateurs, à moins qu'elle ne soit attribuée à un utilisateur spécifique.
4. Pour déconnecter une session, sélectionnez la session ou le bureau, puis sélectionnez **Déconnecter** dans la barre d'actions. Les applications continuent à être exécutées et la machine reste attribuée à cet utilisateur. L'utilisateur peut se reconnecter à la même machine.
5. Pour envoyer un message aux utilisateurs, sélectionnez la session, la machine ou l'utilisateur, puis sélectionnez **Envoyer un message** dans la barre d'actions. Entrez le message.

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 prélancement et de persistance de session aident les utilisateurs spécifiés à accéder rapidement aux applications, en :

- Démarrant les sessions avant qu'elles ne soient demandées (pré-lancement de session)
- Gardant les sessions d'application actives après la fermeture de toutes les applications par un utilisateur (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.

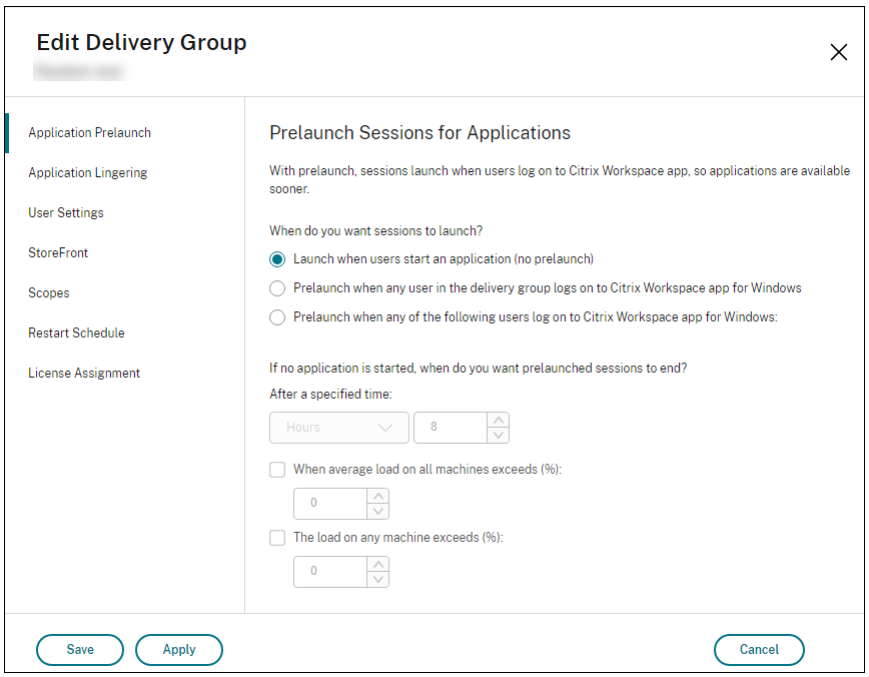
  Vous pouvez configurer deux seuils : la charge de pourcentage moyenne de tous les serveurs dans le groupe de mise à disposition et le pourcentage maximal de charge d'un serveur dans le groupe. Lorsqu'un seuil est dépassé, les sessions qui se sont trouvées dans un état de pré-lancement ou de persistance 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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier** dans la barre d'actions.
3. 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.



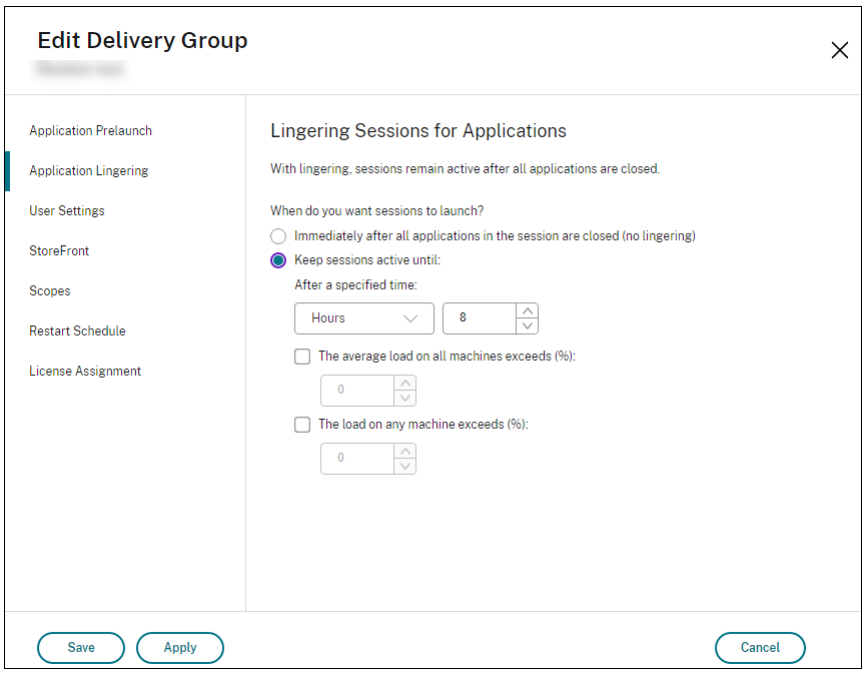
4. Une session pré-lancée est remplacée par une session régulière lorsque l'utilisateur démarre une application. Si l'utilisateur ne démarre pas une application (la session pré-lancée n'est pas utilisée), les paramètres suivants affectent la durée pour laquelle la session reste active.

    - 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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier** 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.

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 **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet 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 **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe, puis sélectionnez **Modifier le groupe de mise à disposition** 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.
5. Sélectionnez **OK** pour appliquer les modifications et fermer la fenêtre.

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 fin mai 2021, la reconnexion n'était pas autorisée pour les sessions de bureaux groupés mono-session qui s'étaient déconnectées des machines en mode de maintenance. Vous pouvez désormais 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

Applications

Affichez les applications d'un groupe de mise à disposition et ajoutez-en d'autres au besoin.

1. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche.
2. Sélectionnez un groupe. Si ce groupe contient des applications, l'option **Afficher les applications** s'affiche dans la barre d'action.
3. Sélectionnez **Afficher les applications**. Vous êtes dirigé vers le nœud **Applications** où toutes les applications disponibles dans ce groupe sont affichées.
4. Pour ajouter d'autres applications à ce groupe, accédez au nœud **Groupes de mise à disposition**, sélectionnez le groupe, puis **Ajouter des applications** dans la barre d'action.

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 devraient 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 12, 2024

Introduction

Les groupes d'applications vous permettent de gérer des collections d'applications. Vous pouvez créer des groupes d'applications pour les applications partagées entre différents groupes de mise à disposition ou 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. Les groupes de mise à disposition peuvent être associés à plus d'un groupe d'applications, et un groupe d'applications peut être associée à plus d'un groupe 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 :

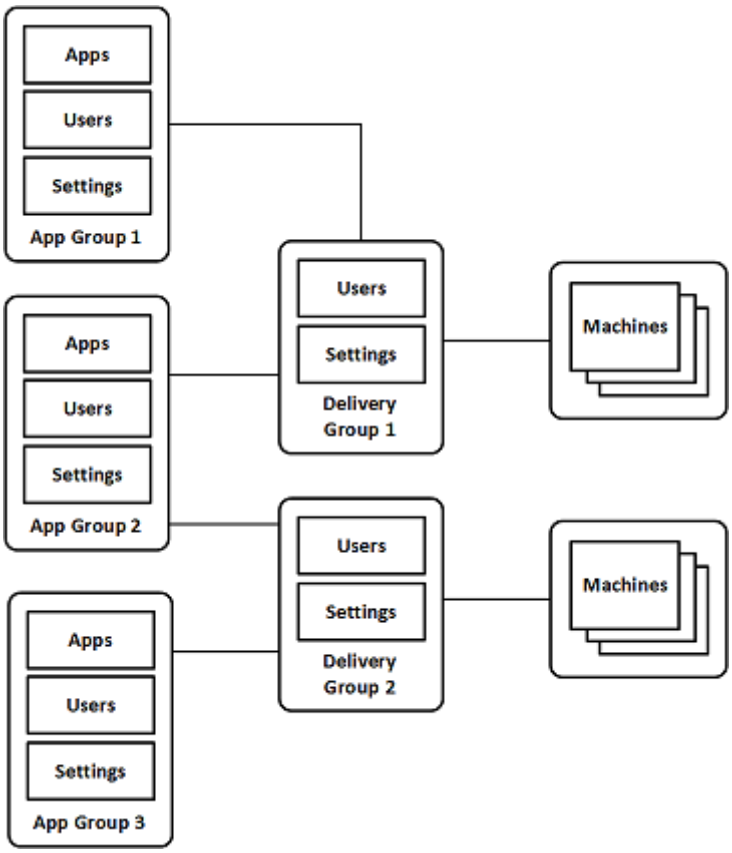
- Le regroupement logique d'applications et de leurs paramètres vous permet de gérer ces applications comme une unité unique. Par exemple, vous n'avez pas besoin d'ajouter (publier) la même application, une par une, à des groupes de mise à disposition individuels.

- 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 qui comprend des groupes d'applications :



Dans cette configuration, les applications sont ajoutées à des groupes d'applications, et non à des

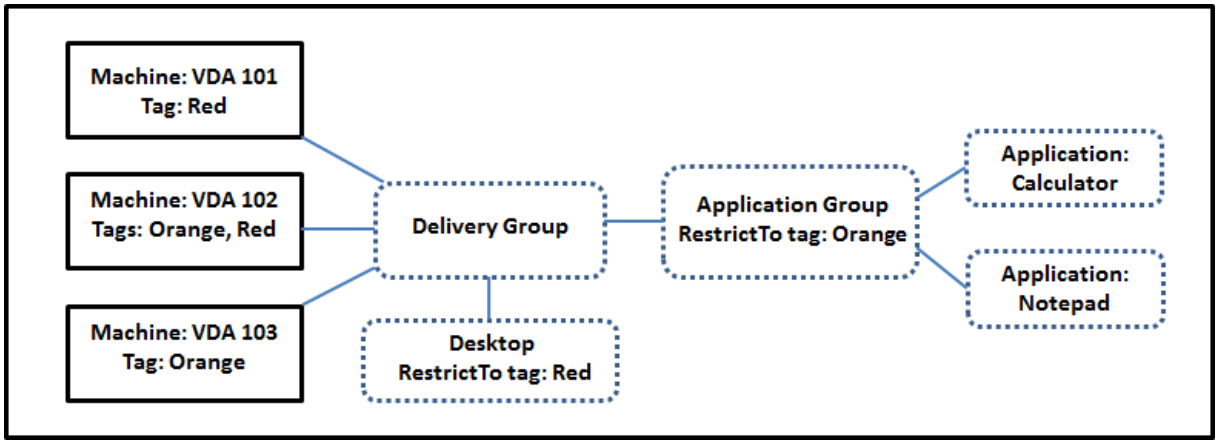
groupes de mise à disposition. Les groupes de mise à disposition spécifient les machines à utiliser. (Bien que cela ne soit pas affiché, les machines se trouvent dans des catalogues de machines).

Le groupe d'applications 1 est associé au groupe de mise à disposition 1. Les applications du groupe d'applications 1 sont accessibles par les utilisateurs spécifiés dans le groupe d'applications 1, à condition qu'ils figurent également dans la liste des utilisateurs du groupe de mise à disposition 1. Cette approche suit les recommandations selon lesquelles la liste d'utilisateurs d'un groupe d'applications doit être 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 (tels que la prise en charge des utilisateurs anonymes) 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 peut se voir attribuer une priorité dans le groupe d'applications 2, ce qui indique l'ordre dans lequel les groupes de mise à disposition vont être vérifiés lorsqu'une application est lancée. La charge des groupes de disposition ayant le même niveau de priorité est équilibrée. Les applications du groupe d'applications 2 sont accessibles par les utilisateurs spécifiés dans le groupe d'applications 2, à condition qu'ils figurent également dans les listes d'utilisateurs du groupe de mise à disposition 1 et du groupe de mise à disposition 2.

Exemple 2

Cette configuration simple utilise des restrictions de balise pour limiter les machines qui seront 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 », 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.

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. Conditions requises :

1. Mise à niveau des VDA sur les machines utilisées dans le groupe de mise à disposition
2. Passage à un niveau de fonction supérieur pour les catalogues de machines contenant ces machines
3. Passage à un niveau de fonction supérieur pour le 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 introduit la notion « d'association » d'une application avec plus d'un groupe d'applications pour opérer une distinction avec l'ajout d'une nouvelle instance de cette application à partir d'une source disponible. De même, les groupes de mise à disposition sont associés à des groupes d'applications (et vice versa), 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. Toutefois, dans certaines situations, vous souhaiterez peut-être désactiver 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 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 :**

  Vous disposez d'applications qui ne fonctionnent pas correctement avec d'autres applications qui sont installées sur la même machine, 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.

Vous 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 et peut toujours exécuter d'autres applications simultanément, mais pas dans la même session. Si l'utilisateur lance une des applications dont la version est différente (qui se trouvent dans un autre groupe d'applications), ou lance 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. Les nouvelles applications sont démarrées dans des sessions existantes sur la machine, si nécessaire, à l'aide du partage de session (à condition que ce comportement soit conforme aux restrictions décrites ici pour le 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. Si le partage de session n'est pas autorisé entre les applications de ce groupe d'applications, un utilisateur spécifié

dans le groupe démarre les applications les unes après les autres dans des sessions distinctes et il peut déplacer chaque application sur un autre écran.

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

Utilisez le processus de création d'un groupe d'applications pour créer des catégories d'applications dans l'application Citrix Workspace. Les catégories d'applications permettent de gérer des collections d'applications dans Citrix Workspace.

Pour créer un groupe d'applications :

1. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet gauche, puis sélectionnez l'onglet **Groupes d'applications**.
2. Pour organiser les groupes d'applications sous forme de dossiers, créez des dossiers dans le dossier racine **Groupes d'applications**.
3. 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.
4. 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 de bureau ou de serveur 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 de création de groupe 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 seront 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 quiconque peut utiliser les 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 que vous spécifiez, seuls les utilisateurs spécifiés dans le groupe de mise à disposition et le groupe d'applications peuvent accéder aux applications dans ce groupe d'applications. 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 déjà 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 l'interface de gestion Configuration complète. Sinon, des noms en double s'afficheront 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.

Sélectionnez la liste déroulante **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 sélectionnez **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 saisi ces informations, sélectionnez **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 sélectionnez **OK**. Cette source ne peut pas être sélectionnée si le site ne dispose d'aucune application.

- **Packages d'applications :** applications dans App-V, MSIX, packagées vis l'attachement d'application MSIX ou des packages d'applications FlexApp. Lorsque vous sélectionnez cette source, la page **Ajouter des applications à partir de packages** s'ouvre. Sélectionnez une source de package d'applications, puis les applications que vous souhaitez ajouter dans la liste qui s'affiche, puis sélectionnez **OK**

  > **Remarque :**
  >
  > Pour publier des applications MSIX ou packagées via l'attachement d'application MSIX, le niveau fonctionnel du groupe de mise à disposition doit être 2106 ou supérieur. Pour les applications FlexApp, le niveau fonctionnel doit être 2206 ou supérieur. Lorsqu'une exigence de niveau fonctionnel n'est pas satisfaite, les options correspondantes de la liste déroulante des **sources de package d'application** sont grisées.
  >
  > **Remarque :**
  >
  > Sur VDA version 2003 et ultérieure, la publication de packages App-V à partir d'URL HTTP n'est pas prise en charge. Vous ne pouvez pas sélectionner ces applications dans la liste.

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 sélectionnez **Terminer**.

Gérer des groupes d'applications

January 31, 2023

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. Pour de plus amples informations, veuillez consulter la section Administration déléguée.

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. De même, si l'application a été expressément ajoutée à des groupes de mise à disposition associés au groupe d'applications (en plus d'être ajoutée 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 ce paramètre lors de la création du groupe.

1. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet gauche, 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. 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.

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 ce paramètre lors de la création du groupe. Pour de plus amples informations, consultez la section Partage de session avec des groupes d'applications.

1. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet gauche, 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. 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.

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, cela peut être 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, si vous démarrez Bloc-notes et qu'il existe une session déconnectée exécutant Bloc-notes, cette session est reconnectée au lieu d'en créer une nouvelle. 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.

Vous pouvez utiliser 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 d'applications 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 PowerShell du Broker 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. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet gauche, 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 sélectionnez **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. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet gauche, 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, sélectionnez **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, sélectionnez **OK**.
5. Pour supprimer des groupes de mise à disposition, cochez les cases des groupes que vous souhaitez supprimer, puis sélectionnez **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 sélectionnez **Modifier la priorité**. Entrez la priorité (0 = priorité la plus élevée), puis sélectionnez **OK**.
7. 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.

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. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet gauche, 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 le menu.

5. Pour modifier ou supprimer une restriction de balise, sélectionnez une autre balise à partir du menu ou supprimez la restriction de balise en désactivant le paramètre **Restreindre les lancements aux machines dotées de balises**.
6. 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.

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. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet gauche, 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, sélectionnez **Ajouter**, puis spécifiez les utilisateurs que vous souhaitez ajouter. Pour supprimer des utilisateurs, sélectionnez un ou plusieurs utilisateurs, puis sélectionnez **Supprimer**.
4. 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.

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 navigation.
2. Sous l'onglet **Toutes les 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 **OK** 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. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet gauche, puis sélectionnez l'onglet **Groupes d'applications**.
2. Sélectionnez un groupe d'applications dans le volet central, 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 **OK** 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 supprimera 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. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet gauche, 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 devez disposer de l'un des rôles intégrés suivants pour créer et gérer des dossiers pour les groupes d'applications :

- 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.
- Toutes les ressources de Configuration complète (telles 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

July 25, 2023

> **Remarque :**
>
> Cet article explique comment configurer Remote PC Access à l'aide de l'interface Configuration complète. Si vous utilisez l'interface Déploiement rapide, suivez les instructions de Remote PC Access dans Déploiement rapide.

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.

- Possibilité d'ajouter des machines à l'aide de fichiers CSV. Cela facilite l'ajout de machines en vrac dans les scénarios comportant des restrictions de structure d'unité d'organisation.
- 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, Citrix DaaS attribue automatiquement plusieurs utilisateurs à la machine non attribuée suivante. Pour restreindre l'attribution automatique à un seul utilisateur, accédez à **Configuration complète > 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 DaaS. Les sessions consomment des licences de la même manière que les autres sessions Citrix Virtual Desktops. Pour Citrix Cloud, Remote PC Access est valable pour Citrix DaaS et Workspace Premium Plus.

Considérations

Bien que toutes les exigences techniques et considérations qui s'appliquent à Citrix Virtual Apps and Desktops et Citrix DaaS 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 et Citrix DaaS 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 suivantes sont disponibles :
  - 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.

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/Linux
  - PC multi-utilisateurs dédiés Windows/Linux. 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/Linux groupés. Ce cas d'utilisation s'applique aux PC physiques auxquels plusieurs utilisateurs aléatoires peuvent accéder, tels que les laboratoires informatiques.

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.
- Vous pouvez choisir des unités d'organisation pour ajouter des machines au catalogue de machines en vrac. Dans certains scénarios, cette solution n'est pas facile en raison des restrictions de structure d'unité d'organisation. Au lieu de cela, vous pouvez ajouter des machines en vrac à l'aide de fichiers CSV. Cette fonctionnalité vous donne plus de flexibilité pour ajouter des machines en vrac. Vous pouvez ajouter uniquement des machines (à utiliser avec des attributions utilisateur automatiques) ou ajouter des machines avec attributions utilisateur.
- 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 :

- Le masquage de moniteur physique pour les VDA Remote PC Access est disponible, mais pas pour toutes les distributions Linux. Pour les distributions Linux non prises en charge, utilisez le VDA Linux sur des machines physiques uniquement en mode non 3D. Sinon, 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.
- Nous recommandons l'utilisation de catalogues de machines de type OS mono-session pour les machines Linux physiques.

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 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.
   - 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 le site de téléchargement de Citrix 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.

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.

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. 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. 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

Pour configurer Wake on LAN, vous pouvez utiliser l'interface de gestion Configuration complète ou PowerShell.

Configurer Wake on LAN dans l'interface Configuration complète Pour créer la connexion Wake on LAN :

1. Naviguez jusqu'au nœud **Hébergement** sur la gauche.
2. Sélectionnez **Ajouter une connexion et des ressources**.
3. Dans la page **Connexion** de l'Assistant, indiquez ce qui suit :
   a) Type de connexion : Wake on LAN de Remote PC
   b) Nom de la zone : sélectionnez la zone dans laquelle se trouve le catalogue Remote PC Access
   c) Nom de la connexion : entrez un nom pour la connexion Wake on LAN
4. Finalisez les étapes restantes dans l'assistant Ajouter une connexion et des ressources.

Pour ajouter la connexion Wake on LAN à un catalogue de machines Remote PC Access :

1. Si vous créez un nouveau catalogue de machines Remote PC Access, vous pouvez ajouter la connexion sur la page **Type de machine** de l'assistant Configuration du catalogue de machines à l'aide de la liste déroulante.
2. Si vous souhaitez ajouter la connexion Wake on LAN à un catalogue de machines existant :

a) Accédez au nœud **Catalogues de machines** sur la gauche.
b) Sélectionnez le catalogue de machines Remote PC Access approprié.
c) Cliquez avec le bouton droit sur le catalogue de machines ou sélectionnez le menu **Plus** au-dessus.
d) Sélectionnez **Modifier le catalogue de machines**.
e) Dans la page **Gestion de l'alimentation**, sélectionnez **Oui**.
f) Sélectionnez la connexion appropriée dans la liste déroulante.
g) Sélectionnez **Enregistrer**.

> **Remarque :**
>
> La configuration de Wake on LAN via l'interface Configuration complète n'est disponible qu'avec Citrix DaaS pour le moment.

Configurer Wake on LAN via PowerShell Pour configurer Wake on LAN via PowerShell :

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.
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)
{

```



```
24      Start-Sleep -s 5
25      $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
            $hypHc.HypervisorConnectionUid
26   }
27
28  <!--NeedCopy-->
```

Lorsque la connexion hôte est prête, exécutez les commandes suivantes pour récupérer l'identifiant unique de la connexion hôte :

```
1 $bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
2 $hypUid = $bhc.Uid
3 <!--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 :

```
1 Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
      RemotePCHypervisorConnectionUid $hypUid
2 <!--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.
- 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 l'interface Configuration complète ou de PowerShell
- Étant donné que le Delivery Controller ne connaît pas l'état d'alimentation d'un PC, l'interface Configuration complète affiche **Non pris en charge** sous état d'alimentation. Le Delivery Controller utilise donc l'état d'enregistrement du VDA pour déterminer si un PC est allumé ou éteint.

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.

Supprimer des composants

February 21, 2023

Pour supprimer des composants que vous avez installés (tels que des VDA), Citrix vous recommande d'utiliser la fonctionnalité Windows de suppression/modification de programmes. Vous pouvez également supprimer des composants à l'aide de la ligne de commande ou d'un script.

Lorsque vous supprimez des composants, les composants pré-requis ne sont pas supprimés, et les paramètres du pare-feu ne sont pas modifiés.

Lorsque vous supprimez un VDA, la machine redémarre automatiquement après la suppression, par défaut.

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 VDA, sélectionnez **Citrix Virtual Delivery Agent** <*version*>, puis cliquez avec le bouton droit de la souris et sélectionnez **Désinstaller**. Le programme d'installation démarre et vous permet de sélectionner les composants à supprimer.
- Pour supprimer le Serveur d'impression universelle, sélectionnez **Serveur d'impression universelle Citrix**, puis cliquez avec le bouton droit de la souris et sélectionnez **Désinstaller**.

Supprimer un VDA à l'aide de la ligne de commande

Exécutez la commande utilisée pour installer le VDA : `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` ou `VDAWorkstationCoreSetup.exe`. Consultez la section Installer à l'aide de la ligne de commande pour une description de la syntaxe.

- Pour supprimer uniquement le VDA ou le application Citrix Workspace, utilisez les options `/remove` et `/components`.

- Pour supprimer le VDA et application Citrix Workspace, utilisez l'option `/removeall`.

Par exemple, la commande suivante supprime le VDA et l'application Citrix Workspace d'une machine d'OS multi-session.

```
VDAServerSetup.exe /removeall
```

Par exemple, la commande suivante supprime le VDA mais pas l'application Citrix Workspace pour Windows (si elle est installée) d'une machine d'OS mono-session.

```
VDAWorkstationSetup.exe /remove /components vda
```

Vous pouvez également supprimer un VDA à l'aide d'un script fourni par Citrix. Consultez la section Supprimer des VDA à l'aide du script.

Couche de personnalisation de l'utilisateur

February 13, 2024

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 fonction 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. La fonctionnalité ne sera pas disponible tant que cette procédure ne sera pas terminée.

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 10 multi-session (Azure Files pris en charge)
- Windows Server 2016 (Azure Files pris en charge)
- Windows Server 2019 (Azure Files pris en charge)

Pour Citrix Virtual Apps and Desktops 7, l'utilisation d'Azure Files avec couches de personnalisation utilisateur est pris en charge sur Windows Server 2019, Windows Server 2016v et Windows 10 client.

> **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 fonctionne uniquement avec les bureaux non persistants.

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 Studio **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 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

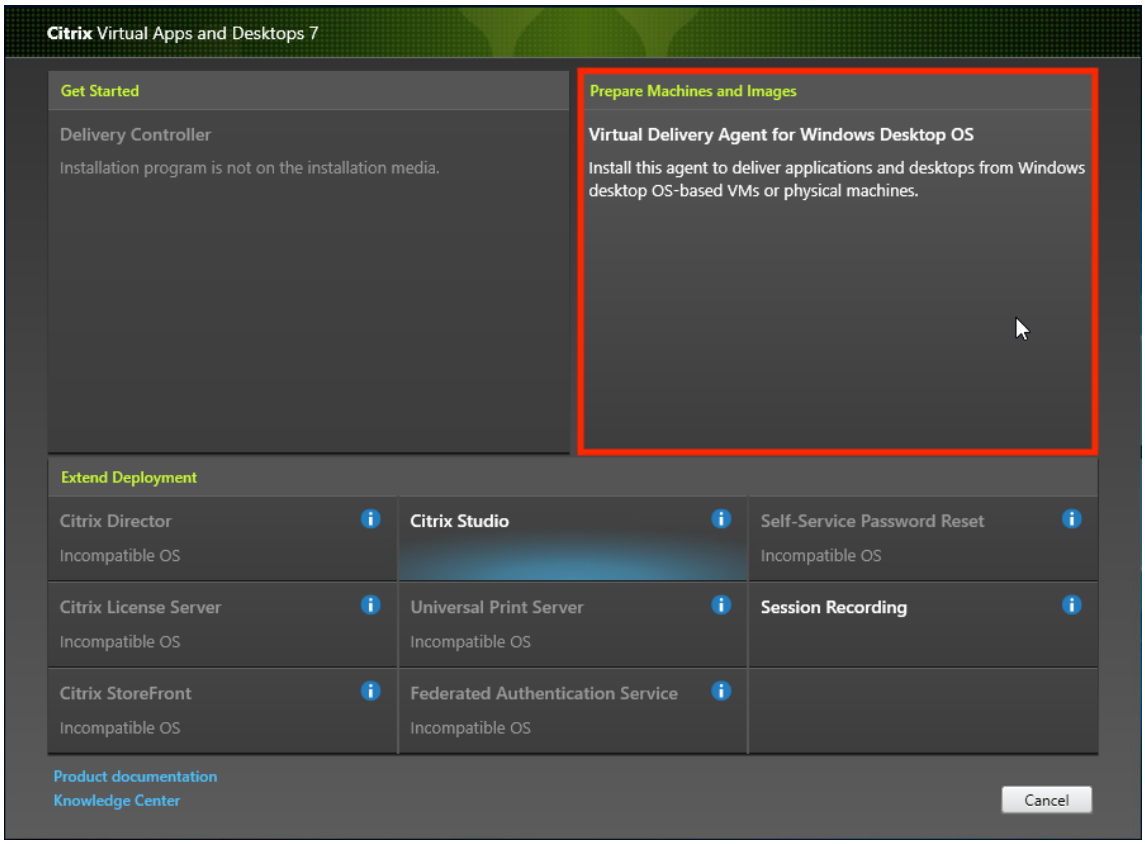
Assurez-vous que votre environnement Citrix Virtual Apps and Desktops peut être utilisé avec cette nouvelle fonctionnalité. Pour plus d'informations sur l'installation, reportez-vous à la section Installer et configurer Citrix Virtual Apps and Desktops.

Étape 2 : Préparer votre image principale

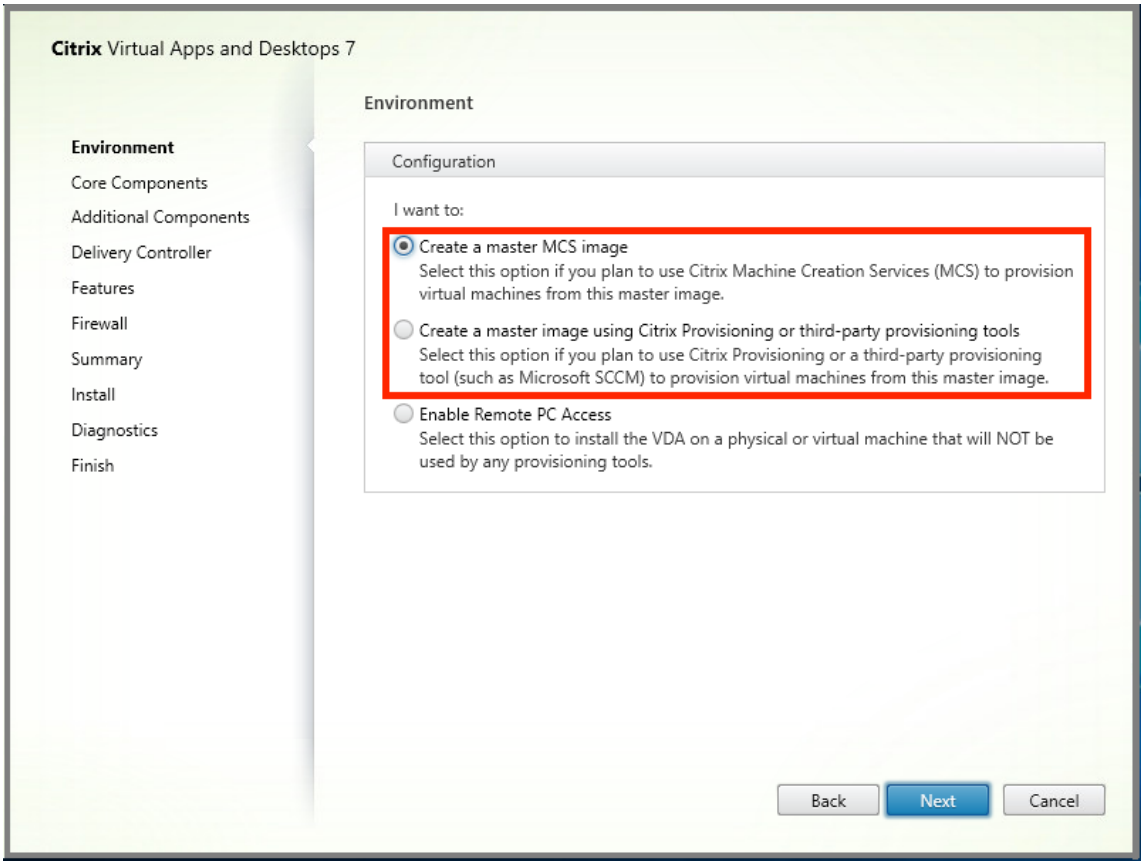
Pour préparer votre image principale :

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 vignette **Virtual Delivery Agent pour système d'exploitation de bureau Windows**.

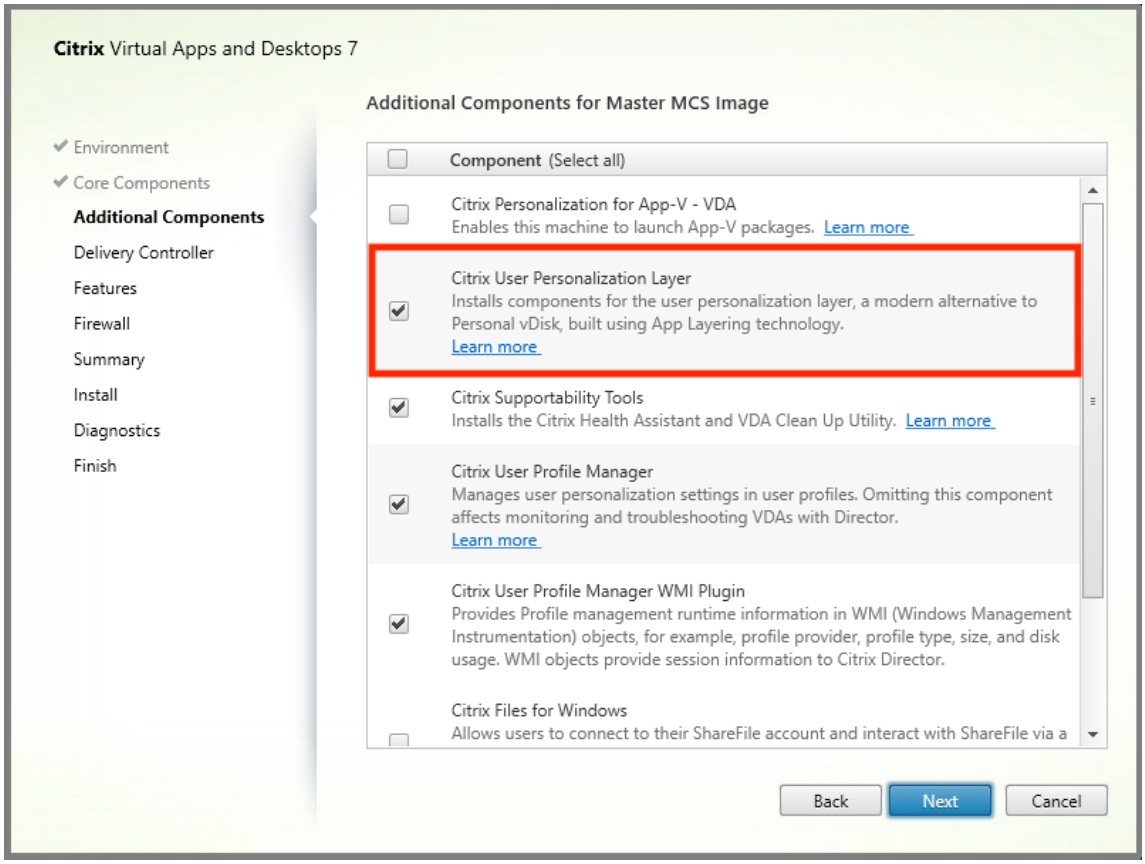


a) **Environnement :** sélectionnez **Créer une image MCS principale** ou **Créer une image principale à l'aide de Citrix Provisioning ou d'outils de provisioning tiers**.



a) **Composants principaux :** cliquez sur **Suivant**.

b) **Composants supplémentaires :** sélectionnez **Couche de personnalisation des utilisateurs Citrix**.



a) Cliquez sur les écrans d'installation restants, 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 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.

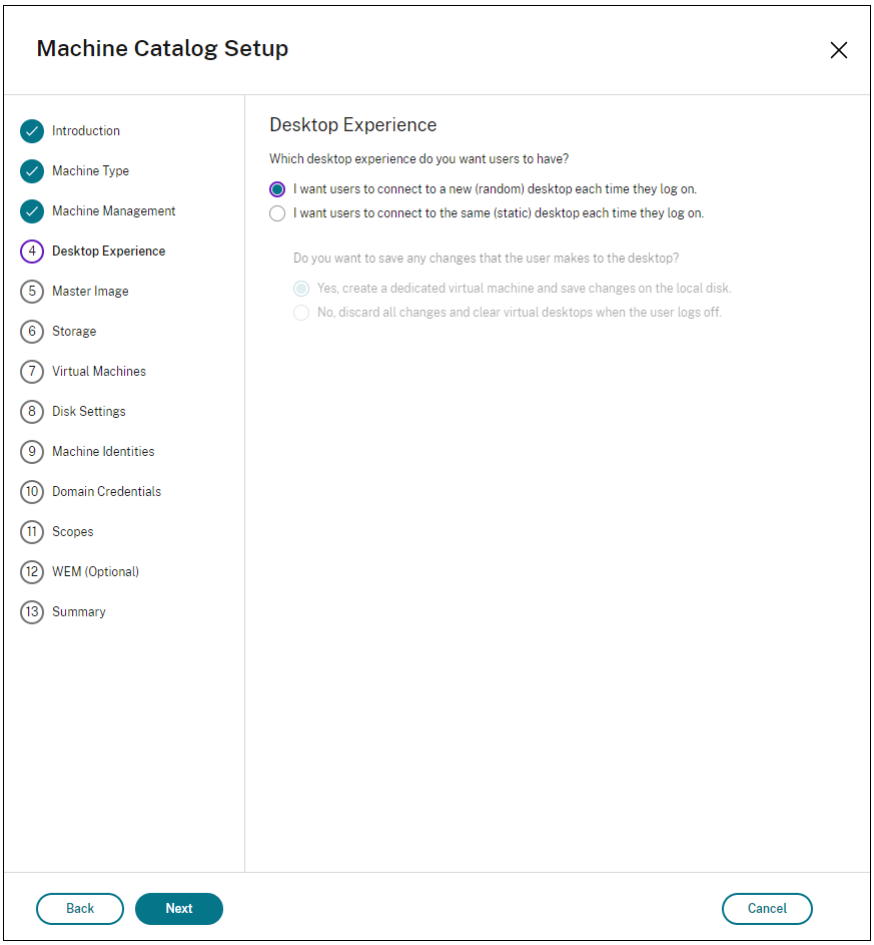
Étape 3 : Créer un catalogue de machines

Dans Studio, suivez les étapes pour créer un catalogue de machines. Utilisez les options suivantes lors de la création du catalogue :

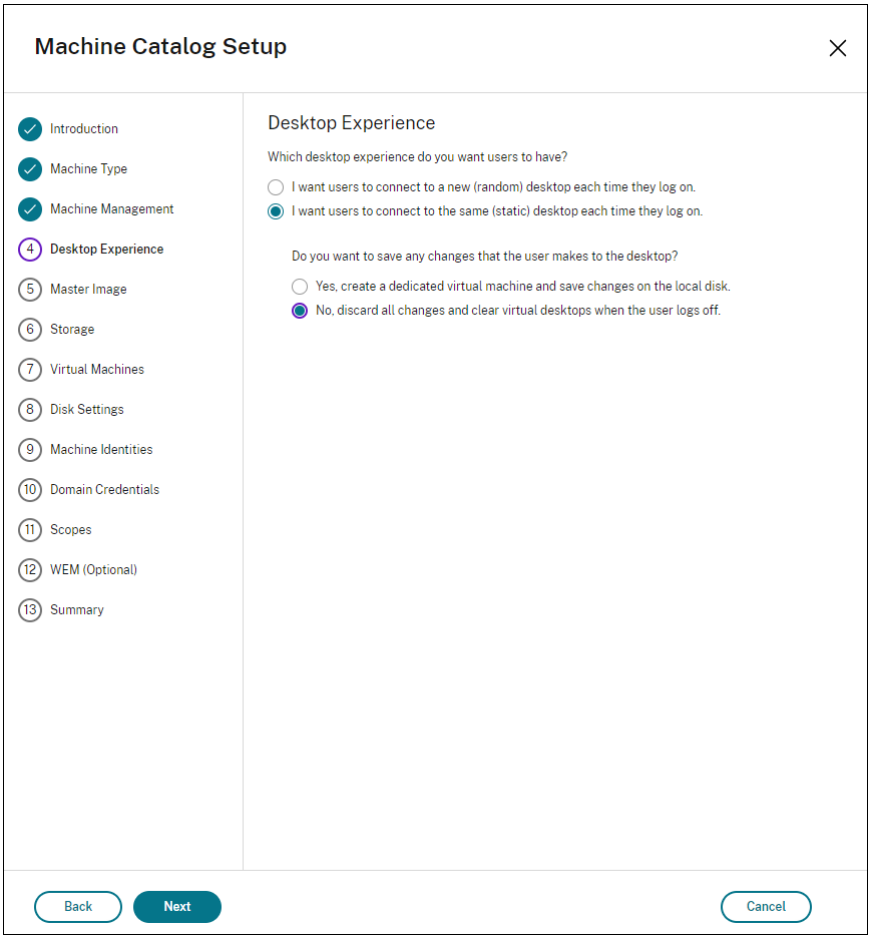
1. Sélectionnez **Système d'exploitation** et définissez sur **OS mono-session**.

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.

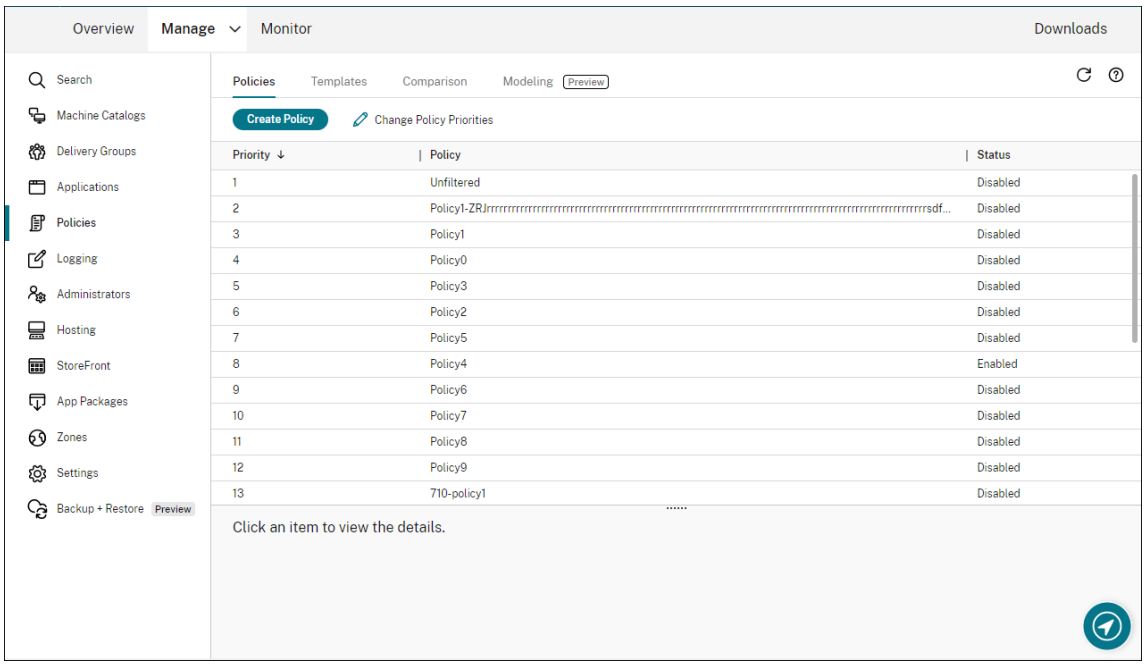
Étape 5 : Créer des stratégies personnalisées de groupe de mise à disposition

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. Tapez « couche utilisateur » dans le champ de recherche. Les trois stratégies suivantes apparaissent dans la liste des stratégies disponibles :

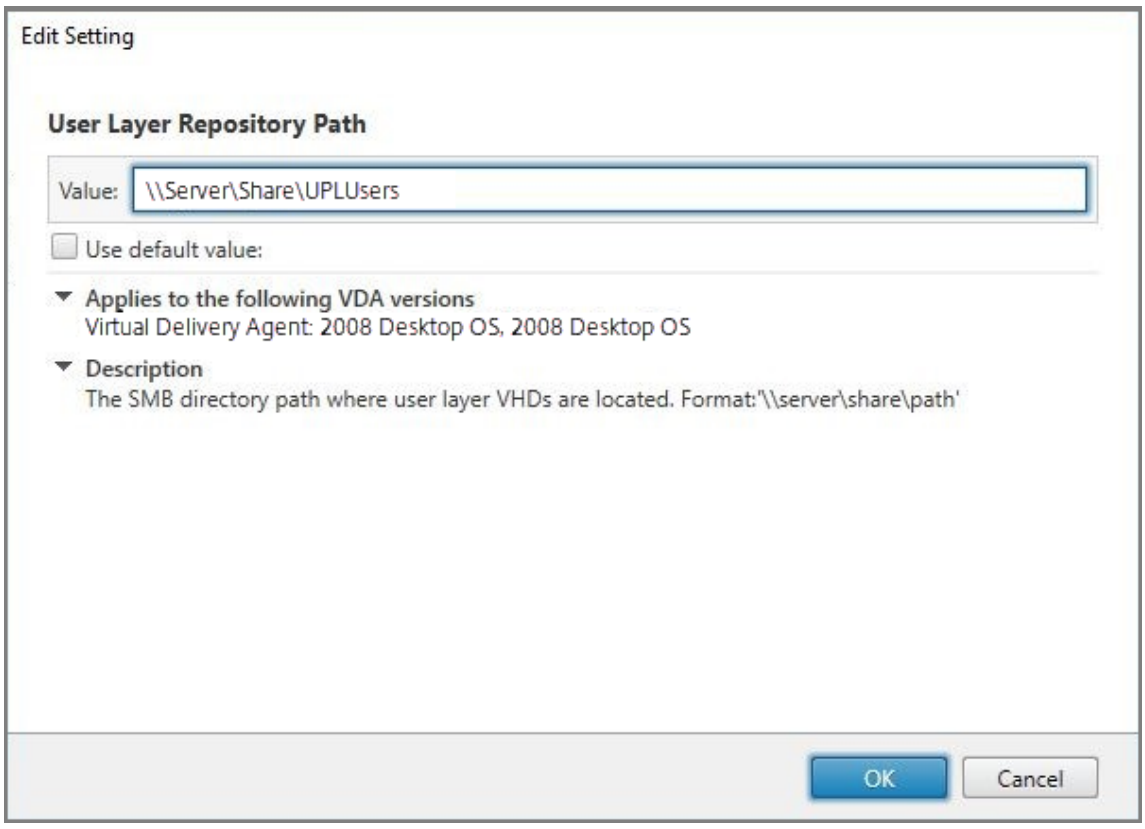
   - Exclusions de couche utilisateur
   - Chemin du référentiel de couche utilisateur
   - Taille de la couche utilisateur en Go

   > **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`

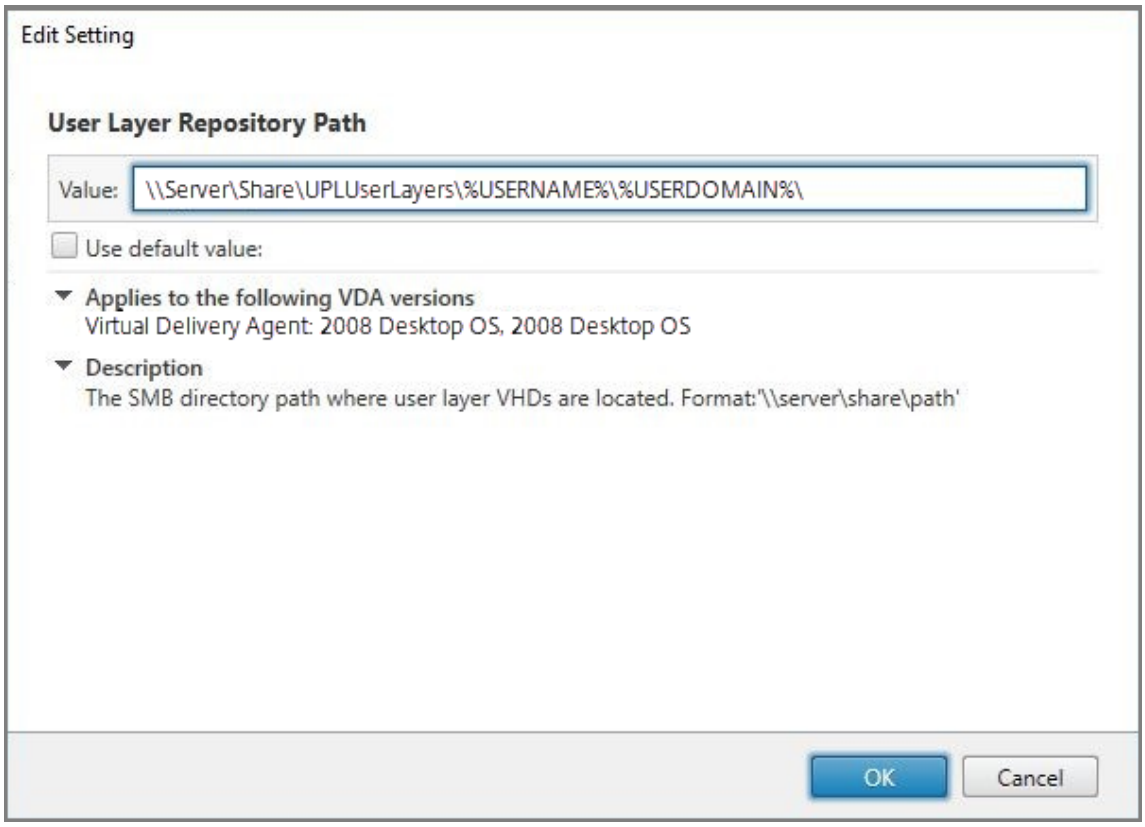


Vous pouvez personnaliser le chemin à l'aide des variables `%USERNAME%` et `%USERDOMAIN%`, des variables d'environnement de la machine et des attributs Active Directory (AD). Lorsqu'elles sont développées, ces variables entraînent des chemins explicites.

Exemples de variables d'environnement :

- **Format du chemin d'accès :** `\\Server-name-or-address\share-name\folder-with-environment-variables`

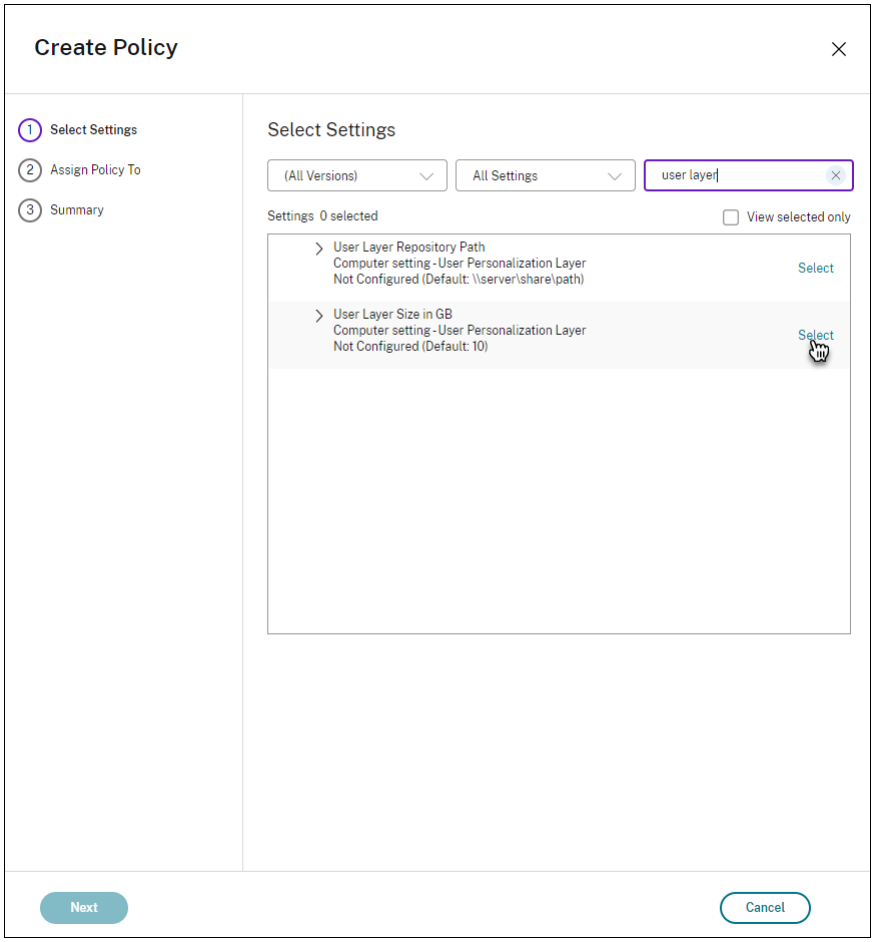
- **Exemple de chemin d'accès :** `\\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%`
- **Exemple de chemin obtenu :**Pour un utilisateur nommé **Alex** dans **CoolCompanyDomain**, le chemin d'accès correspond à :`\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`



Exemple d'attributs AD personnalisés :

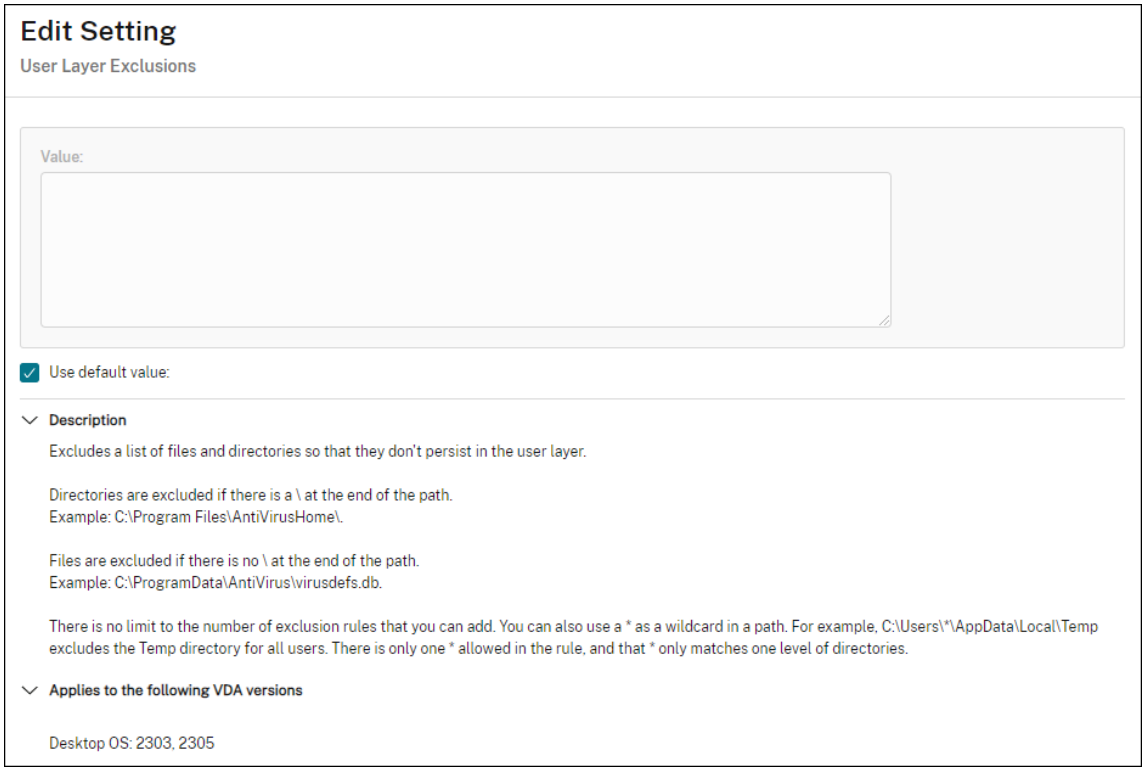
- Format du chemin d'accès : `\\Server-name-or-address\share-name\AD-attribute`
- Exemple de chemin d'accès : `\\Server\share\\#sAMAccountName#`
- Exemple de chemins résultants : `\\Server\share\JohnSmith` (si #sAMAccountName # correspond à JohnSmith pour l'utilisateur actuel)

6. Facultatif : cochez la case en regard de **Taille de la couche utilisateur en Go** et cliquez sur **Modifier** :

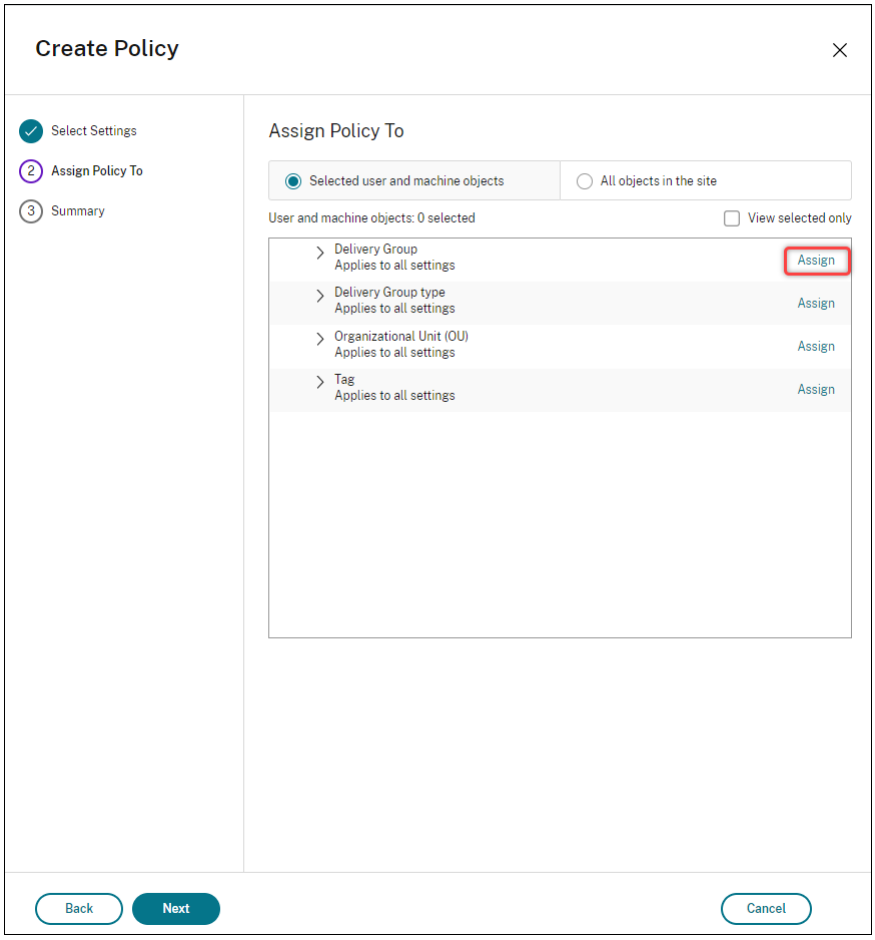


La fenêtre Modifier les paramètres s'affiche.

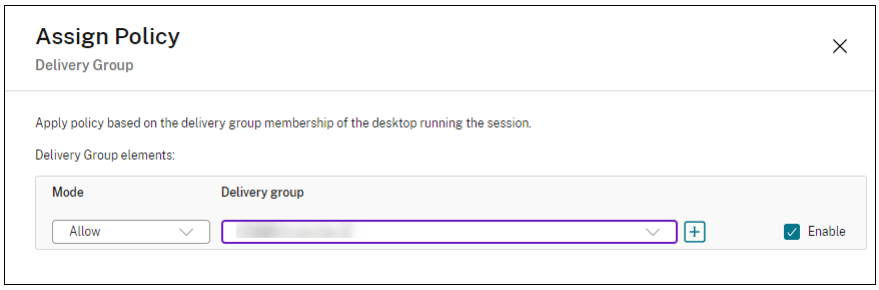
7. Facultatif : remplacez la valeur par défaut de **10 Go** par la taille maximale que chaque couche utilisateur peut atteindre. Cliquez sur **Enregistrer**.
8. Facultatif : cochez la case en regard de **Exclusions de couche utilisateur** et cliquez sur **Modifier**.



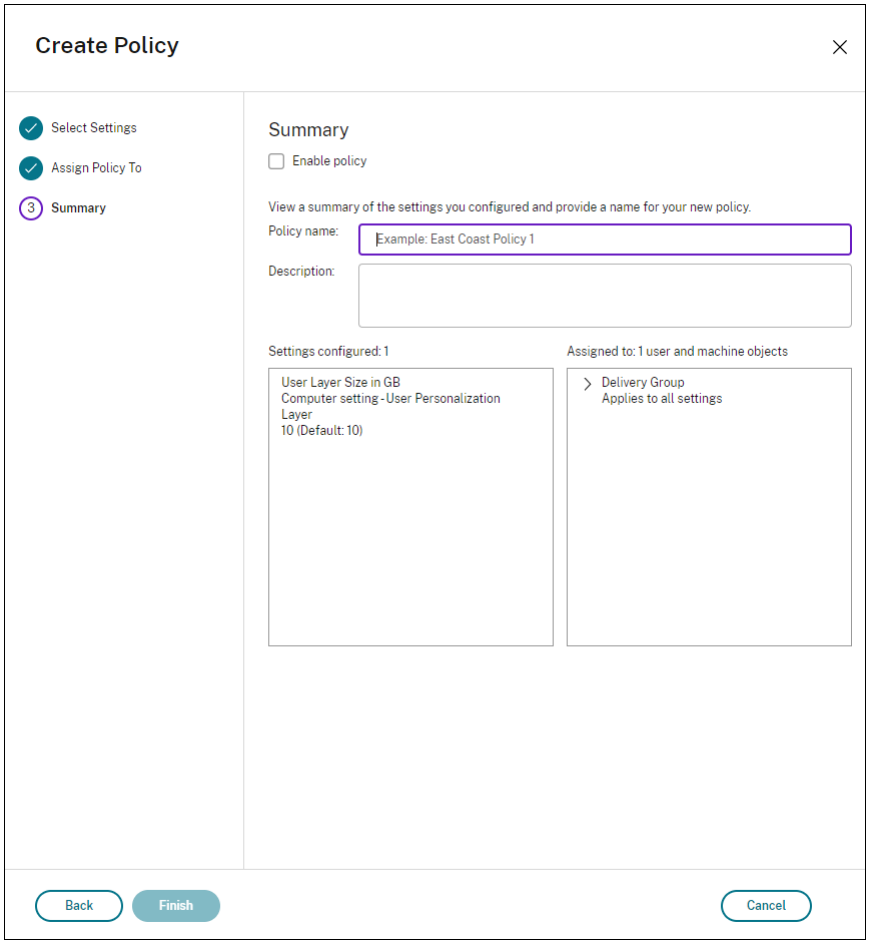
9. Facultatif : spécifiez les fichiers et les dossiers à exclure, puis cliquez sur **Enregistrer**. Pour plus d'informations, consultez la documentation de Citrix App Layering.
10. Cliquez sur **Suivant** pour configurer les utilisateurs et les machines auxquels vous souhaitez attribuer des tâches. Cliquez 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

Nom du paramètre	Valeur	Appliquer à
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
System	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.

```
C:\ProgramData\Unidesk\Logs\ulayersvc.log
<!--NeedCopy-->
```


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.

Mettre à niveau les VDA

May 17, 2024

Introduction

Citrix conserve tous les composants de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) dans votre déploiement à l'exception des VDA.

Avant de procéder à la mise à niveau d'un VDA :

- Lisez intégralement cet article afin de savoir à quoi vous attendre.
- Consultez la stratégie de cycle de vie pour Citrix DaaS.

Pour mettre à niveau un VDA, téléchargez un programme d'installation VDA et exécutez-le sur la machine ou l'image. Vous pouvez utiliser l'interface graphique du programme d'installation ou l'interface de ligne de commande. Pour plus d'informations, reportez-vous aux sections suivantes :

- Programmes d'installation de VDA

- Installer des VDA à l'aide de l'interface graphique
- Installer des VDA à l'aide de la ligne de commande

Si le VDA a été installé à l'origine à l'aide de `VDAWorkstationCoreSetup.exe` :

- cette configuration sera conservée si vous le mettez à niveau avec la dernière version du même programme d'installation.
- Si vous exécutez le programme d'installation `VDAWorkstationSetup.exe` sur cette machine, vous pouvez activer les fonctionnalités qui ne sont pas prises en charge dans `VDAWorkstationCoreSetup.exe`. N'oubliez pas que certaines de ces fonctionnalités peuvent être activées par défaut dans le programme d'installation `VDAWorkstationSetup.exe`. Vous pouvez également installer l'application Citrix Workspace.

> **Remarque :**
>
> 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. Ce redémarrage ne peut pas être évité. La mise à niveau reprend automatiquement après le redémarrage (sauf si vous spécifiez `/noresume` sur la ligne de commande).

Une fois les VDA mis à niveau, mettez à jour les images et les catalogues qui utilisent ce VDA.

Mettre à niveau les VDA à l'aide de l'interface Configuration complète

> **Important :**
>
> - Nous vous recommandons de tester rigoureusement les mises à niveau des VDA avant de passer en production.
> - Vous pouvez basculer entre le VDA CR et le VDA LTSR à condition de passer d'une version antérieure à une version ultérieure. Vous ne pouvez pas passer d'une version ultérieure à une version antérieure, car cela est considéré comme une rétrogradation. Par exemple, vous ne pouvez pas passer de 2212 CR à 2203 LTSR (n'importe quelle CU), mais vous pouvez mettre à niveau de 2112 CR à 2203 LTSR (n'importe quelle CU).
> - Les mises à jour à la demande (telles que les corrections et les correctifs entre les versions majeures) ne sont pas prises en charge.
> - Le VDA CVAD 2402 est disponible via le service de mise à niveau de VDA.

À l'aide de l'interface Configuration complète, vous pouvez mettre à niveau les VDA par catalogue ou par machine. Vous pouvez les mettre à niveau immédiatement ou à une heure planifiée.

Pour en savoir plus sur le service de mise à niveau du VDA, consultez la fiche technique : Service de mise à niveau du VDA Citrix. Vous y trouverez un aperçu du service, des informations détaillées sur son fonctionnement et d'autres ressources utiles.

Logiciels requis

- Plan de contrôle : Citrix DaaS
- Type de VDA : VDA avec OS mono-session ou multi-session. Actuellement, seul le VDA Windows est pris en charge.
- Version du VDA : 2109 ou version ultérieure, ou 2203 LTSR ou version ultérieure

  > **Remarque :**
  >
  > Nous vous recommandons d'utiliser la version CR de VDA la plus récente ou la version LTSR CU de VDA la plus récente.

- Type de provisioning : les machines persistantes (telles que les machines provisionnées par MCS, les machines Remote PC Access, Citrix HDX Plus pour Windows 365). Consultez la section Types de machines pris en charge.
- L'agent de mise à niveau de VDA doit être installé sur les VDA et le service doit être en cours d'exécution.
- Vous êtes autorisé à mettre à niveau des VDA.
- La mise à niveau du VDA est configurée avec la version CR ou LTSR appropriée dans Configuration complète.
- Les VDA ne sont pas utilisés. (Les utilisateurs doivent s'en déconnecter.)

  > **Remarque :**
  >
  > Les mises à niveau sont ignorées pour tous les VDA en cours d'utilisation ou déconnectés. Nous vous recommandons de planifier une fenêtre de mise à niveau et de demander aux utilisateurs de se déconnecter des VDA.

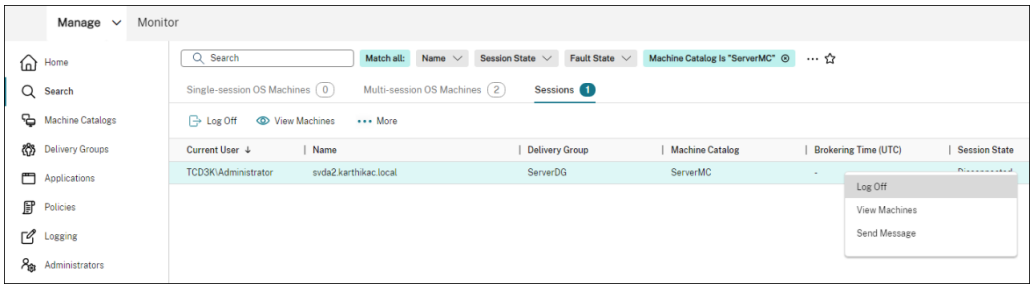
- Les VDA ne sont pas en mode de maintenance. (Un VDA peut être mis en mode de maintenance par un administrateur. Un VDA peut également être automatiquement placé en mode de maintenance s'il a dépassé le nombre maximum de tentatives d'enregistrement autorisées.)
- Les URL pertinentes ont été ajoutées à la liste d'autorisation si le filtrage d'URL est en place. Consultez la section Exigence de mise à niveau du VDA.
- Les VDA doivent appartenir à un groupe de mise à disposition et être enregistrés auprès de DaaS.
- Le niveau fonctionnel est correctement défini afin que la fonctionnalité de mise à niveau du VDA puisse être utilisée. Voir Versions de VDA et niveaux fonctionnels.
- Le VDA de destination prend en charge le système d'exploitation du VDA actuel.

Problèmes connus

Problème 1 : échec de la mise à niveau des VDA LTSR vers les versions de mise à jour cumulative (CU) LTSR Les tentatives de mise à niveau des VDA LTSR vers des versions de mise à jour cumulative (CU) LTSR peuvent échouer. Bien que le processus de mise à niveau semble s'achever correctement dans Configuration complète, la version installée du VDA ne change pas et l'état revient à **Mise à niveau disponible** après une minute ou deux. Le problème se produit avec les VDA sur lesquels un agent de mise à niveau de VDA version 7.35.0.7 ou antérieure est installé.

Pour contourner le problème, connectez-vous au VDA et mettez à niveau l'agent de mise à niveau vers la version 7.37.0.7 ou ultérieure (à l'aide du programme d'installation de VDA version 2303 ou ultérieure). À partir de la version 7.37.0.7, l'agent de mise à niveau de VDA prend en charge la mise à niveau automatique afin que les agents des versions antérieures exécutés sur les VDA puissent effectuer automatiquement la mise à niveau vers la dernière version. Grâce à cette fonctionnalité de mise à jour automatique, le service de mise à niveau de VDA vérifie la version du VDA signalée par l'agent, puis planifie les mises à niveau dans un délai d'une heure pour effectuer automatiquement la mise à niveau de l'agent vers la dernière version. Cette fonctionnalité de mise à niveau automatique réduit vos efforts de maintenance.

Pour que l'agent du VDA effectue la mise à niveau automatique, veillez à fermer les sessions afin que le service de mise à niveau de VDA puisse lancer les mises à niveau automatiques. Vous pouvez fermer les sessions dans Configuration complète.



Si la mise à niveau automatique de l'agent échoue, connectez-vous au VDA et mettez à niveau l'agent manuellement comme suit :

1. Exécutez l'applet de commande suivante pour afficher l'agent de mise à niveau de VDA dans Panneau de configuration > Désinstaller ou modifier un programme.

```
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent Service
      - x64'  }
 ).GetValue('SystemComponent')
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent Service
      - x64'  }
```



```
  ) | Set-ItemProperty -Name SystemComponent -Value 0
<!--NeedCopy-->
```

2. Installez la dernière version de l'agent de mise à niveau de VDA. Pour effectuer une installation silencieuse, utilisez l'applet de commande suivante :

   - `msiexec /i CitrixUpgradeAgent_x64.msi /q`

Vous pouvez identifier la version de l'agent de mise à niveau de VDA à l'aide de l'applet de commande ou d'un script. Voir Dépanner.

Problème 2 : le proxy n'est pas pris en charge Actuellement, l'agent de mise à niveau de VDA ne prend pas en charge les configurations de proxy. Cette limitation peut entraîner des problèmes de connectivité lorsque l'agent tente d'établir des connexions via un serveur proxy.

Vous pouvez appliquer la solution suivante pour résoudre le problème. Suivez les étapes ci-dessous.

1. Localisez le fichier de configuration de l'agent de mise à niveau de VDA à l'adresse suivante : `C:\Program Files\Citrix\CitrixUpgradeAgent\Citrix.UpdateServices.UpdateAgent.exe.config`.
2. Ouvrez le fichier de configuration à l'aide d'un éditeur de texte.
3. Ajoutez les lignes suivantes à la fin du fichier, en remplaçant `ProxyServerName` par le nom réel du serveur proxy :

```
<system.net>
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy proxyaddress="http://PROXYSERVER:PORT" usesystemdefault
        ="false" />
  </defaultProxy>
</system.net>
</configuration>
<!--NeedCopy-->
```

4. Redémarrez le service de l'agent de mise à niveau de Citrix VDA pour appliquer la configuration mise à jour.

Workflow général

Voici un workflow général pour mettre à niveau les VDA dans l'interface Configuration complète :

1. Activez la mise à niveau de VDA pour un catalogue.

   - Vous pouvez activer la mise à niveau du VDA lorsque vous créez un catalogue.
   - Vous pouvez activer la mise à niveau du VDA lorsque vous modifiez un catalogue.

2. Mettez à niveau les VDA par catalogue ou par machine. Pour plus d'informations, voir Configurer la mise à niveau automatique pour les VDA.

> **Remarque :**
>
> Lorsque vous planifiez des mises à niveau de VDA pour un catalogue, n'oubliez pas que toutes les machines du catalogue seront incluses dans la mise à niveau. Nous vous recommandons donc de sauvegarder ces machines avant de lancer la mise à niveau.

Dépannage

En cas d'échec de la mise à niveau, vous pouvez utiliser les journaux suivants pour résoudre vous-même les problèmes ou fournir les journaux lorsque vous contactez le support technique Citrix pour obtenir de l'aide.

- Journaux d'installation pour l'installation initiale du VDA sous `%temp%/Citrix/XenDesktop Installer`
- Journaux de mise à niveau sous `C:\Windows\Temp\Citrix\XenDesktop Installer`

Pour vérifier les versions de l'agent de mise à niveau de VDA, utilisez l'applet de commande suivante : `Get-VusComponentVersion -ComponentType VUS`. Il répertorie tous les VDA et les versions de leur agent de mise à niveau de VDA.

Pour obtenir les noms des VDA, utilisez l'applet de commande suivant : `Get-BrokerMachine -UUID "<version number>"`, où `<version number>` est la version de l'agent de mise à niveau de VDA que vous obtenez à partir de l'applet de commande `Get-VusComponentVersion`.

Pour vérifier les versions de l'agent de mise à niveau de VDA au niveau du catalogue, vous pouvez utiliser le script suivant :

> **Remarque :**
>
> Le script est donné à titre d'exemple et il peut être nécessaire de l'adapter à votre environnement spécifique. Nous vous recommandons de tester le script rigoureusement avant de l'utiliser dans un environnement de production.

```
Param(
    [Parameter (Mandatory=$true)]
    [string] $CatalogName
)

try
{

```



```
9      $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-
           Object -Property UUID
10
11     if($Uuids -eq $null)
12     {
13
14         throw "Cannot find CatalogName "+$CatalogName
15      }
16
17     Write-Output("Catalog Name passed is "+$CatalogName)
18
19    foreach($Uuid in $Uuids)
20     {
21
22         $compVersion = Get-VusComponentVersion -MachineId $machine.UUID
               -ComponentType VUS
23         $Machine = Get-BrokerMachine -UUID $compVersion.MachineId
24         Write-Output("MachineName: "+$Machine.MachineName+", Machine
               UUID:"+$machine.MachineId+", VUA Version:"+$compVersion.
               Version)
25      }
26
27  }
28
29 catch
30 {
31
32     Write-Output("Exception Occured")
33     Write-Host $_
34  }
35
36 <!--NeedCopy-->
```

Journaux relatifs à l'agent de mise à niveau de VDA Vous pouvez également collecter des journaux relatifs à l'agent de mise à niveau de VDA. Les journaux que vous pouvez collecter incluent :

- **Traces CDF (Citrix Diagnostic Facility)**.
- **Journal d'événements Windows**. Informations écrites dans le journal d'événements Windows. Affichez les journaux en accédant à **Observateur d'événements > Journaux des applications et des services > Service de l'agent de mise à niveau de Citrix VDA**.

Si nécessaire, vous pouvez modifier le fichier de configuration de l'agent de mise à niveau de VDA afin que les journaux soient écrits en continu dans un fichier. Pour activer la journalisation dans un fichier, procédez comme suit :

1. Accédez au dossier `C:\Program Files\Citrix\CitrixUpgradeAgent`.
2. Ouvrez le fichier `Citrix.UpdateServices.UpdateAgent.exe.config`.
3. Remplacez la valeur `LogToFile` par 1.

4. Redémarrez le service de l'agent de mise à niveau de Citrix VDA. Un fichier journal est alors créé dans `C:\ProgramData\Citrix\Update Services\Logs`.

> **Remarque :**
>
> - L'activation de la journalisation dans un fichier permet d'écrire des journaux en continu, ce qui peut consommer de l'espace de stockage. N'oubliez pas de désactiver la journalisation une fois le problème résolu. Pour désactiver la journalisation, définissez `LogToFile` sur `0`, puis redémarrez le service de l'agent de mise à niveau de Citrix VDA.
> - Lorsque `LogToFile=1` est défini, les journaux sont écrits uniquement dans le fichier. Ils n'apparaîtront pas dans les traces CDF.

Résoudre les échecs de téléchargement des mises à niveau de VDA Suivez les étapes ci-dessous pour résoudre les échecs de téléchargement liés à la fonctionnalité de mise à niveau du VDA :

1. Assurez-vous que les URL pertinentes ont été ajoutées à la liste d'autorisation si le filtrage d'URL est en place. Consultez la section Exigence de mise à niveau du VDA.
2. Après avoir ajouté les URL nécessaires à la liste d'autorisation, essayez de reprogrammer la mise à niveau du VDA.

Vous pouvez activer le traçage CDF ou configurer `LogToFile` sur `1` pour capturer des journaux détaillés à des fins d'analyse. Si l'échec du téléchargement persiste, vérifiez les erreurs. Si le message d'erreur suivant « Échec du téléchargement : cette liste de contrôle d'accès n'est pas de forme canonique et ne peut donc pas être modifiée. » s'affiche, cela indique que les autorisations sur le dossier `C:/ProgramData/Citrix/UpgradeServices/Downloads/VDA` sont incorrectes. Pour résoudre ce problème, effectuez l'une des opérations suivantes :

- **Option 1** : réinitialisez les listes de contrôle d'accès (ACL) du dossier à l'aide de la commande suivante. (La commande réinitialise les ACL avec les ACL héritées par défaut pour tous les fichiers correspondants.)

  ```
  - icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\
    VDA"/reset /T /C /L /Q
  ```

- **Option 2** : supprimez le dossier VDA sous Téléchargements, puis programmez la mise à niveau du VDA.

Résoudre les échecs de validation des mises à niveau de VDA Suivez les étapes ci-dessous pour résoudre les échecs de téléchargement liés à la fonctionnalité de mise à niveau du VDA :

1. Assurez-vous que les URL pertinentes ont été ajoutées à la liste d'autorisation si le filtrage d'URL est en place, en particulier les URL de la liste de révocation de certificats (CRL) ou du pro-

tocole OCSP (Online Certificate Status Protocol) nécessaires à la vérification de la révocation. Consultez la section Exigence de mise à niveau du VDA.

2. Après avoir ajouté les URL nécessaires à la liste d'autorisation, essayez de reprogrammer la mise à niveau du VDA.

Nous vous recommandons d'activer le traçage CDF ou de configurer `LogToFile` sur 1 pour capturer des journaux détaillés à des fins d'analyse. Les journaux peuvent inclure les erreurs suivantes :

- État de révocation inconnu
- La fonction de révocation n'a pas pu vérifier l'état de révocation du certificat.
- La fonction de révocation n'a pas pu vérifier la révocation car le serveur de révocation était hors ligne.

L'agent de mise à niveau de VDA s'appuie sur les appels système Windows pour valider les certificats et effectuer des contrôles de révocation. Les erreurs ci-dessus indiquent que l'agent n'est pas en mesure d'établir une connexion aux URL CRL ou OCSP.

Notez que l'agent de mise à niveau de VDA ne prend actuellement pas en charge les paramètres de proxy. Les appels CRL et OCSP sortants effectués par CryptoAPI ne reconnaissent pas les configurations de proxy, ce qui peut entraîner des échecs.

Si votre environnement dispose d'une configuration de proxy, vous pouvez configurer le proxy système sur le VDA pour faciliter les appels CRL sortants. Suivez les étapes ci-dessous pour configurer le proxy système :

```
netsh winhttp import proxy source=ie

Or

netsh winhttp set proxy proxy-server=http://Proxy_Server:Port
<!--NeedCopy-->
```

Mettre à niveau les VDA à l'aide de PowerShell

Vous pouvez configurer les mises à niveau des VDA à l'aide du SDK Remote PowerShell. Pour plus d'informations sur le SDK Remote PowerShell, consultez SDK Remote PowerShell Citrix DaaS.

Les applets de commande PowerShell sont les suivantes :

- **Get-VusCatalog**

  Utilisez cette applet de commande pour obtenir les détails d'un catalogue tels que `Name`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR), `Upgrade scheduled` et `StateId` (état de `Upgrade scheduled`).

- **Get-VusMachine**

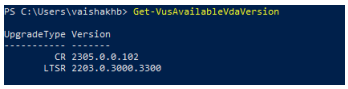
  Utilisez cette applet de commande pour obtenir les détails d'une machine tels que `MachineName`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR) et `StateId` (état de `Upgrade scheduled`).

- **Get-VusComponentVersion**

  Utilisez cette applet de commande pour vérifier si les VDA ont signalé les versions des composants. Utilisez la valeur `MachineId` pour filtrer les VDA. `MachineId` est l'UUID de `Get-BrokerMachine`.

- **Get-VusAvailableVdaVersion**

  Utilisez cette applet de commande pour vérifier la dernière version de CR/LTSR publiée via le service de mise à jour de VDA.

- **Set-VusCatalogUpgradeType**

  Utilisez cette applet de commande pour définir le type de mise à niveau d'un catalogue vers CR ou LTSR. Le type de mise à niveau ne peut être défini qu'au niveau du catalogue de machines.

- **New-VusMachineUpgrade**

  Utilisez cette applet de commande pour configurer les mises à niveau du VDA au niveau des machines.

- **New-VusCatalogSchedule**

  Utilisez cette applet de commande pour planifier les mises à niveau des VDA au niveau du catalogue de machines.

Exemples d'applets de commande au niveau de la machine

- Définissez le type de mise à niveau.

  Exemple :

  ```
  - Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType
    LTSR
  ```

- Utilisez `Get-VusMachine` pour vérifier la valeur `UpgradeState` des machines d'un catalogue.

  Exemple :

  ```
  -Get-VusMachine -CatalogName test-catalog
  ```



```
PS C:\Users> Get-VusMachine -CatalogName test-catalog


CatalogName       : test-catalog
DNSName           : test-machine-1
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-1
MachineUid        : 35
MachineUuid       : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :

CatalogName       : test-catalog
DNSName           : test-machine-2
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-2
MachineUid        : 36
MachineUuid       : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :
```

Si vous constatez que la valeur de `UpgradeState` est `Unknown`, l'une des raisons possibles est que l'agent de mise à niveau Citrix VDA installé sur le VDA n'a pas signalé la version au service de mise à jour de VDA. Vous pouvez utiliser l'applet de commande `Get-VusComponentVersion` pour vérifier si le VDA a signalé les versions des composants.

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

Si aucun résultat n'est affiché, vérifiez les points suivants :

- Le VDA fait partie d'un catalogue et d'un groupe de mise à disposition.
- L'agent de mise à niveau du VDA est installé sur le VDA et en cours d'exécution. Si nécessaire, essayez de redémarrer l'agent.

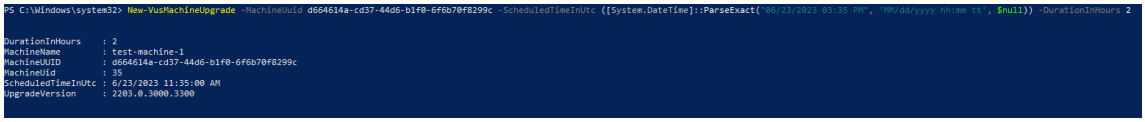
Remarque : si vous n'obtenez pas de résultat, collectez les traces du Centre de diagnostic Citrix lors du redémarrage de l'agent de mise à niveau du VDA et résolvez les problèmes.

- Planifiez les mises à niveau du VDA. Avant de commencer, tenez compte des points suivants :
  - `DurationInHours` : vous permet de fournir la durée en heures du processus de mise à niveau. Les VDA seront mis en mode de maintenance. Le programme d'installation du VDA sera téléchargé et la mise à niveau sera effectuée. Prévoyez une durée plus longue s'il y a de nombreux VDA à mettre à niveau.
  - `UpgradeNow` : utilisez ce commutateur pour planifier une mise à niveau immédiatement ou configurez `ScheduledTimeInUtc`.
  - `ScheduledTimeInUtc` : vous permet de planifier une mise à niveau pour une date et une heure spécifiques.

  Exemple :

  - `New-VusMachineUpgrade -MachineUuid d664614a-cd37-44d6-b1f0-6f6b70f8299c -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 03:35 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 2`

  Vous pouvez utiliser `MachineUuid`, `MachineUid` et `MachineName` pour planifier la mise à niveau du VDA.

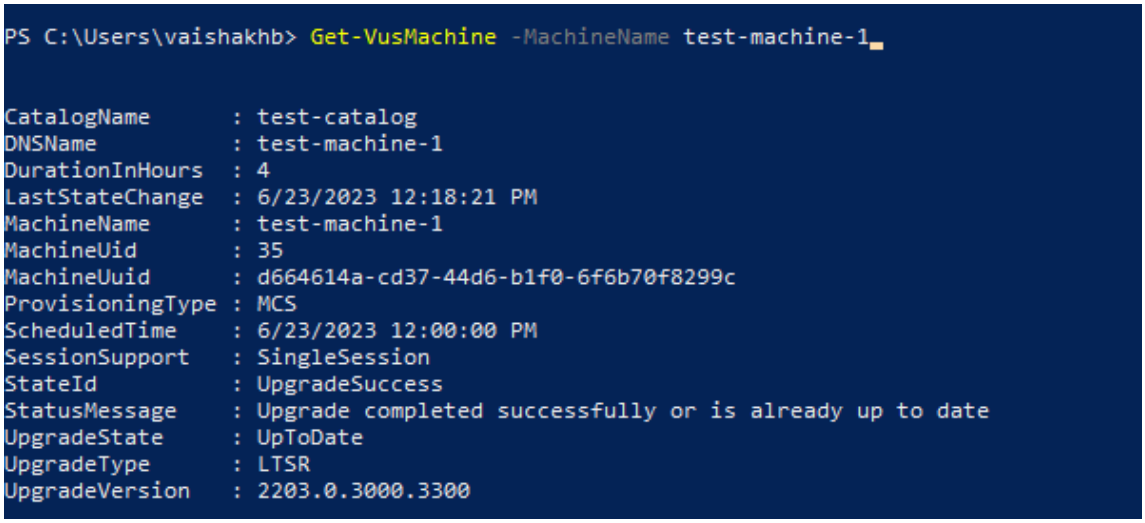


- Vérifiez l'état de la mise à niveau.

  Exemple :
  - `Get-VusMachine -MachineName test-machine-1`

```
PS C:\Windows\system32> Get-VusMachine -MachineName test-machine-1


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 2
LastStateChange  : 6/23/2023 11:47:35 AM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 11:35:00 AM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

Exemples d'applets de commande au niveau du catalogue

- Définissez le type de mise à niveau au niveau du catalogue de machines.

  Exemple :
  - `Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType LTSR`

- Utilisez `Get-VusCatalog` pour vérifier la valeur `UpgradeState` des machines d'un catalogue :

  Exemple :
  - `Get-VusCatalog -Name test-catalog`


```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog


CancelledUpgrades           :
DurationInHours             :
FailedUpgrades              :
InProgressUpgrades          :
LastStateChangeInUtc        :
MaxConcurrentUpgrades       :
Name                        : test-catalog
ProvisioningType            : MCS
ScheduledTimeInUtc          :
SecurityCheckFailedUpgrades :
SessionSupport              : SingleSession
StateId                     :
SuccessfulUpgrades          :
TotalMachines               :
Uid                         : 30
UpgradeState                : UpgradeAvailable
UpgradeType                 : LTSR
UpgradeVersion              :
Uuid                        : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```

Si vous constatez que la valeur de `UpgradeState` est `Unknown`, l'une des raisons possibles est que l'agent de mise à niveau Citrix VDA installé sur le VDA n'a pas signalé la version au service de mise à jour de VDA. Vous pouvez utiliser l'applet de commande `Get-VusComponentVersion` pour vérifier si le VDA a signalé les versions des composants.

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

Si aucun résultat n'est affiché, vérifiez les points suivants :

- Le VDA fait partie d'un catalogue et d'un groupe de mise à disposition.
- L'agent de mise à niveau du VDA est installé sur le VDA et en cours d'exécution. Si nécessaire, essayez de redémarrer l'agent.

Remarque : si vous n'obtenez pas de résultat, collectez les traces du Centre de diagnostic Citrix lors du redémarrage de l'agent de mise à niveau du VDA et résolvez les problèmes.

- Planifiez les mises à niveau du VDA. Avant de commencer, tenez compte des points suivants :
  - `DurationInHours` : vous permet de fournir la durée en heures du processus de mise à niveau. Les VDA du catalogue seront mis en mode de maintenance. Le programme

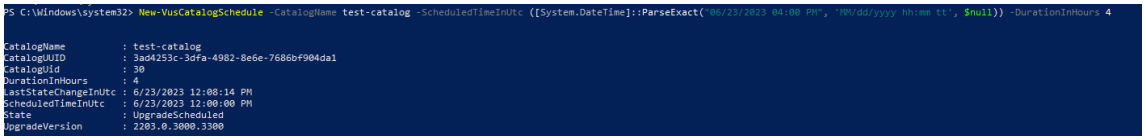
d'installation du VDA sera téléchargé et la mise à niveau sera effectuée sur chaque VDA. Prévoyez une durée plus longue si le catalogue contient de nombreux VDA.

- `UpgradeNow` : utilisez ce commutateur pour planifier une mise à niveau immédiatement ou configurez `ScheduledTimeInUtc`.
- `ScheduledTimeInUtc` : vous permet de planifier une mise à niveau pour une date et une heure spécifiques.

Exemple :

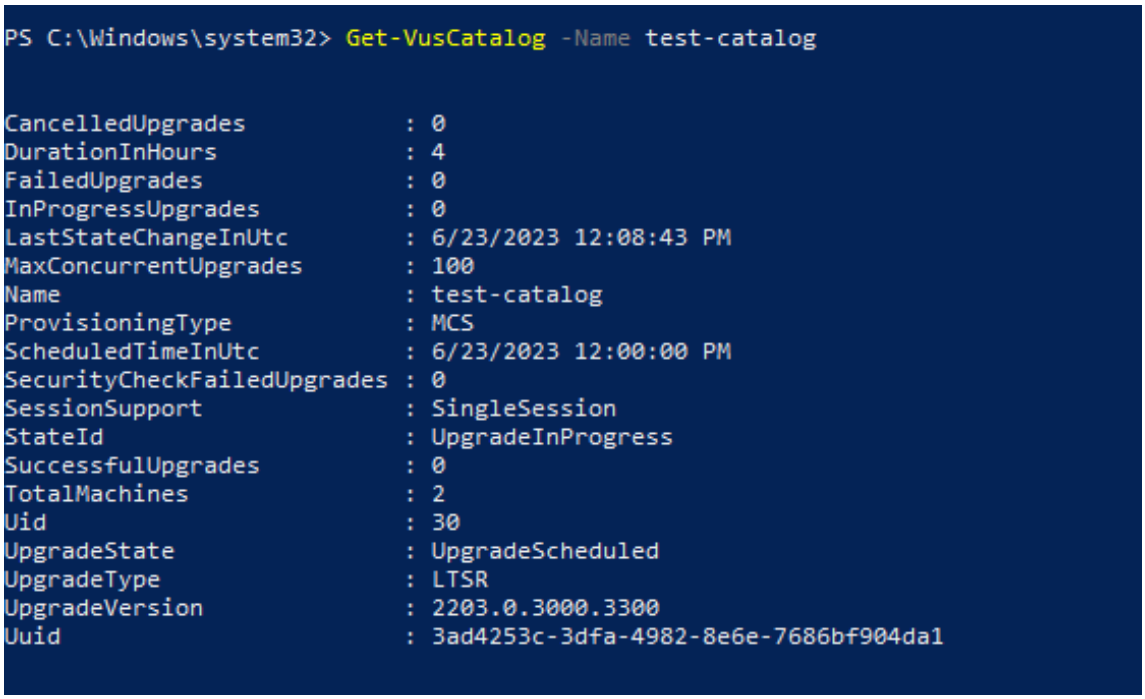
```
- New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc
  ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd
  /yyyy hh:mm tt', $null))-DurationInHours 4
```

Vous pouvez utiliser `CatalogName`, `Uid` et `Uuid` pour planifier la mise à niveau.

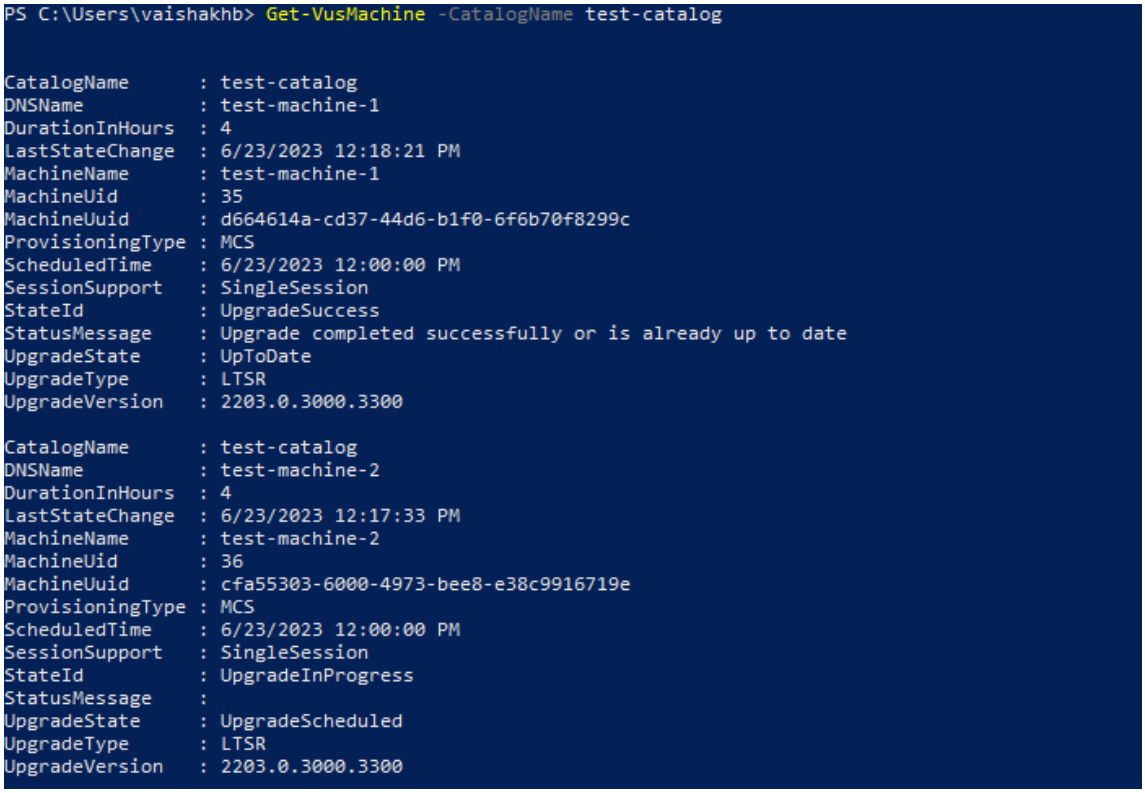


- Vérifiez l'état de la mise à niveau. Utilisez l'applet de commande `Get-VusCatalog` ou `Get-VusMachine` pour vérifier régulièrement l'état de mise à niveau du VDA. Utilisez `MachineUuid`, `MachineUid` et `MachineName` pour filtrer les VDA.

  Exemple :
  `-Get-VusCatalog -Name test-catalog`



Utilisez `Get-VusMachine` pour voir l'état de mise à niveau du VDA de chaque machine d'un catalogue.



Si Personal vDisk est installé sur le VDA

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 1912 LTSR ou ultérieure.

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**. 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 n'importe quelle version), PvD a été installé.
- 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.

Que faire

Si le programme d'installation du VDA ne détecte pas le composant PvD dans le VDA actuellement installé, la mise à niveau se poursuit comme d'habitude.

Si le programme d'installation détecte du composant PvD dans le VDA actuellement installé :

- **Interface graphique :** la mise à niveau s'interrompt. Un message vous demande si vous souhaitez supprimer automatiquement le composant non pris en charge. Si vous cliquez sur **OK**, le composant est supprimé automatiquement et la mise à niveau se poursuit.
- **CLI :** La commande échoue si le programme d'installation détecte le composant PvD. Pour éviter l'échec de la commande, incluez l'option suivante dans la commande : `/remove_pvd_ack`.

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. Veuillez noter que le programme de support étendu pour XenApp et XenDesktop 7.15 LTSR ne s'applique pas aux VDA utilisés avec Citrix DaaS. Pour plus d'informations, consultez le Guide client du support étendu dans le centre de connaissances du support Citrix.

Systèmes d'exploitation antérieurs

L'article Configuration système requise répertorie les systèmes d'exploitation Windows pris en charge pour les VDA de version actuelle.

- Pour les VDA LTSR, consultez l'article sur la configuration système requise pour votre version LTSR.
- Pour les VDA Linux, consultez la documentation Linux Virtual Delivery Agent.

Pour les machines Windows dont les systèmes d'exploitation ne sont plus pris en charge et ne permettent pas d'installer le dernier VDA, vous disposez des options suivantes.

Pour les environnements non-WVD :

- Créez une nouvelle image de la machine sur une version prise en charge de Windows, puis installez le nouveau VDA.
- Si réimager la machine n'est pas une option mais que vous voulez mettre à niveau le système d'exploitation, désinstallez le VDA avant la mise à niveau du système d'exploitation. Sinon, le VDA sera dans un état non pris en charge. Après la mise à niveau du système d'exploitation, installez le nouveau VDA.
- Si la version 7.15 LTSR est installée sur la machine (et vous tentez d'installer une version plus récente), un message vous informe que vous utilisez la dernière version prise en charge.
- Si une version antérieure à LTSR 7.15 est installée sur la machine, un message vous renvoie à l'article CTX139030 pour plus d'informations. Vous pouvez télécharger la version VDA 7.15 LTSR à partir du site Web de Citrix.

Migrer la configuration vers Citrix Cloud

March 30, 2024

Pourquoi utiliser la configuration automatisée

Les administrateurs informatiques chargés d'environnements volumineux ou complexes trouvent souvent les migrations fastidieuses. Ils finissent souvent par écrire leurs propres outils pour accomplir cette tâche avec succès, car ils ont tendance à être spécifiques à leurs cas d'utilisation.

Citrix souhaite faciliter ce processus en automatisant le processus de migration à l'aide de l'outil de configuration automatisée. Les administrateurs peuvent facilement tester les configurations actuelles dans Citrix Cloud et profiter des avantages offerts par Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) tout en conservant leurs environnements actuels *intacts*. Il n'y a pas non plus d'impact sur l'utilisateur final, car la configuration automatisée fonctionne de manière transparente en arrière-plan. Ces avantages incluent une charge administrative réduite lorsque Citrix gère une partie du back-end et du plan de contrôle, des mises à jour automatiques et personnalisables des composants Citrix Cloud, etc.

Citrix utilise la configuration standard du secteur comme code pour fournir un mécanisme permettant d'automatiser les processus de migration. La configuration automatisée détecte et exporte un ou plusieurs sites locaux sous la forme d'un ensemble de fichiers de configuration. La configuration de ces fichiers peut ensuite être importée dans Citrix DaaS.

La configuration automatisée permet également aux administrateurs de fusionner plusieurs sites locaux en un seul site, tout en évitant les collisions de noms. Les administrateurs peuvent contrôler si la configuration sur site ou dans le cloud contrôle les ressources.

La configuration automatisée n'est pas seulement un outil de migration ponctuelle, mais elle peut également automatiser votre configuration quotidienne dans Citrix Cloud. Le déplacement de votre configuration Citrix DaaS peut être bénéfique pour de nombreuses raisons :

- Synchronisation de votre site de la phase de test ou de pré-production à la production
- Sauvegarde et restauration de votre configuration
- Atteindre les limites de ressources
- Migration d'une région à une autre

La vidéo suivante (*2 minutes*) fournit un aperçu rapide de la configuration automatisée.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Pour plus d'informations sur la configuration automatisée, consultez Proof of Concept: Automated Configuration Tool sur Tech Zone.

Pour en savoir plus sur le déplacement de votre déploiement et la préparation de votre configuration locale pour la migration, consultez Deployment Guide: Migrating Citrix Virtual Apps and Desktops from on-premises to Citrix Cloud sur Tech Zone.

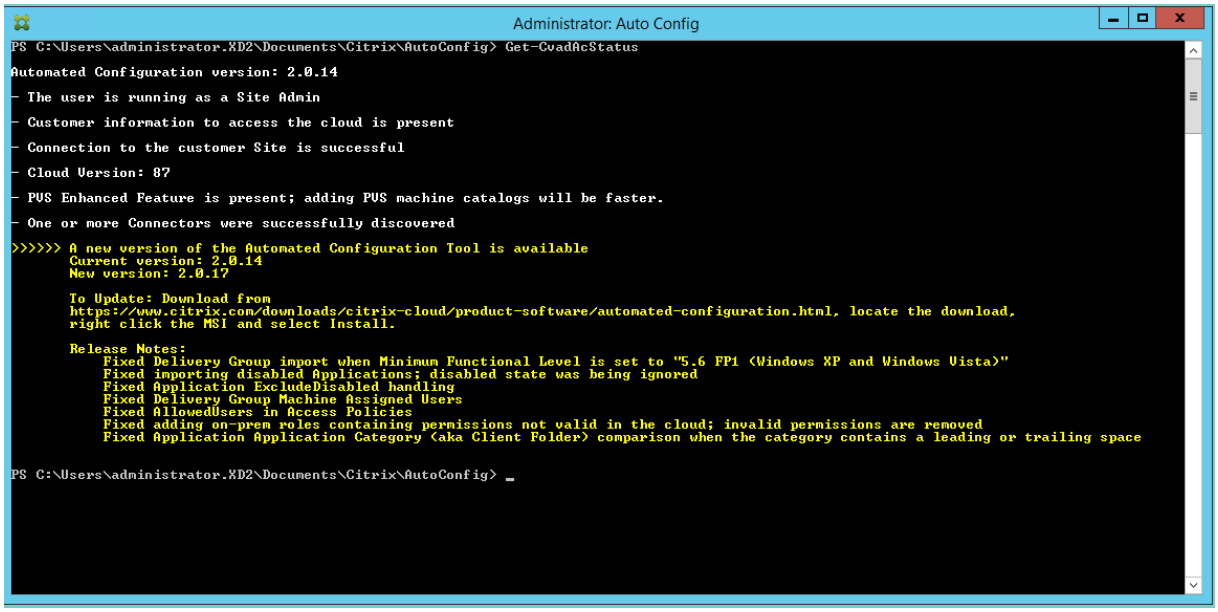
Télécharger l'outil de configuration automatisée

Téléchargez et installez l'outil de configuration automatisée à partir de Téléchargements Citrix.

> **Important :**
>
> Pour éviter les erreurs de fonctionnalité, utilisez toujours la dernière version disponible de la configuration automatisée.

Mise à niveau de la configuration automatisée

Lorsque vous exécutez des applets de commande qui accèdent au cloud dans Configuration automatisée, l'outil vous avertit lorsqu'une version plus récente est disponible.



Vous pouvez vous assurer que vous disposez de la dernière version en suivant les étapes ci-dessous :

1. Double-cliquez sur l'icône **Config automatique**. Une fenêtre PowerShell s'affiche.
2. Exécutez la commande suivante pour vérifier votre numéro de version.

   ```
   Get-CvadAcStatus
   ```

3. Vérifiez la version de votre outil par rapport à la version répertoriée dans l'alerte ou sur Téléchargements Citrix. La dernière version de l'outil se trouve sur cette page.

4. Téléchargez et installez la dernière version de l'outil. Il n'est *pas* nécessaire de désinstaller l'ancienne version pour mettre à niveau Configuration automatisée.

> **Remarque :**
>
> L'alerte apparaît chaque fois que vous exécutez une cmdlet qui accède au cloud. Pour plus d'informations sur les applets de commande, consultez Applets de commande de l'outil de configuration automatisée.

Limitations connues

- Les catalogues de machines provisionnés via Machine Creation Services requièrent une attention particulière. Pour plus d'informations sur MCS, consultez Présentation de la migration des catalogues provisionnés Machine Creation Services.

Objets pris en charge pour la migration

La configuration automatisée prend en charge le déplacement de la configuration des composants suivants :

- Balises
- Administrateur délégué
  - Étendues
  - Rôles
- Connexions hôte
  - Un pool de ressources unique
  - Étendues d'administration
- Catalogues de machines
  - Étendues d'administration
  - Machines
  - Accès PC distant, physiques, groupées, provisionnées, MCS, attribuées
- StoreFront
- Groupes de mise à disposition
  - Stratégie d'accès
  - Association des étendues administrateur
  - Stratégie d'accès aux applications
  - Stratégie d'attribution

  - Stratégie de droit/bureau
  - Programmations d'alimentation
  - Attente de session
  - Pré-démarrage de session
  - Programmes de redémarrage
  - Balises
- Groupes d'applications
  - Association des étendues administrateur
  - Groupes de mise à disposition
  - Utilisateurs et groupes
- Applications
  - Dossiers d'application
  - Icônes
  - Applications
  - FTA configurées par le broker
  - Balises
- Stratégies de groupe
- Préférences de zone utilisateur

Ordre de migration des composants

Les composants et leurs dépendances sont répertoriés ici. Les dépendances d'un composant doivent être en place avant qu'il puisse être importé ou fusionné. Si une dépendance est manquante, cela peut entraîner l'échec de la commande d'importation ou de fusion. La section **Fixups** du fichier journal affiche les dépendances manquantes en cas d'échec d'une importation ou d'une fusion.

1. Balises
   - Aucune pré-dépendance
2. Administrateur délégué
   - Aucune pré-dépendance
3. Connexions hôte
   - Informations de sécurité dans CvadAcSecurity.yml
4. Catalogues de machines
   - Machines présentes dans Active Directory

- Connexions hôte
- Balises

5. StoreFront
6. Groupes de mise à disposition
    - Machines présentes dans Active Directory
    - Utilisateurs présents dans Active Directory
    - Catalogues de machines
    - Balises
7. Groupes d'applications
    - Groupes de mise à disposition
    - Balises
8. Applications
    - Groupes de mise à disposition
    - Groupes d'applications
    - Balises
9. Stratégies de groupe
    - Groupes de mise à disposition
    - Balises
10. Préférences de zone utilisateur

Conditions préalables communes

Voici quelques prérequis communs qui sont nécessaires au bon fonctionnement de la configuration automatisée. Ces conditions préalables sont utilisées à la fois dans les migrations sur site vers cloud et cloud vers cloud.

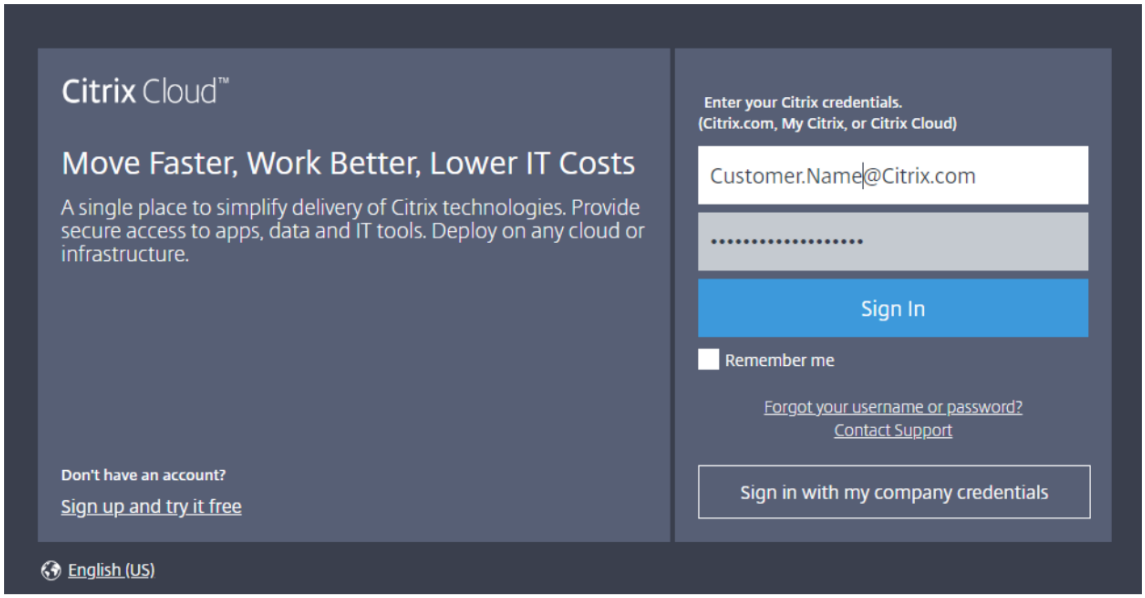
Génération des ID client et de la clé secrète

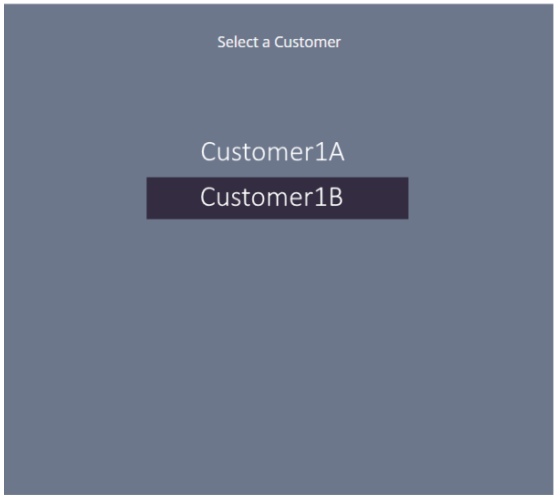
Avant de commencer votre migration à l'aide de la configuration automatisée, vous avez besoin de votre ID client Citrix Cloud et vous devez créer un ID client et une clé secrète pour importer votre configuration dans Citrix Cloud. Toutes les applets de commande accédant au cloud nécessitent ces valeurs.

Les étapes suivantes vous permettent de récupérer l'ID client et de créer l'ID client et la clé secrète.

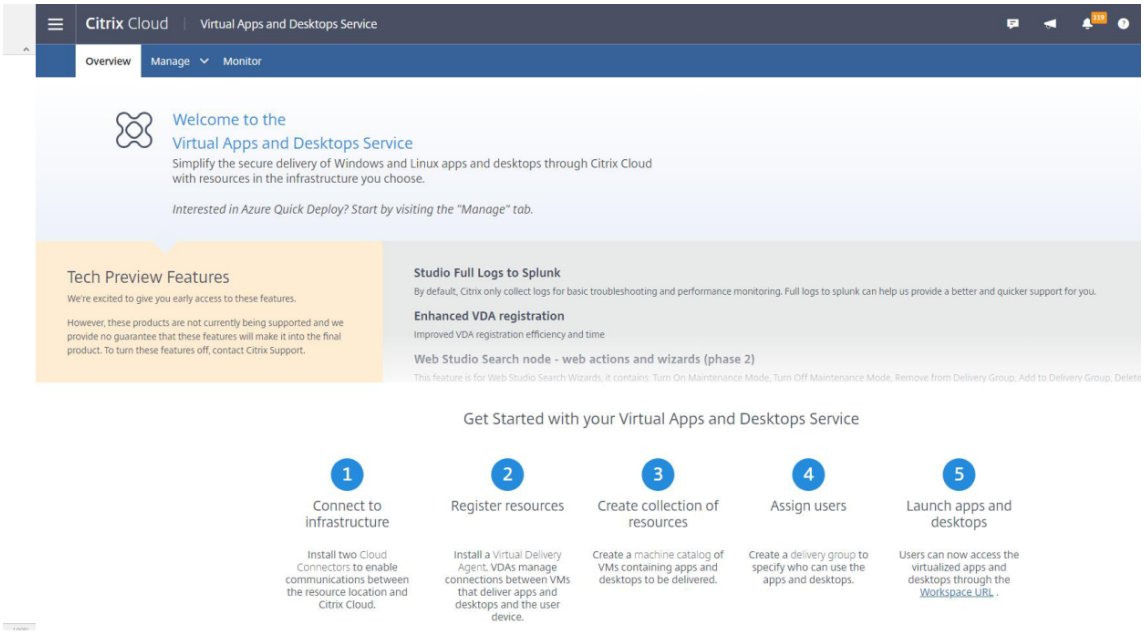
Pour récupérer l'**ID client**, procédez comme suit :

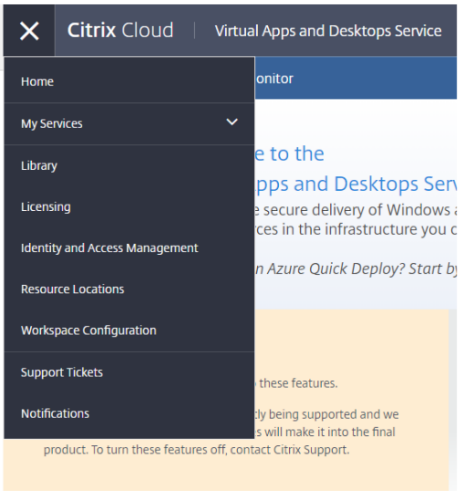
1. Connectez-vous à votre compte Citrix Cloud et sélectionnez le client.



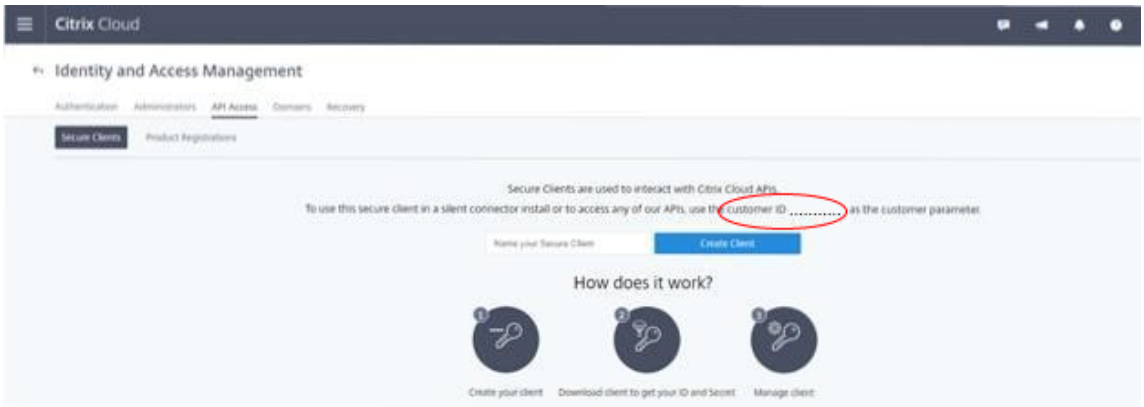


2. Cliquez sur le menu hamburger, puis sélectionnez **Gestion des identités et des accès** dans le menu déroulant.



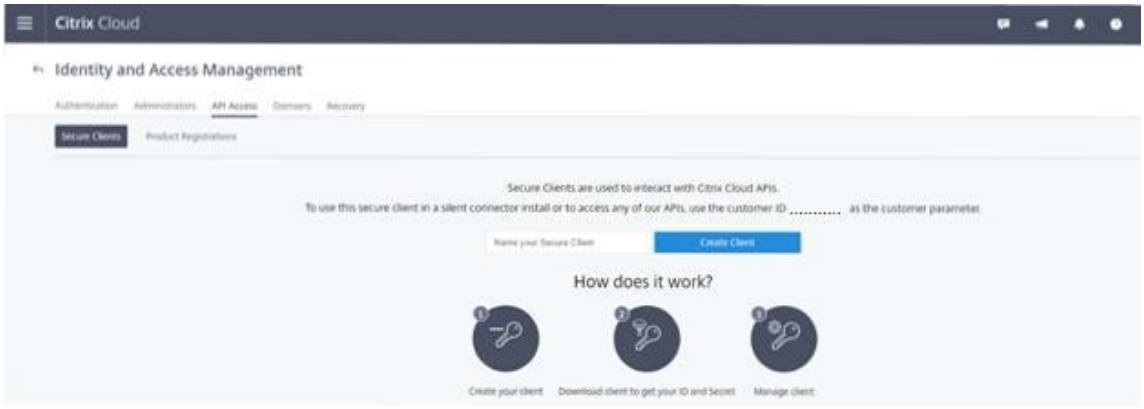


3. L'**ID client** se trouve sur la page **Gestion des identités et des accès**.

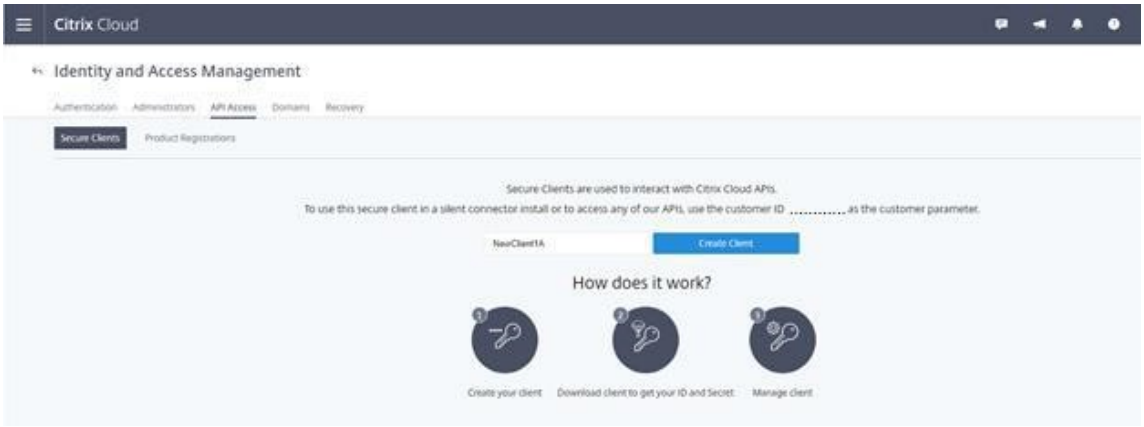


Pour récupérer l'**ID client** et la **clé secrète** :

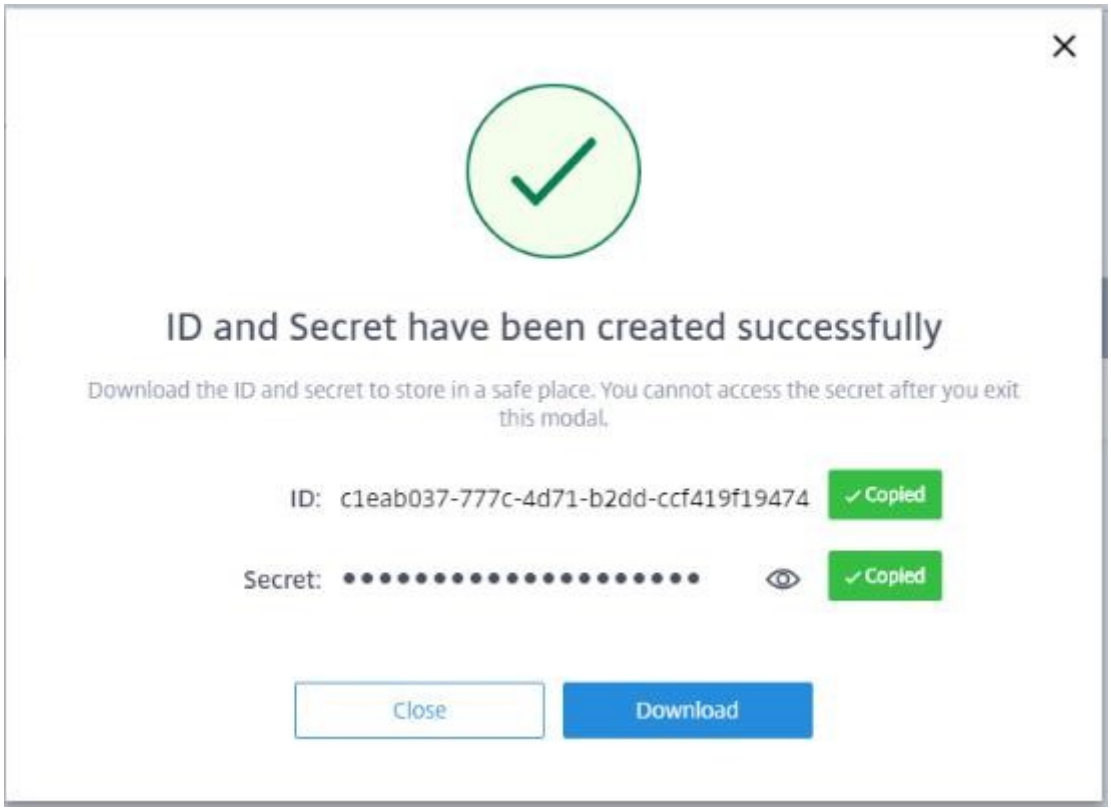
1. Sur la page **Gestion des identités et des accès**, cliquez sur l'onglet **Accès aux API**.



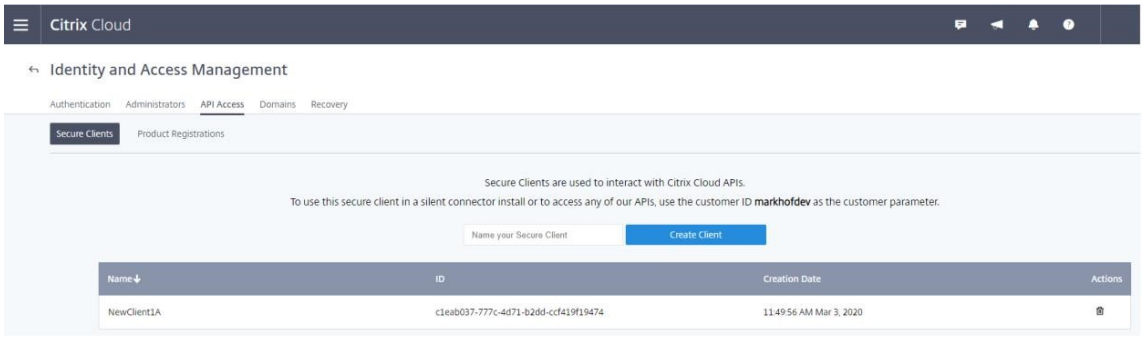
2. Entrez un nom dans la zone. Ce nom est utilisé pour différencier plusieurs ID client et clés secrètes. Cliquez sur **Créer un client** pour créer l'ID client et la clé secrète.



3. La boîte de dialogue suivante s'affiche lorsque vous avez réussi à créer l'ID client et la clé secrète. Veillez à copier les deux valeurs dans un emplacement sécurisé et de télécharger le fichier .csv contenant ces informations. Le fichier .csv peut être utilisé pour créer le fichier CustomerInfo.yml.



4. L'ID client et la clé secrète sont créés avec succès.



Placez ces valeurs dans un emplacement sécurisé et ne les partagez qu'avec les membres de l'entreprise de confiance qui ont besoin d'accéder à l'outil ou aux API Rest cloud. L'ID client et la clé secrète n'expirent pas. S'ils sont compromis, supprimez-les immédiatement à l'aide de l'icône **Corbeille** et créez-en de nouveaux.

> **Remarque :**
>
> La clé secrète ne peut pas être récupérée si elle est perdue ou oubliée ; un nouvel ID client et une clé secrète doivent être créés.

Remplissage du fichier d'informations client

L'utilisation du fichier CustomerInfo.yml élimine la nécessité de fournir des paramètres d'informations client lors de l'exécution de chaque applet de commande. Toutes les informations client peuvent être remplacées à l'aide des paramètres de l'applet de commande.

Créez le fichier CustomerInfo.yml à l'aide de l'applet de commande `New-CvadAcCustomerInfoFile` .

> **Important :**
>
> Ne modifiez pas manuellement le fichier CustomerInfo.yml. Cela peut entraîner des erreurs de mise en forme.

`New-CvadAcCustomerInfoFile` comporte les paramètres requis suivants.

- CustomerId : ID client.
- ClientId : ID client créé sur Citrix Cloud.
- Secret : secret du client créé sur Citrix Cloud.

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId 6813EEA6
-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaw==
```

Vous pouvez également créer le fichier CustomerInfo.yml à l'aide du paramètre `SecurityCsvFileSpec` qui pointe vers le fichier security.csv téléchargé. Vous devez également spécifier le CustomerID.

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:\Users\my_user_name
\downloads/security.csv -CustomerId markhof123
```

Mettez à jour le fichier CustomerInfo.yml à l'aide de l'applet de commande `Set-CvadAcCustomerInfoFile` . L'applet de commande modifie uniquement l'ID client.

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

Voici un exemple de fichier CustomerInfo.yml.

```
# Created/Updated on 2020/01/29 16:46:47
CustomerId: 'markhof123'
ClientId: '6713FEA6-46CC-4F8A-BC71-539F2DDK5384'
Secret: 'TwBLaaabbbaaaaaaaaaaw=='
Environment: Production
AltRootUrl: ''
StopOnError: False
AlternateFolder: ''
Locale: 'en-us'
Editor: 'C:\Program Files\Notepad++\notepad++.exe'
Confirm: True
DisplayLog: True
```


Remplissage du fichier de mappage de zones

Une zone locale est l'équivalent de l'emplacement des ressources cloud. Contrairement aux autres composants du site, vous ne pouvez pas importer automatiquement la zone locale vers le cloud. Elle doit être mappée manuellement à l'aide du fichier ZoneMapping.yml. Des échecs d'importation peuvent se produire si le nom de la zone n'est pas associé à un nom d'emplacement de ressources existant.

Pour les sites locaux n'ayant qu'une zone et les sites cloud qu'un seul emplacement de ressources, l'outil Configuration automatisée établit l'association correcte, éliminant ainsi la nécessité de gérer manuellement le fichier ZoneMapping.yml.

Pour les sites locaux comportant plusieurs zones ou sites cloud ayant plusieurs emplacements de ressources, le fichier ZoneMapping.yml doit être mis à jour manuellement pour refléter le mappage correct des zones locales aux emplacements de ressources cloud. Cette opération doit être effectuée avant de tenter une opération d'importation dans le cloud.

Le fichier ZoneMapping.yml se trouve sous *%HOMEPATH%\Documents\Citrix\AutoConfig*. Le contenu du fichier .yml est un dictionnaire avec le nom de la zone comme clé et le nom de l'emplacement de ressources comme valeur.

À titre d'exemple, un site Citrix Virtual Apps and Desktops local avec une zone principale appelée « Zone-1 » et une zone secondaire appelée « Zone-2 » est migré vers un déploiement Citrix DaaS avec deux emplacements de ressources cloud nouvellement créés appelés « Cloud-RL-1 » et « Cloud-RL-2 ». Dans ce cas, le fichier ZoneMapping.yml serait configuré comme suit :

```
1               Zone-1: Cloud-RL-1
2
3               Zone-2: Cloud-RL-2
```

> **Remarque :**
>
> Les deux-points et le nom de l'emplacement de ressources doivent être séparés par un espace. Si des espaces sont utilisés dans le nom de la zone ou de l'emplacement des ressources, placez le nom entre guillemets.

Connexions hôte

Les connexions hôtes et les hyperviseurs associés peuvent être exportés et importés à l'aide de la configuration automatisée.

L'ajout d'un hyperviseur à une connexion hôte nécessite des informations de sécurité spécifiques au type d'hyperviseur. Ces informations ne peuvent pas être exportées à partir du site local pour des raisons de sécurité. Vous devez fournir les informations manuellement afin que l'outil de configu-

ration automatisée puisse importer avec succès les connexions hôte et les hyperviseurs sur le site cloud.

Le processus d'exportation crée le fichier CvadAcSecurity.yml sous *%HOMEPATH%\Documents\Citrix\AutoConfig* contenant des espaces réservés pour chaque élément de sécurité nécessaire au type d'hyperviseur spécifique. Vous devez mettre à jour le fichier CvadAcSecurity.yml avant l'importation dans le site cloud. Les mises à jour de l'administrateur sont conservées pour plusieurs exportations avec de nouveaux espaces réservés de sécurité ajoutés au besoin. Les éléments de sécurité ne sont jamais supprimés. Pour plus d'informations, voir Mettre à jour manuellement le fichier CvadAcSecurity.yml

```
            HostConn1:
            ConnectionType: XenServer
            UserName: root
            PasswordKey: rootPassword
            HostCon2:
            ConnectionType: AWS
            ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH
            SecretKey: TwBLaaaaaaaaaaaaaaaaw==
            Region: East
```

Informations de sécurité par hyperviseur La liste suivante répertorie les informations de sécurité requises pour chaque type d'hyperviseur.

- XenServer, Hyper-V, VMware
  - Nom d'utilisateur
  - Mot de passe en texte clair
- Microsoft Azure
  - ID d'abonnement
  - ID de l'application
  - Secret d'application
- Amazon Web Services
  - ID du compte de service
  - Secret d'application
  - Région

Considérations de sécurité particulières Toutes les informations de sécurité sont saisies sous forme de texte clair. Si le texte clair n'est pas recommandé, les connexions hôtes et les hyperviseurs associés peuvent être créés manuellement à l'aide de l'interface **Gérer > Configuration complète**. Les noms de connexions hôte et d'hyperviseur doivent correspondre exactement à leurs homologues

locaux afin que les catalogues de machines qui utilisent les connexions hôtes soient importés avec succès.

Activation des sites

Le Delivery Controller dans les sites locaux et dans le cloud contrôle les ressources telles que la négociation des bureaux, des applications et le redémarrage des machines. Des problèmes se produisent lorsqu'un ensemble commun de ressources est contrôlé par deux sites ou plus. Une telle situation peut se produire lors de la migration d'un site local vers un site cloud. Il est possible pour les Delivery Controller locaux et cloud de gérer le même ensemble de ressources. Avec une telle double gestion, les ressources peuvent devenir indisponibles et ingérables, ce qui peut être difficile à diagnostiquer.

L'activation de site vous permet de contrôler l'endroit où le site actif est contrôlé.

L'activation du site est gérée en utilisant le mode de maintenance du groupe de mise à disposition Les groupes de mise à disposition sont placés en mode maintenance lorsque le site est inactif. Le mode de maintenance est supprimé des groupes de mise à disposition pour les sites actifs.

L'activation du site n'affecte pas et ne gère pas l'enregistrement des VDA ni les catalogues de machines.

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

Toutes les applets de commande prennent en charge le `ExcludeByName` filtrage et `IncludeByName` . Ce paramètre vous permet de sélectionner les groupes de mise à disposition dont le mode de maintenance peut être modifié. Les groupes de mise à disposition peuvent être modifiés de manière sélective si nécessaire.

Importation et transfert du contrôle vers le cloud

Vous trouverez ci-dessous une description générale sur la façon d'importer et de transférer le contrôle du site local vers le site cloud.

1. Exportez et importez le site local dans le cloud. Assurez-vous que le paramètre `-SiteActive` n'est présent sur aucune des applets de commande d'importation. Le site local est actif et le site cloud inactif. Par défaut, les groupes de mise à disposition de sites cloud sont en mode de maintenance.
2. Vérifiez le contenu et la configuration du cloud.
3. Pendant les heures creuses, définir le site local sur inactif. Le paramètre `-SiteActive` doit être absent. Tous les groupes de mise à disposition sur site sont en mode de maintenance.
    - `Set-CvadAcSiteActiveStateOnPrem`

4. Définissez le site cloud sur actif. Le paramètre `–SiteActive` doit être présent. Aucun groupe de mise à disposition de site cloud n'est en mode de maintenance.
   - `Set-CvadAcSiteActiveStateCloud –SiteActive`
5. Vérifiez que le site cloud est actif et que le site local est inactif.

Transfert du contrôle vers le site local

Pour transférer le contrôle du site cloud vers le site local :

1. Pendant les heures creuses, définissez le site cloud sur inactif. Tous les groupes de mise à disposition de sites cloud sont en mode de maintenance.
   - `Set-CvadAcSiteActiveStateCloud`
2. Définissez le site local sur actif. Aucun groupe de mise à disposition local n'est en mode de maintenance.
   - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

Informations supplémentaires sur l'activation du site

- Si l'alimentation d'aucune machine n'est gérée et qu'il n'y a pas de programme de redémarrage (ce qui signifie généralement qu'il n'y a pas de connexion hôte non plus), tous les groupes de mise à disposition cloud peuvent être importés comme actifs. Ajoutez `-SiteActive` à `Merge-CvadAcToSite`/`Import-CvadAcToSite` ou exécutez `Set-CvadAcSiteActiveStateCloud -SiteActive` après l'importation.
- Si l'alimentation des machines est gérée ou si des redémarrages sont programmés, un processus différent est nécessaire. Par exemple, lorsque vous passez d'un site local au cloud dans cette situation, définissez le site local sur inactif à l'aide de `Set-CvadAcSiteActiveStateOnPrem`. Ensuite, définissez le site cloud sur actif à l'aide de `Set-CvadAcSiteActiveStateCloud -SiteActive`.
- Les applets de commande `Set-CvadAcSiteActiveStateCloud` et `Set-CvadAcSiteActiveStat` sont également utilisées pour inverser le processus. Par exemple, exécutez `Set-CvadAcSiteActiveStateCloud` sans le paramètre `-SiteActive`, puis exécutez `Set-CvadAcSiteActiveStateOnPrem` avec le paramètre `-SiteActive`.

Présentation de la migration des catalogues provisionnés Machine Creation Services

> **Remarque :**
>
> Cette fonctionnalité n'est disponible que sur les versions 3.0 et ultérieures. Vérifiez votre version en utilisant `Get-CvadAcStatus` dans la configuration automatisée.

Les catalogues Machine Creation Services (MCS) créent deux types de catalogues différents :

- Lorsque les modifications apportées à une machine sont perdues ou annulées (généralement avec OS de serveur, où les applications sont publiées), il s'agit d'un cas d'utilisation VDI regroupé/multi-session
- Lorsque les modifications apportées à une machine sont conservées lors du redémarrage (généralement OS client avec un utilisateur dédié), il s'agit d'un cas d'utilisation VDI statique

Le type de catalogue peut être confirmé dans le nœud de catalogue de Citrix Studio et en examinant la valeur « Données utilisateur » du catalogue.

> **Remarque :**
>
> MCS ne peut pas être sauvegardé depuis le cloud à l'aide de la configuration automatisée.

Catalogues VDI et multi-sessions regroupés

Les catalogues avec la valeur « Données utilisateur : Abandonner » sont des catalogues VDI regroupés et ne peuvent migrer que l'image principale et la configuration. Les machines virtuelles de ces catalogues ne sont pas migrées. Cela s'explique par le fait que le cycle de vie de la machine virtuelle est maintenu par le site à partir duquel vous importez, ce qui signifie que chaque fois que les machines sont allumées, leur état peut changer. Cela rend l'importation impossible car les données d'importation des machines virtuelles sont rapidement désynchronisées.

Lorsque vous migrez ces catalogues à l'aide de l'outil, il crée des métadonnées de catalogue et lance la création de l'image principale, mais aucune machine n'est importée.

Comme ce processus peut prendre un certain temps à être créé en fonction de la taille de l'image principale, la commande d'importation de l'outil démarre uniquement la création du catalogue MCS et n'attend pas qu'elle se termine. Une fois l'importation terminée, surveillez la progression de la création du catalogue à l'aide de l'interface de gestion Configuration complète dans le déploiement cloud.

Une fois l'image principale créée, vous pouvez provisionner des machines. Les considérations relatives à la capacité doivent être prises en compte, car votre utilisation sur site consomme de la capacité.

Tous les autres objets (groupes de mise à disposition, applications, stratégies, etc.) qui utilisent ce catalogue peuvent être importés sans attendre la création de l'image principale. Lorsque la création du

catalogue est terminée, les machines peuvent être ajoutées au catalogue importé, puis les utilisateurs peuvent lancer leurs ressources.

> **Remarque :**
>
> Utilisez les mêmes commandes disponibles dans l'outil pour migrer les catalogues et tous les autres objets.

Catalogues VDI statiques

> **Remarque :**
>
> Comme cette opération importe des détails de bas niveau qui sont stockés dans la base de données, ce processus doit être exécuté à partir d'une machine disposant d'un accès à la base de données.

Les catalogues VDI statiques migrent l'image principale, les configurations et toutes les machines virtuelles. Contrairement au cas d'utilisation de VDI regroupés, aucune image n'a besoin d'être créée.

Les VDA doivent être dirigés vers le connecteur pour pouvoir s'enregistrer dans le cloud.

Reportez-vous à la section Activation des sites pour activer le site cloud, afin que la planification du redémarrage, la gestion de l'alimentation et les autres éléments soient contrôlés par le cloud.

Une fois la migration terminée, si vous souhaitez supprimer ce catalogue de votre site local, vous devez choisir de quitter la machine virtuelle et le compte AD. Sinon, ils sont supprimés et le site cloud pointe vers la machine virtuelle supprimée.

Mettre à jour les balises MCS pour détecter les ressources orphelines après la migration

Après avoir migré une configuration locale vers un site cloud ou votre configuration cloud vers un autre site cloud, vous devez mettre à jour les balises d'identification du site MCS en cas de machines virtuelles persistantes afin que les ressources orphelines puissent être détectées correctement. Pour cela, utilisez la commande PowerShell `Set-ProvResourceTags`. Actuellement, cette fonctionnalité est applicable à Azure.

Voici le détail des étapes :

1. Mettez à jour les balises d'identification du site MCS à partir du nouveau site Citrix à l'aide de la commande PowerShell `Set-ProvResourceTags`. Par exemple :

```
Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <
    String>] [-VMBatchSize XX] [-ResourceType XX]
<!--NeedCopy-->
```


Ou

```
Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <
    String>] [-VMBatchSize XX] [-ResourceType XX]
<!--NeedCopy-->
```

Les détails des paramètres sont les suivants :

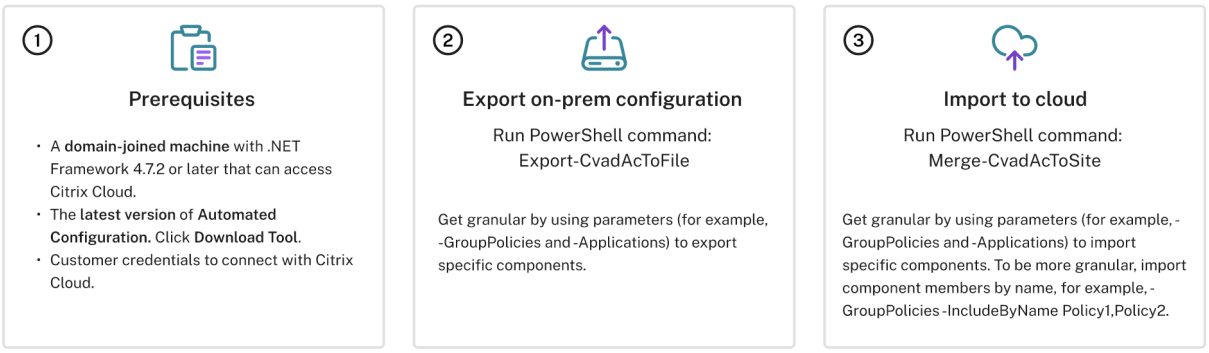
- `ProvisioningSchemeUid` ou `ProvisioningSchemeName` est un paramètre obligatoire.
- `VMName` est un paramètre facultatif. Si aucun paramètre `VMName` n'est spécifié, les balises de toutes les machines virtuelles de ce catalogue de machines sont mises à jour.
- `VMBatchSize` est un paramètre facultatif permettant de diviser toutes les machines virtuelles en lots. Si aucun paramètre `VMBatchSize` n'est spécifié, la valeur par défaut (10) est appliquée. La plage est comprise entre 1 et 60.
- `ResourceType` peut être l'un des types suivants :
  - `MachineCatalog` : pour mettre à jour les balises des ressources du catalogue de machines.
  - `VirtualMachine` : pour mettre à jour les balises des ressources liées à la VM.
  - `All` : (ResourceType par défaut) pour mettre à jour les balises du catalogue de machines et des ressources associées à la VM.

Migration d'une configuration locale vers le cloud

May 17, 2024

La configuration automatisée vous permet d'automatiser le déplacement de votre configuration locale vers un site cloud.

L'image suivante présente une vue de haut niveau de ce que la configuration automatisée peut faire pour migrer votre configuration vers le cloud.



Conditions préalables à la migration de votre configuration

Pour *exporter* votre configuration à partir de Citrix Virtual Apps and Desktops, vous avez besoin de la configuration suivante :

- Citrix Virtual Apps and Desktops : version actuelle et précédente ou Citrix Virtual Apps and Desktops, XenApp et XenDesktop LTSR : toutes les versions
- Une machine jointe au domaine avec .NET Framework 4.7.2 ou version ultérieure et le kit SDK Citrix PowerShell. Ceci est automatiquement installé sur le Delivery Controller. (Pour s'exécuter sur une machine autre que le Delivery Controller local, Citrix Studio doit être installé, car Studio installe les composants logiciels enfichables PowerShell appropriés. Le programme d'installation de Studio se trouve sur le support d'installation de Citrix Virtual Apps and Desktops.)

Pour *importer* votre configuration dans Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), vous avez besoin de la configuration suivante :

- Une machine avec accès à Citrix Cloud. Il n'est pas nécessaire que ce soit un Delivery Controller ou une machine jointe à un domaine.
- Citrix DaaS provisionné.
- Emplacement de ressources actif, avec Connector installé et joint au même domaine que l'installation locale.
- La connectivité aux sites accédant à Citrix Cloud doit être autorisée et disponible. Pour plus d'informations, consultez la section Configuration requise pour le système et la connectivité.

> **Remarque :**
>
> La configuration automatisée ne peut pas être installée sur un système Cloud Connector.

Exportation de votre configuration locale Citrix Virtual Apps and Desktops

> **Important :**
>
> - Vous devez inclure votre fichier CustomerInfo.yml avec vos ID client et les informations de clé secrète. Pour savoir comment récupérer vos ID client et de votre clé secrète, reportez-vous à la section Génération des ID client et de la clé secrète. Pour plus d'informations sur l'ajout de ces informations au fichier CustomerInfo.yml, reportez-vous à la section Remplissage du fichier d'informations client.
> - Le fichier ZoneMapping.yml doit inclure des informations qui mappent votre zone locale aux emplacements de ressources dans le cloud. Pour savoir comment mapper vos zones, reportez-vous à la section Remplissage du fichier de mappage de zones.
> - Si vous disposez de connexions hôtes, vous devez entrer les informations correspondantes dans le fichier CvadAcSecurity.yml.

1. Installez la configuration automatisée.
2. Double-cliquez sur l'icône **Config automatique**. Une fenêtre PowerShell s'affiche.
3. Exécutez la commande suivante pour exporter tous les composants. L'exportation de votre configuration locale *ne* la modifie en aucune façon.

   ```
   Export-CvadAcToFile
   ```

Après avoir exécuté une applet de commande pour la première fois, un dossier d'exportation contenant les journaux et les fichiers de configuration .yml est créé. Le dossier se trouve sous *%HOMEPATH%\Documents\Citrix\AutoConfig*. Chaque exportation successive crée un sous-dossier. Le dossier parent *%HOMEPATH%\Documents\Citrix\AutoConfig* contient toujours les fichiers exportés au cours de l'exportation la plus récente.

> **Remarque :**
>
> Si la configuration automatisée n'est pas installée sur le Delivery Controller, exécutez `import-module Citrix.AutoConfig.Commands` avant d'utiliser l'outil via PowerShell. Cette étape n'est pas nécessaire si vous ouvrez Configuration automatisée à l'aide de l'icône **Config automatique**.

Si vous rencontrez des erreurs ou des exceptions, consultez la section **Fixups** du fichier journal.

Importation de votre configuration vers Citrix DaaS

> **Important :**
>
> - Vous devez inclure votre fichier CustomerInfo.yml avec vos ID client et les informations de clé secrète. Pour savoir comment récupérer vos ID client et de votre clé secrète, reportez-vous à la section Génération des ID client et de la clé secrète. Pour plus d'informations sur l'ajout de ces informations au fichier CustomerInfo.yml, reportez-vous à la section Remplissage du fichier d'informations client.
> - Le fichier ZoneMapping.yml doit inclure des informations qui mappent votre zone locale aux emplacements de ressources dans le cloud. Pour savoir comment mapper vos zones, reportez-vous à la section Remplissage du fichier de mappage de zones.
> - Si vous disposez de connexions hôtes, vous devez entrer les informations correspondantes dans le fichier CvadAcSecurity.yml.
> - Lors de la migration d'un déploiement local vers le cloud, assurez-vous que les objets de stratégie de groupe de domaine et d'unité d'organisation contenant les paramètres Citrix sont migrés vers le cloud. Citrix Web Studio n'étant pas compatible avec GPMC, les objets de stratégie de groupe de domaine et d'unité d'organisation ne sont pas visibles dans la console Web Studio. Le moteur de stratégie Citrix applique les objets de stratégie de

> groupe de domaine et d'unité d'organisation sur les VDA et les utilisateurs qui se trouvent dans les domaines et les unités d'organisation. Après s'être connecté à un VDA, un utilisateur peut constater que les stratégies du domaine et des GPO de l'unité d'organisation sont appliquées à sa session. Cependant, les administrateurs ne peuvent pas voir ces stratégies et paramètres, ce qui peut prêter à confusion.

Exécution d'une importation

1. Double-cliquez sur l'icône **Config automatique**. Une fenêtre PowerShell s'affiche.
2. Exécutez la commande suivante pour importer tous les composants.

   ```
   Merge-CvadAcToSite
   ```

Comparez l'état attendu avec le nouvel état actuel. Diverses options d'importation contrôlent si les résultats d'importation sont identiques ou un sous-ensemble du site local.

Après l'exécution de l'applet de commande, un dossier d'exportation contenant les journaux et les fichiers de configuration .yml est créé. Le dossier se trouve sous *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Si vous rencontrez des erreurs ou des exceptions, consultez la section **Fixups** du fichier journal.

> **Remarque :**
>
> Si la configuration automatisée n'est pas installée sur le Delivery Controller, exécutez `import -module Citrix.AutoConfig.Commands` avant d'utiliser l'outil via PowerShell. Cette étape n'est pas nécessaire si vous ouvrez Configuration automatisée à l'aide de l'icône **Config automatique**.

Pour revenir à votre configuration Citrix DaaS d'origine, consultez Sauvegarde de la configuration Citrix DaaS.

Opération d'importation en détail

Le processus d'importation est conçu pour effectuer les mises à jour appropriées, appliquer uniquement les mises à jour nécessaires et vérifier que toutes les mises à jour ont été correctement effectuées. Vous trouverez ci-dessous les étapes de toutes les opérations d'importation.

1. Consultez le fichier .yml exporté (état attendu).
2. Consultez le cloud (état actuel).
3. Sauvegardez l'état du cloud avant importation dans les fichiers .yml (la pré-sauvegarde peut être restaurée si nécessaire).
4. Évaluez les différences entre l'état attendu et l'état actuel. Cela détermine les mises à jour à effectuer.

5. Effectuez les mises à jour.
6. Consultez de nouveau le cloud (nouvel état actuel).
7. Sauvegardez l'état du cloud post-importation dans les fichiers .yml (la post-sauvegarde peut être restaurée si nécessaire).
8. Comparez le nouvel état actuel avec l'état attendu.
9. Générez un rapport des résultats de la comparaison.

Migration granulaire

> **Important :**
>
> Pour plus d'informations sur l'ordre de migration des composants, consultez Ordre de migration des composants.

Vous pouvez migrer de manière sélective des composants uniquement ou même des noms de composants uniquement.

- Les paramètres de composants pris en charge incluent `MachineCatalogs` et `Tags` entre autres.
- Les paramètres de nom de composant pris en charge incluent les paramètres `IncludeByName` et `ExcludeByName` entre autres.

Pour plus d'informations sur les paramètres et leur utilisation, consultez la rubrique Paramètres de migration granulaire.

Activation des sites

L'activation du site vous permet de contrôler quel site est actif et contrôle vos ressources. Pour plus d'informations, consultez Activation de sites.

Fusion de plusieurs sites en un seul site

March 30, 2024

La prise en charge multisite de la configuration automatisée fournit une méthode pour fusionner plusieurs sites locaux en un seul site cloud.

La prise en charge multisite ajoute des préfixes et des suffixes uniques aux noms de composants basés sur chaque site local, garantissant ainsi l'unicité des noms après la fusion de plusieurs sites locaux en un seul site cloud.

Des préfixes et des suffixes peuvent être affectés à chacun des composants suivants pour chaque site.

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`
- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`
- `GroupPolicy`
- `HostConnection`
- `MachineCatalog`
- `StoreFront`
- `Tag`

Les dossiers d'application prennent en charge l'ajout de préfixe, de suffixe et le changement de racine. Le changement de racine ajoute un dossier de niveau supérieur supplémentaire à la structure de dossiers existante d'une application.

Règles d'ajout de préfixe et de suffixe

1. Les préfixes et les suffixes ne peuvent contenir aucun des caractères spéciaux suivants : `\ , / ; : # . * ? = < > | ( )"' { } [ ]`
2. Les préfixes et les suffixes peuvent contenir des espaces de fin mais pas des espaces de début.
3. Les préfixes et les suffixes doivent être placés entre guillemets pour pouvoir contenir des espaces de fin.
4. Les préfixes et les suffixes sont appliqués au moment de l'importation, de la fusion et de l'ajout. Les fichiers .yml source ne sont jamais modifiés.
5. Le processus ajoute automatiquement des préfixes et des suffixes aux noms de composants dépendants le cas échéant. Par exemple, si les noms de catalogue de machines sont préfixés par « East », les groupes de mise à disposition qui les référencent sont également préfixés par « East ».
6. Si un nom de composant commence déjà par le préfixe ou le suffixe, aucun préfixe ou suffixe n'est ajouté. Les noms de composants ne peuvent pas contenir de préfixes ou de suffixes doubles identiques.
7. Les préfixes et les suffixes peuvent être utilisés individuellement ou combinés.
8. L'utilisation d'un préfixe ou d'un suffixe sur un composant est facultative.

> **Remarque :**
>
> L'interface Configuration complète affiche les composants par ordre alphabétique.

Grouper par site

Utilisez un préfixe pour regrouper visuellement les composants d'un seul site. Chaque site est répertorié dans son propre groupe avec préfixe appliqué par ordre alphabétique pour contrôler l'ordre des différents groupes de sites.

Grouper par nom

Utilisez un suffixe pour regrouper visuellement des composants de nom similaire dans plusieurs sites. Les composants de même nom provenant de différents sites alternent visuellement.

Fichier SitePrefixes.yml

Pour les préfixes de site, le processus commence par le fichier SiteMerging.yml qui contient le mappage de préfixe et de suffixe pour un ou plusieurs sites locaux. Vous pouvez gérer le fichier SiteMerging.yml manuellement ou à l'aide des applets de commande disponibles répertoriées dans la section Fusion de plusieurs applets de commande de sites locaux.

Exportation, importation, fusion et ajout

La fusion ne peut pas commencer tant que vous n'avez pas exporté un site local. Pour exporter un site local, consultez la section Migration d'une configuration locale vers le cloud.

Dossier cible central pour l'exportation

Les méthodes décrites dans cette section placent plusieurs exportations de sites dans un emplacement central de partage de fichiers. Le fichier SiteMerging.yml, le fichier CustomerInfo.yml et tous les fichiers d'exportation résident dans cet emplacement de partage de fichiers, ce qui vous permet d'effectuer l'importation à partir d'un emplacement indépendant des sites locaux.

Les opérations d'accès au cloud ne font jamais référence aux sites locaux ou à Active Directory, ce qui vous permet d'effectuer des opérations d'accès au cloud depuis n'importe où.

Partage direct de fichiers

Les opérations d'exportation, d'importation, de fusion et de création/ajout fournissent un paramètre pour utiliser un dossier cible ou source autre que le dossier par défaut, *%HOMEPATH%\Documents\Citrix\AutoConfig*. Les exemples suivants utilisent un partage de fichiers central situé sur `\\share.central.net` auquel l'administrateur a déjà accès, après avoir fourni des informations d'identification si nécessaire.

Pour effectuer l'exportation vers un dossier cible spécifique au site, utilisez le paramètre `–TargetFolder` :

Depuis le DDC East :

```
mkdir \\share.central.net\AutoConfig\SiteEast

Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\
SiteEast
```

Depuis le DDC West :

```
mkdir \\share.central.net\AutoConfig\SiteWest

Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\
SiteWest
```

Une fois les exportations terminées, créez les fichiers CustomerInfo.yml et SiteMerging.yml et placez-les dans `\\share.central.net\AutoConfig`.

> **Remarque :**
>
> N'utilisez pas le paramètre `SiteRootFolder` lors de la création de SitePrefixes.yml si vous utilisez cette méthode de référence de partage de fichiers direct.

Pour importer, fusionner ou ajouter à partir du partage de fichiers direct, vous devez décider de la machine à partir de laquelle vous souhaitez effectuer l'opération d'accès au cloud. Les options sont les suivantes :

- Un des DDC locaux où l'outil est déjà installé.
- La machine hébergeant le partage de fichiers.
- Une autre machine.

La configuration automatisée doit être installée sur la machine accédant au cloud. Ni le SDK PowerShell local, ni le DDC, ni Active Directory ne sont utilisés, de sorte que les exigences d'accès au cloud sont plus simples que les exigences d'exportation.

Pour fusionner le DDC East sur le cloud :


```
Merge-CvadAcToSite –SiteName East –SourceFolder \\share.central.
net\AutoConfig\SiteEast -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

Pour fusionner le DDC West sur le cloud :

```
Merge-CvadAcToSite –SiteName West –SourceFolder \\share.central.
net\AutoConfig\SiteWest -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

Voici un exemple de fichier SitePrefixes.yml basé sur l'exemple précédent.

```
    East:
      SiteRootFolder: "" # Important: leave this empty
      AdminScopePrefix: "East_"
      AdminRolePrefix: "East_"
      ApplicationAdminPrefix: "East_"
      ApplicationFolderPrefix: "" # Note that a new parent root folder
         is used instead
      ApplicationFolderRoot: "East"
      ApplicationGroupPrefix: "East_"
      ApplicationUserPrefix: "East_"
      DeliveryGroupPrefix: "East_"
      GroupPolicyPrefix: "East_"
      HostConnectionPrefix: "East_"
      MachineCatalogPrefix: "East_"
      StoreFrontPrefix: "East_"
      TagPrefix: "East_"
      AdminScopeSuffix: "_east"
      AdminRoleSuffix: "_east"
      ApplicationAdminSuffix: "_east"
      ApplicationFolderSuffix: "_east"
      ApplicationGroupSuffix: "_east"
      ApplicationUserSuffix: "_east"
      DeliveryGroupSuffix: "_east"
      GroupPolicySuffix: "_east"
      HostConnectionSuffix: "_east"
      MachineCatalogSuffix: "_east"
      StoreFrontSuffix: "_east"
      TagSuffix: "_east"
    West:
      SiteRootFolder: "" # Important: leave this empty
      AdminScopePrefix: "Western "
      AdminRolePrefix: "Western "
      ApplicationAdminPrefix: "Western "
      ApplicationFolderPrefix: "" # Note that a new parent root folder
         is used instead
      ApplicationFolderRoot: "Western"
      ApplicationGroupPrefix: "Western "
      ApplicationUserPrefix: "Western "
      DeliveryGroupPrefix: "Western "
      GroupPolicyPrefix: "Western "
      HostConnectionPrefix: "Western "
```



```
40        MachineCatalogPrefix: "Western "
41        StoreFrontPrefix: "Western "
42        TagPrefix: "Western "
43        AdminScopeSuffix: ""
44        AdminRoleSuffix: ""
45        ApplicationAdminSuffix: ""
46        ApplicationFolderSuffix: ""
47        ApplicationGroupSuffix: ""
48        ApplicationUserSuffix: ""
49        DeliveryGroupSuffix: ""
50        GroupPolicySuffix: ""
51        HostConnectionSuffix: ""
52        MachineCatalogSuffix: ""
53        StoreFrontSuffix: ""
54        TagSuffix: ""
```

Référence de partage de fichiers à l'aide de SiteMerging.yml

Cette méthode utilise le membre `SiteRootFolder` du jeu de préfixes du site. Bien qu'elle soit plus impliquée que la méthode de partage de fichiers direct, cette méthode réduit les chances de cibler le mauvais dossier lors de l'exportation, de l'importation, de la fusion ou de l'ajout.

Tout d'abord, définissez le `SiteRootFolder` pour chaque site dans le fichier SiteMerging.yml. Vous devez le faire sur l'emplacement partagé.

```
New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \\share.
central.net\AutoConfig\SiteEast -SitePrefixesFolder \\share.central.
net\AutoConfig
```

```
New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest -
SitePrefixesFolder \\share.central.net\AutoConfig
```

Dans cet exemple, East est une spécification de dossier complète et West est une spécification de dossier relative.

Pour utiliser un dossier d'exportation cible spécifique au site à l'aide du fichier SiteMerging.yml :

Depuis le DDC East :

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Depuis le DDC West :

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```


L'applet de commande d'exportation utilise l'emplacement du dossier CustomerInfo.yml pour localiser le fichier SiteMerging.yml. Dans le cas du dossier East, la spécification `SiteRootFolder` est complète. Elle est utilisée telle quelle. Dans le cas du dossier West, la spécification `SiteRootFolder` n'est pas complète. Elle est combinée avec l'emplacement du dossier CustomerInfo.yml pour récupérer un emplacement de dossier complet pour West.

Pour fusionner le DDC East sur le cloud :

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Pour fusionner le DDC West sur le cloud :

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Voici un exemple de fichier SitePrefixes.yml basé sur l'exemple précédent.

```
    East:
    SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"
    AdminScopePrefix: "East_"
    AdminRolePrefix: "East_"
    ApplicationAdminPrefix: "East_"
    ApplicationFolderPrefix: "" # Note that a new parent root folder
        is used instead
    ApplicationFolderRoot: "East"
    ApplicationGroupPrefix: "East_"
    ApplicationUserPrefix: "East_"
    DeliveryGroupPrefix: "East_"
    GroupPolicyPrefix: "East_"
    HostConnectionPrefix: "East_"
    MachineCatalogPrefix: "East_"
    StoreFrontPrefix: "East_"
    TagPrefix: "East_"
    AdminScopeSuffix: "_east"
    AdminRoleSuffix: "_east"
    ApplicationAdminSuffix: "_east"
    ApplicationFolderSuffix: "_east"
    ApplicationGroupSuffix: "_east"
    ApplicationUserSuffix: "_east"
    DeliveryGroupSuffix: "_east"
    GroupPolicySuffix: "_east"
    HostConnectionSuffix: "_east"
    MachineCatalogSuffix: "_east"
    StoreFrontSuffix: "_east"
    TagSuffix: "_east"
  West:
    SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"
    AdminScopePrefix: "Western "
    AdminRolePrefix: "Western "
    ApplicationAdminPrefix: "Western "
    ApplicationFolderPrefix: "" # Note that a new parent root folder
        is used instead
```



```
34        ApplicationFolderRoot: "Western"
35        ApplicationGroupPrefix: "Western "
36        ApplicationUserPrefix: "Western "
37        DeliveryGroupPrefix: "Western "
38        GroupPolicyPrefix: "Western "
39        HostConnectionPrefix: "Western "
40        MachineCatalogPrefix: "Western "
41        StoreFrontPrefix: "Western "
42        TagPrefix: "Western "
43        AdminScopeSuffix: ""
44        AdminRoleSuffix: ""
45        ApplicationAdminSuffix: ""
46        ApplicationFolderSuffix: ""
47        ApplicationGroupSuffix: ""
48        ApplicationUserSuffix: ""
49        DeliveryGroupSuffix: ""
50        GroupPolicySuffix: ""
51        HostConnectionSuffix: ""
52        MachineCatalogSuffix: ""
53        StoreFrontSuffix: ""
54        TagSuffix: ""
```

Si aucune méthode de partage de fichiers central n'est utilisée et que l'importation, la fusion ou l'ajout est effectué à partir de DDC individuels, créez et répliquez le fichier SiteMerging.yml sur chaque DDC en cours de migration vers le cloud. L'emplacement par défaut est *%HOMEPATH%\Documents\Citrix\AutoConfig*. Vous devez spécifier le paramètre `–SiteName` pour sélectionner les préfixes de site corrects.

Fusionner les sites

Citrix recommande d'effectuer les opérations cloud par étapes et de procéder à un examen complet de chaque résultat avant d'effectuer la prochaine opération cloud. Par exemple, si vous fusionnez trois sites vers un seul site cloud :

1. Fusionnez le site initial sur le cloud à l'aide de la valeur `SiteName` appropriée.
2. Consultez les résultats dans l'interface de gestion Configuration complète.
3. Si les résultats sont incorrects, déterminez le problème et sa cause, corrigez-le, puis relancez la fusion. Si nécessaire, supprimez les composants cloud et commencez à partir de zéro en utilisant `Remove-CvadAcFromSite` pour le composant et les membres sélectionnés. Si les résultats sont corrects, continuez.
4. Si la fusion initiale est correcte, fusionnez le deuxième site sur le site cloud unique.
5. Répétez les étapes 2 et 3.
6. Si la deuxième fusion est correcte, fusionnez le troisième site sur le site cloud unique.
7. Répétez les étapes 2 et 3.
8. Examinez les ressources du point de vue de l'utilisateur et vérifiez que la vue est à l'état souhaité.

Supprimer un composant à l'aide du préfixe de site

Vous pouvez supprimer certains composants de site unique à l'aide du préfixe du paramètre `–IncludeByName` de l'applet de commande `Remove-CvadAcFromSite`. Dans l'exemple suivant, les groupes de mise à disposition DDC West ne sont pas corrects. Pour supprimer les groupes de mise à disposition uniquement pour le site West :

```
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName "Western *"
```

Pour supprimer tous les composants West, exécutez les applets de commande suivantes dans l'ordre indiqué.

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName "Western *"
Remove-CvadAcFromSite –Applications –IncludeByName "Western *"
Remove-CvadAcFromSite – ApplicationGroups –IncludeByName "Western *"
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName "Western *"
Remove-CvadAcFromSite –MachineCatalogs –IncludeByName "Western *"
Remove-CvadAcFromSite –HostConnections –IncludeByName "Western *"
Remove-CvadAcFromSite –Tags –IncludeByName "Western *"
```

Pour supprimer les stratégies de groupe des composants East, utilisez le suffixe :

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName "*_east"
```

Migration d'une configuration cloud vers le cloud

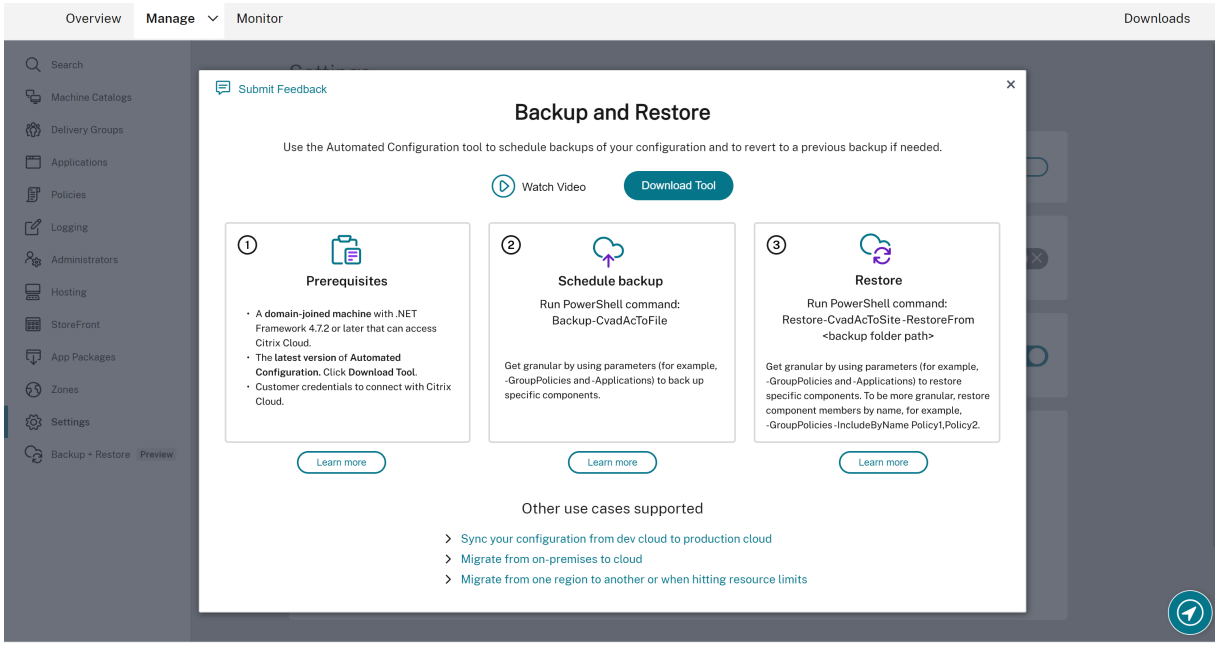
April 18, 2024

La configuration automatisée vous permet d'automatiser le déplacement de votre configuration cloud vers un autre site cloud ou de restaurer votre propre site cloud.

L'utilisation de la configuration automatisée peut résoudre de nombreux cas d'utilisation :

- Synchronisation de votre site de la phase de test ou de pré-production à la production
- Sauvegarde et restauration de votre configuration
- Atteindre les limites de ressources
- Migration d'une région à une autre

Dans Configuration complète sur Citrix Cloud, consultez le nœud Sauvegarde et restauration pour plus d'informations sur la configuration automatisée et la façon dont elle peut être utilisée pour migrer votre configuration du cloud vers le cloud.



Conditions préalables à la migration de votre configuration

Pour sauvegarder et restaurer votre configuration, les conditions préalables suivantes sont requises :

- L'instance Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) est provisionnée.
- L'emplacement de ressources sur lequel Connector est installé est actif.
- La connectivité aux sites accédant à Citrix Cloud doit être autorisée et disponible. Pour plus d'informations, consultez la section Configuration requise pour le système et la connectivité.

> **Remarque :**
>
> MCS ne peut pas être sauvegardé depuis le cloud à l'aide de la configuration automatisée.

Sauvegarde de la configuration Citrix DaaS

> **Important :**
>
> - Vous devez inclure votre fichier CustomerInfo.yml avec vos ID client et les informations de clé secrète. Pour savoir comment récupérer vos ID client et de votre clé secrète, reportez-vous à la section Génération des ID client et de la clé secrète. Pour plus d'informations sur l'ajout de ces informations au fichier CustomerInfo.yml, reportez-vous à la section Remplissage du fichier d'informations client.
> - Lorsque vous exécutez les commandes de sauvegarde, le fichier CustomerInfo.yml doit con-

tenir les informations relatives au client du site source à partir duquel vous effectuez la sauvegarde.
- Lorsque vous exécutez les commandes de restauration, le fichier CustomerInfo.yml doit contenir les informations relatives au client du site de destination sur lequel vous restaurez les configurations.
- Le fichier ZoneMapping.yml doit inclure des informations qui mappent vos emplacements de ressources dans le cloud. Pour savoir comment mapper vos zones, reportez-vous à la section Remplissage du fichier de mappage de zones.
- Si vous disposez de connexions hôtes, vous devez entrer les informations correspondantes dans le fichier CvadAcSecurity.yml.

1. Installez la configuration automatisée.

   Remarque :

   Pour la migration d'un cloud à un autre, la configuration automatisée peut être installée sur une machine ayant accès à Internet à laquelle l'administrateur a un accès direct.

2. Double-cliquez sur l'icône **Config automatique**. Une fenêtre PowerShell s'affiche.
3. Exécutez la commande suivante pour effectuer une sauvegarde.

   ```
   Backup-CvadAcToFile
   ```

Après avoir exécuté une applet de commande pour la première fois, un dossier d'exportation contenant les journaux et les fichiers de configuration .yml est créé. Le dossier se trouve sous *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Si vous rencontrez des erreurs ou des exceptions, consultez la section **Fixups** du fichier journal.

Restauration de la configuration dans Citrix DaaS

1. Double-cliquez sur l'icône **Config automatique**. Une fenêtre PowerShell s'affiche.
2. Exécutez la commande suivante pour effectuer une restauration.

   ```
   Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
   ```

Comparez l'état attendu avec le nouvel état actuel.

Après l'exécution de l'applet de commande, un dossier d'exportation contenant les journaux et les fichiers de configuration .yml est créé. Le dossier se trouve sous *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Si vous rencontrez des erreurs ou des exceptions, consultez la section **Fixups** du fichier journal.

Le processus de sauvegarde et de restauration vous protège contre les modifications ou la corruption involontaires de la configuration du site cloud. Alors que la configuration automatisée effectue

des sauvegardes à chaque fois qu'une modification est apportée, cette sauvegarde reflète l'état de la configuration du site cloud avant les modifications. Pour vous protéger, vous devez sauvegarder périodiquement la configuration de votre site cloud et l'enregistrer dans un endroit sûr. Si une modification ou une corruption indésirable a lieu, la sauvegarde peut être utilisée pour corriger la modification ou la corruption à un niveau granulaire ou complet de configuration du site.

Migration granulaire

> **Important :**
>
> Pour plus d'informations sur l'ordre de migration des composants, consultez Ordre de migration des composants.

Restauration de composants entiers

La restauration d'un composant implique la sélection d'un ou de plusieurs paramètres de composant.

Pour restaurer l'ensemble des composants Groupe de mise à disposition et Catalogue de machines, suivez cet exemple :

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

Restauration des membres d'un composant

La restauration d'un ou de plusieurs membres de composant utilise la fonction `IncludeByName` . L'applet de commande `Restore` est appelée avec le paramètre `RestoreFolder` ainsi que le composant unique sélectionné et la liste d'inclusion.

Pour restaurer deux stratégies de groupe à partir d'une sauvegarde, suivez l'exemple suivant :

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss

-GroupPolicies -IncludeByName Policy1,Policy2

-DeliveryGroups -MachineCatalogs
```

Restauration de l'intégralité de la configuration du site cloud

Restaurer la configuration complète du site cloud signifie que vous sélectionnez tous les composants pour la restauration.

Pour restaurer l'intégralité de la configuration du site cloud, suivez l'exemple suivant :

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

Activation des sites

L'activation du site vous permet de contrôler quel site est actif et contrôle vos ressources. Pour plus d'informations, consultez Activation de sites.

Applets de commande de l'outil de configuration automatisée

March 30, 2024

Cette page répertorie tous les applets de commande et paramètres pris en charge par l'outil.

Toutes les applets de commande acceptent des paramètres de l'un des types suivants.

- Chaîne
- Liste des chaînes
- Booléen : `$true` ou `$false`
- SwitchParameter : la présence du paramètre signifie `$true` ; l'absence du paramètre signifie `$false`

> **Remarque :**
>
> SwitchParameter est la méthode préférée pour les sélections true ou false, mais les booléens sont toujours utilisés dans l'outil en raison de problèmes hérités.

Le tableau suivant récapitule toutes les applets de commande. Consultez chaque section pour connaître les paramètres pris en charge par chaque applet de commande.

Catégorie	Applet de commande	Description
Migration du site vers le cloud	`Export-CvadAcToFile`	Exporte les fichiers locaux vers des fichiers YAML.
		`Import-CvadAcToSite`
		`Merge-CvadAcToSite`
		`New-CvadAcToSite`
		`Sync-CvadAcToSite`

Catégorie	Applet de commande	Description
		Migration granulaire Pour les composants, utilisez les paramètres avec les commandes ci-dessus. Exemples : `MachineCatalogs`, `Tags`. Pour les noms de composants, utilisez les paramètres avec les commandes ci-dessus. Exemples : `IncludeByName`, `ExcludeByName`.
Applets de commande cloud vers cloud	`Backup-CvadAcToFile`	Sauvegarde toute la configuration de votre site cloud.
	`Restore-CvadAcToSite`	
	`Remove-CvadAcFromSite`	*Migration granulaire* Pour les composants, utilisez les paramètres avec les commandes ci-dessus. Exemples : `MachineCatalogs`, `Tags`. Pour les noms de composants, utilisez les paramètres avec les commandes ci-dessus. Exemples : `IncludeByName`, `ExcludeByName`.
Autres applets de commande de base	`Compare-CvadAcToSite`	Compare les fichiers .yml locaux avec la configuration cloud.
Applets de commande liées aux conditions préalables	`New-CvadAcCustomerInfoFile`	Crée un fichier d'informations client.
	`Set-CvadAcCustomerInfoFile`	

Catégorie	Applet de commande	Description
Applets de commande de support et de dépannage	`New-CvadAcZipInfoForSupport`	Zippe tous les fichiers journaux et .yml dans un seul fichier zip à envoyer à Citrix pour obtenir de l'assistance.
	`Get-CvadAcStatus`	
	`Test-CvadAcConnectionWithSite`	
	`Find-CvadAcConnector`	
	`Get-CvadAcCustomerSites`	
	`New-CvadAcTemplateToFile`	
	`Show-CvadAcDocument`	
	`Find-CvadAcInFile`	
Applets de commande d'activation de site	`Set-CvadAcSiteActiveStateOnPrem`	Définit l'état du site local sur actif ou inactif.
	`Set-CvadAcSiteActiveStateCloud`	
Fusion de plusieurs applets de commande de sites locaux	`New-CvadAcSiteMergingInfo`	Crée un jeu d'informations préfixe/suffixe de fusion de site.
	`Set-CvadAcSiteMergingInfo`	
	`Remove-CvadAcSiteMergingInfo`	

Pour plus d'informations sur les paramètres et leur utilisation, consultez la rubrique Paramètres de migration granulaire.

Applets de commande de base

Applets de commande site vers cloud

- `Export-CvadAcToFile` - Exporte les fichiers locaux vers des fichiers YAML.

  Exporte la configuration à partir de votre configuration locale. Il s'agit de l'opération d'exportation par défaut pour l'outil de configuration automatisée. Aucune modification n'est apportée à la configuration du site local. Les fichiers exportés sont placés dans le répertoire *%CHEMINDEBASE%\Documents\Citrix\AutoConfig* dans un sous-dossier **Export** à nom unique. Le dossier *%HOMEPATH%\Documents\Citrix\AutoConfig* contient toujours la dernière configuration de site local exportée.

  Paramètres :

Nom	Description	Requis ?	Type
Migrer par composants	Voir Migrer par composants		SwitchParameters
Filtrage par noms d'objets	Voir Filtrage par noms d'objets		Liste des chaînes
`TargetFolder`	Spécifie le dossier de destination de l'exportation.		Chaîne
`Locale`	Spécifie la langue du texte lisible qui peut être exporté.		Chaîne
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter
`AdminAddress`	Spécifie le DNS ou l'adresse IP du Delivery Controller lorsque l'exportation n'est pas exécutée sur le Delivery Controller.		Chaîne
`CheckUserAndMachines`	Vérifie si les utilisateurs et les machines sont dans Active Directory. Les utilisateurs et les machines qui ne sont pas dans Active Directory peuvent entraîner des échecs d'importation.		`$true` ou `$false`
`ZipResults`	Compresse les fichiers YAML de sauvegarde en un seul fichier zip. Le fichier se trouve dans le même dossier que les fichiers YAML sauvegardés et porte le même nom que le dossier.		SwitchParameter

  Renvoie :

  - Voir Valeurs de retour de l'applet de commande

Il existe trois façons d'importer des données dans le cloud. L'exécution d'applets de commande spécifiques peut entraîner l'une des trois combinaisons d'actions sur le site cloud :

- Ajouter, mettre à jour et supprimer
- Ajouter et mettre à jour uniquement
- Ajouter uniquement

Applet de commande	Add	Mise à jour	Supprimer
Importer	X	X	X
Merge	X	X	
New	X		

- `Import-CvadAcToSite` - Importe les fichiers YAML dans le cloud. Prend en charge les opérations de création, de mise à jour et de suppression

  Importe tous les fichiers locaux dans le cloud. Cette commande garantit que l'état final du cloud est identique à l'état local. Cette option supprime toutes les modifications qui existent dans le cloud. Les fichiers de configuration de site importés proviennent de *%CHEMINDEBASE%\Documents\Citrix\AutoConfig*. *Utilisez cette commande avec prudence.*

  Paramètres :

Nom	Description	Requis ?	Type
Migrer par composants	Voir Migrer par composants.		SwitchParameters
Filtrage par noms d'objets	Voir Filtrage par noms d'objets.		Liste des chaînes
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud.		SwitchParameters
`SourceFolder`	Identifie un dossier racine de substitution pour *%HOMEPATH%\Documents\Citrix\AutoConfig*.		Chaîne
`Locale`	Spécifie la langue du texte lisible qui peut être exporté.		Chaîne
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter
`DisplayLog`	Affiche le fichier journal à la fin de l'applet de commande. Définissez sur `$false` pour supprimer l'affichage du journal.		`$true` ou `$false`

Nom	Description	Requis ?	Type
`Merge`	Lorsque cette valeur est définie sur `$true`, ajoute uniquement des composants au site cloud. Les composants ne sont pas supprimés. Définissez sur `$false` pour supprimer des composants.		`$true` ou `$false`
`AddOnly`	Lorsque cette option est définie sur `$true`, ajoute uniquement les nouveaux composants, ne met pas à jour ou ne supprime pas les composants existants. Définissez sur `$false` pour autoriser les mises à jour et les suppressions. `Merge` est ignoré lorsque ce paramètre est `$true`.		`$true` ou `$false`
`MergePolicies`	Fusionne les paramètres de stratégie et les filtres. La fusion se produit uniquement lorsqu'une stratégie en cours d'importation existe déjà dans le DDC cloud. Après la fusion des stratégies, les stratégies DDC cloud contiennent les paramètres et filtres qu'elles avaient déjà, en plus de tous les nouveaux paramètres et filtres importés. Notez que, en cas de collisions de paramètres et de filtres, les valeurs importées sont prioritaires.		SwitchParameter
`OnErrorAction`	Voir Paramètre OnErrorAction.		Chaîne

Renvoie :

- Voir Valeurs de retour de l'applet de commande

- `Merge-CvadAcToSite` - Importe les fichiers YAML dans le cloud. Prend en charge les opérations de création et de mise à jour

  Fusionne les fichiers locaux dans le cloud, mais *ne supprime aucun* composant dans le cloud ou sur site. Cela préserve les modifications déjà apportées dans le cloud. Si un composant portant le même nom existe dans Citrix Cloud, cette commande peut modifier ce composant. Il s'agit de l'opération d'importation par défaut pour l'outil de configuration automatisée. Les fichiers de configuration de site fusionnés proviennent de *%CHEMINDEBASE%\Documents\Citrix\AutoConfig*.

  Paramètres :

Nom	Description	Requis ?	Type
Migrer par composants	Voir Migrer par composants.		SwitchParameters
Filtrage par noms d'objets	Voir Filtrage par noms d'objets.		Liste des chaînes
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud.		SwitchParameters
`SourceFolder`	Identifie un dossier racine de substitution pour *%HOMEPATH%\Documents\Citrix\AutoConfig*.		Chaîne
`Locale`	Spécifie la langue du texte lisible qui peut être exporté.		Chaîne
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter
`DisplayLog`	Affiche le fichier journal à la fin de l'applet de commande. Définissez sur `$false` pour supprimer l'affichage du journal.		`$true` ou `$false`
`Merge`	Lorsque cette valeur est définie sur `$true`, ajoute uniquement des composants au site cloud. Les composants ne sont pas supprimés. Définissez sur `$false` pour supprimer des composants.		`$true` ou `$false`
`AddOnly`	Lorsque cette option est définie sur `$true`, ajoute uniquement les nouveaux composants, ne met pas à jour ou ne supprime pas les composants existants. Définissez sur `$false` pour autoriser les mises à jour et les suppressions. `Merge` est ignoré lorsque ce paramètre est `$true`.		`$true` ou `$false`
`MergePolicies`	Fusionne les paramètres de stratégie et les filtres. La fusion se produit uniquement lorsqu'une stratégie en cours d'importation existe déjà dans le DDC cloud. Après la fusion des stratégies, les stratégies DDC cloud contiennent les paramètres et filtres qu'elles avaient déjà, en plus de tous les nouveaux paramètres et filtres importés. Notez que, en cas de collisions de paramètres et de filtres, les valeurs importées sont prioritaires.		SwitchParameter
`OnErrorAction`	Voir Paramètre OnErrorAction.		Chaîne

Renvoie :

- Voir Valeurs de retour de l'applet de commande

- `New-CvadAcToSite` - Importe les fichiers YAML dans le cloud. Prend en charge les opérations de création et de mise à jour

  Importe la configuration de site locale dans le cloud, mais ajoute uniquement les nouveaux composants. Les composants de site cloud existants ne sont ni mis à jour ni supprimés. Utilisez cette commande si les composants de site cloud existants doivent rester inchangés.

  Paramètres :

Nom	Description	Requis ?	Type
Migrer par composants	Voir Migrer par composants.		SwitchParameters
Filtrage par noms d'objets	Voir Filtrage par noms d'objets.		Liste des chaînes
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud.		SwitchParameters
`SourceFolder`	Identifie un dossier racine de substitution pour *%HOMEPATH%\Documents\Citrix\AutoConfig*.		Chaîne
`Locale`	Spécifie la langue du texte lisible qui peut être exporté.		Chaîne
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter
`DisplayLog`	Affiche le fichier journal à la fin de l'applet de commande. Définissez sur `$false` pour supprimer l'affichage du journal.		`$true` ou `$false`
`OnErrorAction`	Voir Paramètre OnErrorAction.		Chaîne

  Renvoie :

  - Voir Valeurs de retour de l'applet de commande

- `Sync-CvadAcToSite` - Exporte et importe en une seule étape.

  Sync effectue à la fois une exportation et une importation en une seule étape. Utilisez le paramètre `SourceTargetFolder` pour spécifier le dossier de destination d'exportation/importation.

  Paramètres :

Nom	Description	Requis ?	Type
Migrer par composants	Voir Migrer par composants		SwitchParameters
Filtrage par noms d'objets	Voir Filtrage par noms d'objets		Liste des chaînes
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud		SwitchParameters
`SourceTargetFolder`	Spécifie le dossier de destination de l'exportation/importation.		Chaîne
`Locale`	Spécifie la langue du texte lisible qui peut être exporté.		Chaîne
`AdminAddress`	Spécifie le DNS ou l'adresse IP du Delivery Controller lorsque l'exportation n'est pas exécutée sur le Delivery Controller.		Chaîne
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter
`DisplayLog`	Affiche le fichier journal à la fin de l'applet de commande. Définissez sur `$false` pour supprimer l'affichage du journal.		`$true` ou `$false`
`Merge`	Lorsque cette valeur est définie sur `$true`, ajoute uniquement des composants au site cloud. Les composants ne sont pas supprimés. Définissez sur `$false` pour supprimer des composants.		`$true` ou `$false`
`AddOnly`	Lorsque cette option est définie sur `$true`, ajoute uniquement les nouveaux composants, ne met pas à jour ou ne supprime pas les composants existants. Définissez sur `$false` pour autoriser les mises à jour et les suppressions. `Merge` est ignoré lorsque ce paramètre est `$true`.		`$true` ou `$false`

Nom	Description	Requis ?	Type
MergePolicies	Fusionne les paramètres de stratégie et les filtres. La fusion se produit uniquement lorsqu'une stratégie en cours d'importation existe déjà dans le DDC cloud. Après la fusion des stratégies, les stratégies DDC cloud contiennent les paramètres et filtres qu'elles avaient déjà, en plus de tous les nouveaux paramètres et filtres importés. Notez que, en cas de collisions de paramètres et de filtres, les valeurs importées sont prioritaires.		SwitchParameter

Renvoie :

- Voir Valeurs de retour de l'applet de commande

Applets de commande cloud vers cloud

- Backup-CvadAcToFile - Sauvegarde toute la configuration de votre site cloud.

  Exporte votre configuration cloud vers des fichiers .yml. Cette sauvegarde peut être utilisée dans un processus de sauvegarde et de restauration pour restaurer des composants perdus.

  Paramètres :

Nom	Description	Requis ?	Type
Migrer par composants	Voir Migrer par composants		SwitchParameters
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud		SwitchParameters
TargetFolder	Spécifie le dossier de destination de l'exportation.		Chaîne
Locale	Spécifie la langue du texte lisible qui peut être exporté.		Chaîne
Quiet	Supprime la journalisation sur la console.		SwitchParameter
DisplayLog	Affiche le fichier journal à la fin de l'applet de commande. Définissez sur $false pour supprimer l'affichage du journal.		$true ou $false

Nom	Description	Requis ?	Type
`ZipResults`	Compresse les fichiers YAML de sauvegarde en un seul fichier zip. Le fichier se trouve dans le même dossier que les fichiers YAML sauvegardés et porte le même nom que le dossier.		SwitchParameter

Renvoie :

- Voir Valeurs de retour de l'applet de commande

- `Restore-CvadAcToSite` - Restaure les fichiers YAML de sauvegarde sur le site cloud. Ce site cloud peut être identique au site cloud source ou différent.

  Restaure la configuration précédente du site cloud. Les fichiers importés proviennent du dossier spécifié à l'aide du paramètre `-RestoreFolder`, qui identifie le dossier contenant les fichiers .yml à restaurer sur le site cloud. La spécification du dossier doit être complète. Cette applet de commande peut être utilisée pour revenir à votre configuration précédente ou pour sauvegarder et restaurer votre site cloud. Cette commande peut ajouter, supprimer et mettre à jour votre site cloud.

  Paramètres :

Nom	Description	Requis ?	Type
Migrer par composants	Voir Migrer par composants.		SwitchParameters
Filtrage par noms d'objets	Voir Filtrage par noms d'objets.		Liste des chaînes
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud.		SwitchParameters
`RestoreFolder`	Identifie le dossier contenant les fichiers .yml à restaurer sur le site cloud. La spécification du dossier doit être complète.		Chaîne
`Locale`	Spécifie la langue du texte lisible qui peut être exporté.		Chaîne
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter
`DisplayLog`	Affiche le fichier journal à la fin de l'applet de commande. Définissez sur `$false` pour supprimer l'affichage du journal.		`$true` ou `$false`

Nom	Description	Requis ?	Type
`Merge`	Lorsque cette valeur est définie sur `$true`, ajoute uniquement des composants au site cloud. Les composants ne sont pas supprimés. Définissez sur `$false` pour supprimer des composants.		`$true` ou `$false`
`AddOnly`	Lorsque cette option est définie sur `$true`, ajoute uniquement les nouveaux composants, ne met pas à jour ou ne supprime pas les composants existants. Définissez sur `$false` pour autoriser les mises à jour et les suppressions. `Merge` est ignoré lorsque ce paramètre est `$true`.		`$true` ou `$false`
`MergePolicies`	Fusionne les paramètres de stratégie et les filtres. La fusion se produit uniquement lorsqu'une stratégie en cours d'importation existe déjà dans le DDC cloud. Après la fusion des stratégies, les stratégies DDC cloud contiennent les paramètres et filtres qu'elles avaient déjà, en plus de tous les nouveaux paramètres et filtres importés. Notez que, en cas de collisions de paramètres et de filtres, les valeurs importées sont prioritaires.		SwitchParameter
`OnErrorAction`	Voir Paramètre OnErrorAction.		Chaîne

Renvoie :

- Voir Valeurs de retour de l'applet de commande

- `Remove-CvadAcFromSite` - Supprime des membres de composants du cloud.

  Permet de réinitialiser l'intégralité du site ou de supprimer des éléments d'un composant (par exemple, supprimer un catalogue de machines de la liste des catalogues). Cette commande peut être utilisée lorsqu'elle est couplée avec le paramètre `IncludeByName` pour supprimer sélectivement des membres spécifiques.

  Paramètres :

Nom	Description	Requis ?	Type
Migrer par composants	Voir Migrer par composants		SwitchParameters

Nom	Description	Requis ?	Type
Filtrage par noms d'objets	Voir Filtrage par noms d'objets		Liste des chaînes
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud		SwitchParameters
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter
`DisplayLog`	Affiche le fichier journal à la fin de l'applet de commande. Définissez sur `$false` pour supprimer l'affichage du journal.		`$true` ou `$false`

Renvoie :

- Voir Valeurs de retour de l'applet de commande

Autres applets de commande de base

- `Compare-CvadAcToSite` - compare les fichiers .yml locaux avec la configuration cloud, produisant un rapport sur les modifications apportées par une applet de commande `Import`, `Merge` ou `Restore`.

  Paramètres :

Nom	Description	Requis ?	Type
Migrer par composants	Voir Migrer par composants.		SwitchParameters
Filtrage par noms d'objets	Voir Filtrage par noms d'objets.		Liste des chaînes
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud.		SwitchParameters
`SourceFolder`	Identifie un dossier racine de substitution pour *%HOMEPATH%\Documents\Citrix\AutoConfig*.		Chaîne
`Locale`	Spécifie la langue du texte lisible qui peut être exporté.		Chaîne
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter
`DisplayLog`	Affiche le fichier journal à la fin de l'applet de commande. Définissez sur `$false` pour supprimer l'affichage du journal.		`$true` ou `$false`

Nom	Description	Requis ?	Type
`Merge`	Lorsque cette valeur est définie sur `$true`, ajoute uniquement des composants au site cloud. Les composants ne sont pas supprimés. Définissez sur `$false` pour supprimer des composants.		`$true` ou `$false`
`AddOnly`	Lorsque cette option est définie sur `$true`, ajoute uniquement les nouveaux composants, ne met pas à jour ou ne supprime pas les composants existants. Définissez sur `$false` pour autoriser les mises à jour et les suppressions. `Merge` est ignoré lorsque ce paramètre est `$true`.		`$true` ou `$false`
`OnErrorAction`	Voir Paramètre OnErrorAction.		Chaîne

Renvoie :

- Voir Valeurs de retour de l'applet de commande

Paramètres de migration granulaire

Migrer par composants

Les composants suivants peuvent être spécifiés avec les applets de commande appropriées. L'option `All` est automatiquement sélectionnée lorsqu'aucun paramètre de composant n'est spécifié. Pour éviter les erreurs, nous vous recommandons de migrer les composants dans l'ordre suivant :

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`

- UserZonePreference

Filtrage par noms d'objets

Migrer par noms de composants Les paramètres IncludeByName et ExcludeByName permettent d'inclure et d'exclure des membres de composants dans les applets de commande par nom. Il n'est possible de choisir qu'un seul composant (par exemple, les groupes de mise à disposition) à la fois dans les applets de commande prises en charge. Si un membre de composant se trouve dans les deux zones, l'exclusion a priorité sur tout autre paramètre et une entrée est ajoutée à la liste de correction du journal, identifiant le nom du membre (et du composant) qui a été exclu.

IncludeByName et ExcludeByName acceptent une liste des noms de membres de composants. Les noms peuvent contenir un ou plusieurs caractères génériques. Deux types de caractères génériques sont pris en charge. La liste des noms de membres de composants doit être placée entre guillemets simples lorsqu'un nom contient des caractères spéciaux.

- * correspond à n'importe quel nombre de caractères
- ? Correspond à un seul caractère

IncludeByName et ExcludeByName peuvent également accepter un fichier contenant une liste de membres où chaque membre peut être explicite ou contenir des caractères génériques. Chaque ligne du fichier peut contenir un membre. Les espaces de début et de fin sont retirés du nom du membre. Le nom de fichier doit être précédé du signe @ et être entouré de guillemets simples (une exigence PowerShell pour que le @ ne soit pas réinterprété). Plusieurs fichiers peuvent être répertoriés en plus d'être mélangés avec des noms de membres.

Exemple de fusion de tous les groupes de mise à disposition dont les noms commencent par DgSite1 et contiennent Home2 :

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

Par nom du groupe de mise à disposition ByDeliveryGroupName filtre par nom du groupe de mise à disposition pour les applications et les groupes d'applications. Ce paramètre est toujours une liste d'inclusion identifiant les membres à inclure en fonction de leur association de groupe de mise à disposition.

ByDeliveryGroupName accepte une liste des noms de groupe de mise à disposition. Les noms peuvent contenir un ou plusieurs caractères génériques. Deux types de caractères génériques sont pris en charge.

- * correspond à n'importe quel nombre de caractères
- ? correspond à un seul caractère

L'exemple suivant fusionne toutes les applications qui font référence à tous les noms de groupe de mise à disposition commençant par `EastDg`.

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

Exclude Disabled `ExcludeDisabled` filtre des opérations d'importation toutes les applications et les groupes d'applications qui sont désactivés. `ExcludeDisabled` est **`false`** par défaut, ce qui signifie que toutes les applications et tous les groupes d'applications sont importés quel que soit leur état activé.

Par nom de machine `ByMachineName` filtre par le nom de la machine pour les catalogues de machines et les groupes de mise à disposition. Ce paramètre est toujours une liste d'inclusion identifiant les membres à inclure en fonction de leur association de nom de machine.

`ByMachineName` accepte une liste de noms de machines où les noms peuvent contenir un ou plusieurs caractères génériques. Deux types de caractères génériques sont pris en charge.

- * correspond à n'importe quel nombre de caractères
- ? correspond à un seul caractère

Lors de l'exportation ou de l'importation, si l'utilisation de `ByMachineName` et d'un filtre de nom de machine ne renvoie aucune machine dans le catalogue de machines ou le groupe de mise à disposition, le catalogue de machines ou le groupe de mise à disposition est exclu de l'exportation ou de l'importation.

> **Remarque :**
>
> Si `ByMachineName` est utilisé dans une applet de commande de tout type d'importation, `MergeMachines` est défini sur `$true`.

Fusionner des machines `MergeMachines`, si défini sur `$true`, indique à l'opération d'importation d'ajouter des machines uniquement au catalogue de machines ou au groupe de mise à disposition. Les machines ne sont pas retirées, ce qui permet des ajouts incrémentiels.

`MergeMachines` se règle sur false par défaut, ce qui signifie que les machines sont supprimées si elles ne sont pas présentes dans le fichier .yml du catalogue de machines ou du groupe de mise à disposition. `MergeMachines` est défini sur `$true` lorsque `ByMachineName` est utilisé mais peut être remplacé en définissant `MergeMachines` sur false.

Applets de commande liées aux conditions préalables

- `New-CvadAcCustomerInfoFile` - Crée un fichier d'informations client. Par défaut, le fichier d'informations client se trouve sous *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Paramètres :

Nom	Description	Requis ?	Type
`CustomerId`	ID du client.	x	Chaîne
`ClientId`	ID client créé sur Citrix Cloud. CustomerId et Secret doivent être spécifiés lors de l'utilisation de ce paramètre.	Conditionnellement	Chaîne
`Secret`	Clé secrète du client créée sur Citrix Cloud. CustomerId et ClientId doivent être spécifiés lors de l'utilisation de ce paramètre.	Conditionnellement	Chaîne
`Environment`	Environnement Production, ProductionGov ou ProductionJP.		Énumération
`LogFileName`	Remplace le préfixe du fichier journal de CitrixLog par autre chose.		Chaîne
`AltRootUrl`	À utiliser uniquement sous la direction de Citrix.		Chaîne
`StopOnError`	Arrête l'opération lors de la première erreur.		`$true` ou `$false`
`TargetFolder`	Utilise le dossier spécifié comme dossier racine au lieu de *%HOMEPATH%\Documents\Citrix\AutoConfig*.		Chaîne
`Locale`	Utilise les paramètres régionaux spécifiés au lieu des paramètres régionaux dérivés du système sur lequel l'outil est exécuté.		Chaîne
`Editor`	Utilise l'éditeur spécifié pour afficher le journal à la fin de chaque applet de commande. Notepad.exe est l'éditeur par défaut. Ce paramètre doit inclure la spécification complète du fichier à l'éditeur et l'éditeur doit prendre la spécification du fichier journal comme seul paramètre.		Chaîne

Nom	Description	Requis ?	Type
`SecurityCsvFileSpec`	Spécification de fichier complète pointant vers le fichier SecurityClient.csv téléchargé à partir de Gestion des identités et des accès Citrix. CustomerID doit être spécifié lors de l'utilisation de ce paramètre.		Chaîne

Renvoie :

- Voir Valeurs de retour de l'applet de commande

- `Set-CvadAcCustomerInfoFile` - Met à jour un fichier d'informations client existant. Seuls les paramètres spécifiés par l'applet de commande sont modifiés. Toutes les valeurs de paramètres non spécifiées dans le fichier CustomerInfo.yml restent inchangées.

  Paramètres :

Nom	Description	Requis ?	Type
`CustomerId`	ID du client.		Chaîne
`ClientId`	ID client créé sur Citrix Cloud.		Chaîne
`Secret`	Clé secrète du client créée sur Citrix Cloud.		Chaîne
`Environment`	Environnement Production, ProductionGov ou ProductionJP.		Énumération
`LogFileName`	Remplace le préfixe du fichier journal de CitrixLog par autre chose.		Chaîne
`StopOnError`	Arrête l'opération lors de la première erreur.		`$true` ou `$false`
`TargetFolder`	Utilise le dossier spécifié comme dossier racine au lieu de *%HOMEPATH%\Documents\Citrix\AutoConfig*.		Chaîne
`Locale`	Utilise les paramètres régionaux spécifiés au lieu des paramètres régionaux dérivés du système sur lequel l'outil est exécuté.		Chaîne

Nom	Description	Requis ?	Type
`Editor`	Utilise l'éditeur spécifié pour afficher le journal à la fin de chaque applet de commande. Notepad.exe est l'éditeur par défaut. Ce paramètre doit inclure la spécification complète du fichier à l'éditeur et l'éditeur doit prendre la spécification du fichier journal comme seul paramètre.		Chaîne
`SecurityCsvFileSpec`	Spécification de fichier complète pointant vers le fichier SecurityClient.csv téléchargé à partir de Gestion des identités et des accès Citrix. CustomerID doit être spécifié lors de l'utilisation de ce paramètre.		Chaîne

Renvoie :

- Voir Valeurs de retour de l'applet de commande

Paramètres liés aux conditions préalables

Outre les paramètres d'accès au cloud, les paramètres suivants peuvent être utilisés avec les applets de commande liées aux conditions préalables :

- `Environment` - environnement Production ou ProductionGov.
- `LogFileName` - remplace le préfixe du fichier journal de CitrixLog par autre chose.
- `StopOnError` - arrête l'opération lors de la première erreur.
- `AlternateRootFolder` - utilise le dossier spécifié comme dossier racine au lieu de *%HOMEPATH%\Documents\Citrix\AutoConfig*.
- `Locale` - utilise les paramètres régionaux spécifiés au lieu des paramètres régionaux dérivés du système sur lequel l'outil est exécuté.
- `Editor` - utilise l'éditeur spécifié pour afficher le journal à la fin de chaque applet de commande. Notepad.exe est l'éditeur par défaut. Ce paramètre doit inclure la spécification complète du fichier à l'éditeur et l'éditeur doit prendre la spécification du fichier journal comme seul paramètre.

Applets de commande de support et de dépannage

- `New-CvadAcZipInfoForSupport` - Zippe tous les fichiers journaux et .yml dans un seul fichier zip à envoyer à Citrix pour obtenir de l'assistance. Les informations sensibles du

client (CustomerInfo.yml et CvadAcSecurity.yml) ne sont pas incluses dans le zip. Le fichier Icon.yml est également exclu en raison de sa taille. Le fichier zip est placé dans *%HOMEPATH%\Documents\Citrix\AutoConfig* et nommé *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, en fonction de la date et de l'horodatage. Ce fichier zip peut également servir de sauvegarde.

Paramètres :

Nom	Description	Requis ?	Type
`TargetFolder`	Spécifie un dossier cible dans lequel créer et enregistrer le fichier zip.		Chaîne
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter

Renvoie :

- Le fichier Zip avec le nom et l'emplacement du fichier zip est affiché sur l'invite de commandes.

- `Get-CvadAcStatus` - Permet de tester la connectivité et de s'assurer que toutes les conditions préalables sont remplies. Renvoie des informations sur l'outil, telles que le numéro de version et la connectivité avec le cloud et l'état du connecteur.

  Paramètres :

Nom	Description	Requis ?	Type
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud		SwitchParameters
`SiteId`	Identifie le site auquel se connecter.		Chaîne
`AdminAddress`	Adresse DNS ou l'adresse IP du Delivery Controller local utilisé pour vérifier le niveau d'accès des administrateurs. Cette opération est requise si l'outil n'est pas exécuté sur un Delivery Controller.		Chaîne

  Renvoie :

  - Affiche les résultats pour chaque élément.

- `Test-CvadAcConnectionWithSite` - Teste la connexion avec le site cloud pour vérifier que la connexion de communication fonctionne. Cette applet de commande utilise les paramètres d'accès au cloud ou le fichier CustomerInfo.yml pour spécifier les informations de connexion du client.

Paramètres :

Nom	Description	Requis ?	Type
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud		SwitchParameters
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter

Renvoie :

- Les résultats des tests sont affichés sur la ligne de commande.

- `Find-CvadAcConnector` - Localise les connecteurs existants et détermine leur état d'exécution. Cette applet de commande utilise les informations du fichier CustomerInfo.yml ou du paramètre CustomerID pour localiser les connecteurs du client.

  Paramètres :

Nom	Description	Requis ?	Type
`CustomerInfoFileSpe`	Spécification de fichier pointant vers un fichier d'informations client pour remplacer l'emplacement et le nom par défaut. Ce paramètre est ignoré lorsque le paramètre `CustomerId` est fourni.		Chaîne
`CustomerId`	ID du client. Ce paramètre remplace la même valeur dans le fichier CustomerInfo.yml.		Chaîne

  Renvoie :

  - Les résultats sont affichés sur la ligne de commande.

- `Get-CvadAcCustomerSites` - Renvoie la liste de tous les sites clients. Cette applet de commande utilise les paramètres d'accès au cloud ou le fichier CustomerInfo.yml pour spécifier les informations de connexion du client.

  Paramètres :

  - Voir Paramètres d'accès au cloud

  Renvoie :

  - Affiche la liste des ID de site client trouvés.

- `New-CvadAcTemplateToFile` - Crée un fichier modèle pour les composants sélectionnés, ce qui vous permet de créer manuellement un fichier d'importation.

  Paramètres :

Nom	Description	Requis ?	Type
Migrer par composants	Voir Migrer par composants		SwitchParameters
`TargetFolder`	Spécifie le dossier de destination de l'exportation.		Chaîne

  Renvoie :

  - Voir Valeurs de retour de l'applet de commande

- `Show-CvadAcDocument` - Affiche cette documentation dans le navigateur par défaut.

  Paramètres :

  - Aucun.

  Renvoie :

  - Affichez cette page Web dans le navigateur Web par défaut.

- `Find-CvadAcInFile` - Recherche dans les recherches de fichier les fichiers YAML des composants à la recherche de membres correspondant à un ou plusieurs noms pouvant contenir des caractères génériques. Le résultat est un rapport des membres trouvés. La fonction de rechercher dans le fichier ne peut rechercher qu'un seul composant à la fois. La recherche dans le fichier recherche tous les fichiers YAML du dossier actuel et de tous les sous-dossiers. Utilisez `FindSourceFolder` pour limiter le nombre de fichiers à rechercher.

  Paramètres :

Nom	Description	Requis ?	Type
Migrer par composants	Voir Migrer par composants. Remarque : la valeur `-All` n'est pas valide.		SwitchParameters
`IncludeByName`	Liste spécifiant les noms des groupes de mise à disposition à inclure lors de la définition de l'état du site sur actif. Les caractères génériques '*'et '?'sont pris en charge dans les noms.		Liste des chaînes
`Unique`	Signale uniquement les membres trouvés uniques.		SwitchParameter

Nom	Description	Requis ?	Type
`IncludeYaml`	Inclut le YAML spécifique au membre.		SwitchParameter
`FindSourceFolder`	Dossier dans lequel commence la recherche.		Chaîne
`DisplayLog`	Affiche le fichier journal à la fin de l'applet de commande. Définissez sur `$false` pour supprimer l'affichage du journal.		SwitchParameter
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter

Renvoie :

- Crée un rapport contenant les membres trouvés pour le composant spécifié.

Applets de commande d'activation de site

Pour plus d'informations sur l'activation de sites et l'utilisation de ces applets de commande, consultez Activation de sites.

- `Set-CvadAcSiteActiveStateOnPrem` - Définit l'état du site local sur actif ou inactif.

  Paramètres :

Nom	Description	Requis ?	Type
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud		SwitchParameters
`SiteActive`	Lorsque ce paramètre est présent, définit le site local sur actif, supprimant ainsi le mode de maintenance de tous les groupes de mise à disposition. Lorsque ce paramètre n'est pas présent, le mode de maintenance est défini sur tous les groupes de mise à disposition.		SwitchParameter
`IncludeByName`	Liste spécifiant les noms des groupes de mise à disposition à inclure lors de la définition de l'état du site sur actif. Les caractères génériques '*' et '?' sont pris en charge dans les noms.		Liste des chaînes

Nom	Description	Requis ?	Type
`ExcludeByName`	Liste spécifiant les noms des groupes de mise à disposition à exclure lors de la définition de l'état du site sur actif. Les caractères génériques '*' et '?' sont pris en charge dans les noms.		Liste des chaînes
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter
`DisplayLog`	Affiche le fichier journal à la fin de l'applet de commande. Définissez sur `$false` pour supprimer l'affichage du journal.		`$true or $false`

Renvoie :

- Voir Valeurs de retour de l'applet de commande

- `Set-CvadAcSiteActiveStateCloud` - Définit l'état du site cloud sur actif ou inactif.

  Paramètres :

Nom	Description	Requis ?	Type
Paramètres d'accès au cloud	Voir Paramètres d'accès au cloud		SwitchParameters
`SiteActive`	Lorsque ce paramètre est présent, définit le site cloud sur actif, supprimant ainsi le mode de maintenance de tous les groupes de mise à disposition. Lorsque ce paramètre n'est pas présent, le mode de maintenance est défini sur tous les groupes de mise à disposition.		SwitchParameter
`IncludeByName`	Liste spécifiant les noms des groupes de mise à disposition à inclure lors de la définition de l'état du site sur actif. Les caractères génériques '*' et '?' sont pris en charge dans les noms.		Liste des chaînes
`ExcludeByName`	Liste spécifiant les noms des groupes de mise à disposition à exclure lors de la définition de l'état du site sur actif. Les caractères génériques '*' et '?' sont pris en charge dans les noms.		Liste des chaînes
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter

Nom	Description	Requis ?	Type
`DisplayLog`	Affiche le fichier journal à la fin de l'applet de commande. Définissez sur `$false` pour supprimer l'affichage du journal.		`$true or $false`

Renvoie :

- Voir Valeurs de retour de l'applet de commande

Fusion de plusieurs applets de commande de sites locaux

Pour plus d'informations sur la fusion de sites et l'utilisation de ces applets de commande, consultez la rubrique Fusion de plusieurs sites en un seul site.

- `New-CvadAcSiteMergingInfo` - crée un jeu d'informations préfixe/suffixe de fusion de site. Il n'est pas nécessaire de connaître tous les préfixes ou suffixes au début. Ils peuvent être mis à jour avec `Set-CvadAcSiteMergingInfo` ou en modifiant manuellement le fichier SiteMerging.yml.
  Paramètres :

Nom	Description	Requis ?	Type
`SiteName`	Nom utilisé pour identifier l'ensemble de préfixes/suffixes pour un site spécifique. Il peut correspondre au nom du site, mais ce n'est pas obligatoire.	x	Chaîne
Paramètres de fusion de sites	Voir Paramètres de fusion de sites		SwitchParameters
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter

Renvoie :

- Aucun

- `Set-CvadAcSiteMergingInfo` - met à jour un jeu d'informations préfixe/suffixe de fusion de site existant.

Paramètres :

Nom	Description	Requis ?	Type
`SiteName`	Nom utilisé pour identifier l'ensemble de préfixes/suffixes pour un site spécifique. Il peut correspondre au nom du site, mais ce n'est pas obligatoire.	x	Chaîne
Paramètres de fusion de sites	Voir Paramètres de fusion de sites		SwitchParameters
`Quiet`	Supprime la journalisation sur la console.		SwitchParameter

Renvoie :

- Aucun

- `Remove-CvadAcSiteMergingInfo` - supprime un jeu d'informations préfixe/suffixe de fusion de site existant.

  Paramètres :

  - `SiteName` —Identifie l'ensemble des préfixes et suffixes de site. Il s'agit d'une chaîne de caractères qui est obligatoire.

  Renvoie :

  - Aucun

Paramètres de fusion de sites

Les paramètres suivants peuvent être utilisés lors de l'exécution des applets de commande de fusion de sites. Tous les paramètres répertoriés sont des chaînes.

- `SiteName` - nom utilisé pour identifier l'ensemble de préfixes/suffixes pour un site spécifique. Il peut correspondre au nom du site, mais ce n'est pas obligatoire. SiteName est un paramètre obligatoire.
- `AdminScopedPrefix` - préfixe à appliquer aux étendues administrateur.
- `ApplicationPrefix` - préfixe à appliquer aux applications.

- `ApplicationFolderPrefix` - préfixe à appliquer aux dossiers d'application ; `ApplicationFolderP` peut être combiné avec `ApplicationFolderRoot`.
- `ApplicationFolderRoot` - nouveau dossier racine des dossiers d'application. Ce paramètre crée une hiérarchie de dossiers supplémentaire. `ApplicationFolderRoot` peut être combiné avec `ApplicationFolderPrefix`.
- `ApplicationGroupPrefix` - préfixe pour les groupes d'applications.
- `ApplicationUserPrefix` - préfixe à appliquer au nom de l'application que l'utilisateur voit.
- `ApplicationAdminPrefix` - préfixe à appliquer au nom de l'application que l'administrateur voit.
- `DeliveryGroupPrefix` - préfixe à appliquer aux groupes de mise à disposition.
- `GroupPolicyPrefix` - préfixe à appliquer aux noms de stratégie.
- `HostConnectionPrefix` - préfixe à appliquer aux connexions hôtes.
- `MachineCatalogPrefix` - préfixe à appliquer aux catalogues de machines.
- `StoreFrontPrefix` - préfixe à appliquer aux noms StoreFront.
- `TagPrefix` - préfixe à appliquer aux balises.
- `AdminScopedSuffix` - suffixe à appliquer aux étendues administrateur.
- `ApplicationSuffix` - suffixe à appliquer aux applications.
- `ApplicationFolderSuffix` - suffixe à appliquer aux dossiers d'application ; `ApplicationFolderS` peut être combiné avec `ApplicationFolderRoot`.
- `ApplicationGroupSuffix` - suffixe pour les groupes d'applications.
- `ApplicationUserSuffix` - suffixe à appliquer au nom de l'application que l'utilisateur voit.
- `ApplicationAdminSuffix` - suffixe à appliquer au nom de l'application que l'administrateur voit.
- `DeliveryGroupSuffix` - suffixe à appliquer aux groupes de mise à disposition.
- `GroupPolicySuffix` - suffixe à appliquer aux noms de stratégie.
- `HostConnectionSuffix` - suffixe à appliquer aux connexions hôtes.
- `MachineCatalogSuffix` - suffixe à appliquer aux catalogues de machines.
- `StoreFrontSuffix` - suffixe à appliquer aux noms StoreFront.
- `TagSuffix` - suffixe à appliquer aux balises.
- `SiteRootFolder` - nom de dossier complet à utiliser pour les exportations et les importations ; il peut s'agir d'un dossier local ou d'un partage de fichiers.

Paramètres génériques

Paramètres d'accès au cloud

Toutes les applets de commande accédant au cloud prennent en charge les paramètres supplémentaires suivants.

> **Remarque :**
>
> CustomerID, ClientID et Secret peuvent être placés dans le fichier CustomerInfo.yml ou spécifiés avec l'applet de commande à l'aide des paramètres suivants. Lorsqu'ils sont spécifiés aux deux emplacements, les paramètres de l'applet de commande ont priorité.

- `CustomerId` - ID client utilisé dans les API REST, requis pour accéder à toutes les API REST. Votre ID client se trouve dans Citrix Cloud.
- `ClientId` - ID client créé sur le site Web Gestion des identités et des accès de Citrix Cloud. Ceci est nécessaire pour obtenir le jeton de porteur requis pour l'authentification de toutes les API Rest.
- `Secret` - clé secrète créée sur le site Web Gestion des identités et des accès de Citrix Cloud. Ceci est nécessaire pour obtenir le jeton de porteur requis pour l'authentification de toutes les API Rest.
- `CustomerInfoFileSpec` - spécification de fichier pointant vers un fichier d'informations client pour remplacer l'emplacement et le nom par défaut.

Paramètres des modes de migration

Les applets de commande modifiant la configuration du site cloud (`Import`, `Restore`, `Merge`, `New` et `Sync`) prennent en charge les paramètres supplémentaires suivants pour offrir une plus grande flexibilité.

- `CheckMode` - Effectue l'opération d'importation mais n'apporte *aucune* modification. Toutes les modifications attendues sont signalées avant la fin de l'importation. Vous pouvez utiliser cette commande pour tester votre importation avant de l'effectuer.
- `BackupFirst` - Sauvegarde le contenu du cloud dans des fichiers .yml avant de modifier la configuration du cloud. Cette option est activée par défaut.
- `Confirm` - Lorsque la valeur est true, invite les utilisateurs à confirmer qu'ils souhaitent apporter des modifications à la configuration du site cloud. L'applet de commande `Remove` affiche une invite en raison de sa nature destructrice. Définissez la valeur false si aucune invite n'est souhaitée, comme pour l'exécution dans des scripts automatisés. `Confirm` est true par défaut.
- `SecurityFileFolder` - dossier complet contenant le fichier CustomerInfo.yml qui peut pointer vers un dossier local ou un dossier de partage réseau sous contrôle d'authentification. L'outil ne demandera pas d'informations d'identification ; l'accès à la ressource contrôlée doit être obtenu avant d'exécuter l'outil.
- `SiteName` - spécifie le préfixe et le suffixe de fusion de sites à utiliser lors de l'importation.
- `SiteActive` - indique si le site importé est actif ou inactif. Par défaut, ce paramètre est défini sur `$false`, ce qui signifie que le site importé est inactif.

Paramètres d'affichage du journal

Les applets de commande `Export`, `Import`, `Sync`, `Restore`, `Backup`, `Compare` et `Remove` affichent le fichier du journal lorsque l'opération se termine. Vous pouvez supprimer l'affichage en définissant le paramètre `-DisplayLog` sur `$false`. Notepad.exe est utilisé par défaut pour afficher le fichier journal. Vous pouvez spécifier un éditeur différent dans le fichier CustomerInfo.yml.

```
Editor: C:\Program Files\Notepad++\notepad++.exe
```

Valeurs de retour de l'applet de commande

ActionResult

Toutes les applets de commande renvoient la valeur suivante.

```
1              public class ActionResult
2              {
3
4                  public bool                          Overall_Success;
5                  public Dictionary<string, string>    Individual_Success;
6                  public object                        CustomResult;
7               }
```

`Overall_Success` renvoie un seul booléen indiquant le succès global de l'applet de commande sur tous les composants sélectionnés : true signifie succès et false signifie échec.

`Individual_Success` renvoie une ou trois valeurs pour chaque composant principal. Le résultat d'un composant peut être Success, Failure ou Skipped. Skipped indique que le composant n'a pas été sélectionné pour l'exécution par l'applet de commande.

`CustomResult` est spécifique à l'applet de commande.

CustomResult

`Import`, `Merge`, `Restore`, `Sync`, `Compare`, `Compare File` et `Remove` renvoient les informations de résultat personnalisées suivantes à une seule instance de `EvaluationResultData`.

> **Remarque :**
>
> Les applets de commande `Export` et `Template` ne renvoient pas de résultat personnalisé.

```
1                  public class EvaluationResultData
2                  {
3
4                      public Dictionary<string, Dictionary<string,
                           ActionResultValues >> EvaluationResults;
```



```
5                       public int                  Added;
6                       public int                  Updated;
7                       public int                  Deleted;
8                       public int                  NoChange;
9                       public int                  TotalChanged;
10                      public EvaluationResults     OverallResult;
11                      public string               CloudBackupFolder;
12                      public string               SourceBackupFolder;
13                   }
14
15                  Where:
16                  public enum ActionResultValues
17                 {
18
19                      Add,
20                      Update,
21                      Delete,
22                      Identical,
23                      DoNothing
24                   }
25
26                  public enum EvaluationResults
27                  {
28
29                      Success,
30                      Failure,
31                      Skipped
32                   }
```

`EvaluationResults` affiche une liste avec une entrée par composant sélectionné. La clé est le nom du composant et la valeur est une liste de chaque membre de composant et de l'action effectuée sur ce membre. Les actions peuvent être l'une des valeurs `ActionResultValues`.

`Added`, `Updated`, `Deleted` et `NoChange` indiquent le nombre total de membres de composants ajoutés, mis à jour, supprimés ou sur lesquels aucune action n'a été effectuée, dans cet ordre.

`TotalChanged` est la somme de `Added`, `Updated` et `Deleted`.

`OverallResult` est un booléen unique indiquant le résultat de l'applet de commande. True indique le succès total de tous les composants et false indique l'échec du traitement d'un ou de plusieurs composants.

`CloudBackupFolder` est la spécification de fichier complète de la sauvegarde de la configuration du site cloud avant que l'applet de commande effectue des actions de modification du cloud.

`SourceBackupFolder` est la spécification de fichier complète de la sauvegarde du fichier source effectuée après la fin de l'applet de commande. Par défaut, ces fichiers se trouvent sous *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Aide de PowerShell

L'aide de PowerShell est disponible pour chaque applet de commande. Tous les paramètres sont documentés avec chaque applet de commande et une brève explication de l'applet de commande est également proposée. Pour accéder à l'aide d'une applet de commande, tapez `Get-Help` devant l'applet de commande.

```
Get-Help Import-CvadAcToSite
```

Dépannage de la configuration automatisée et informations supplémentaires

March 30, 2024

> **Important :**
>
> Pour connaître les messages d'erreur courants relatifs à la configuration automatisée et aux solutions correspondantes, consultez la *FAQ sur le dépannage* de l'article CTX277730 du centre de connaissances.

Erreurs de l'outil de configuration automatisée

Les opérations de l'outil de configuration automatisée peuvent parfois générer des erreurs. Dans ce cas, des défaillances peuvent survenir lors du traitement de composants tels que des catalogues de machines, des groupes de mise à disposition ou des stratégies de groupe, par exemple. L'utilisation des paramètres `OnErrorAction` et de continuation vous permet de détecter les erreurs en cours de traitement, de les résoudre et de reprendre là où vous vous êtes arrêté.

La valeur par défaut de `OnErrorAction` est `StopCompEnd`. Lorsqu'une erreur se produit, l'outil termine le traitement du composant actuel. Aucun composant supplémentaire n'est traité et les erreurs ne se répercutent pas sur les composants dépendants en aval. Une fois les erreurs résolues, vous pouvez réexécuter vos applets de commande en appliquant n'importe quel paramètre de continuation.

Paramètre OnErrorAction

Vous pouvez définir les valeurs du paramètre `OnErrorAction` sur les commandes de migration afin de contrôler la manière dont l'outil répond aux erreurs détectées lors du traitement des composants.

Ce tableau présente les valeurs du paramètre et leurs descriptions :

Valeur	Description
`Continue`	Essaie de traiter autant de composants que possible.
`Pause`	S'arrête à la fin du traitement et vous invite à continuer ou à arrêter.
`StopCompEnd`	Essaie de traiter la plus grande partie possible du composant. S'arrête une fois que le composant est terminé. (par défaut)
`StopImmediately`	Le traitement s'arrête lorsqu'une erreur est détectée.

Applets de commande de migration

Vous pouvez appliquer le paramètre `OnErrorAction` aux commandes de migration suivantes :

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`
- `Restore-CvadAcToSite`

Exemple : `Merge-CvadAcToSite -OnErrorAction StopImmediately`

Paramètres de reprise

Ces paramètres définissent la manière dont l'outil reprend après une pause ou l'arrêt d'une opération en raison d'une erreur.

Vous pouvez appliquer des paramètres de reprise aux applets de commande de migration qui incluent l'une des valeurs de paramètre `OnErrorAction` suivantes :

- `Pause`
- `StopCompEnd`
- `StopImmediately`

Ce tableau présente les valeurs du paramètre et leurs descriptions :

Valeur	Description
`-AllRemaining`	Nécessite un composant de départ. Le traitement commence au niveau du composant de départ et traite tous les composants restants. Plusieurs composants sont traités.
`-Resume`	Utilise le composant de `CurrentComponent.txt` comme point de départ. Tout ce qui reste est défini sur true. Plusieurs composants sont traités.
`-Repeat`	Utilise le composant de `CurrentComponent.txt` comme point de départ. Tout ce qui reste est défini sur false. Un seul composant est traité.

Le dernier composant traité est stocké dans le fichier `CurrentComponent.txt` du dossier Auto-Config. Il n'est pas recommandé de modifier ce fichier.
Si vous spécifiez `-Resume` ou `-Repeat` et que le fichier `CurrentComponent.txt` est manquant ou non valide, le traitement s'arrête et vous êtes invité à sélectionner un composant.

Configuration de l'action OnErrorAction dans le fichier CustomerInfo.yml

Vous pouvez également définir des valeurs de `OnErrorAction` dans le fichier `CustomerInfo.yml`. Définissez les valeurs à l'aide des applets de commande suivantes :

- Pour un nouveau fichier : `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- Pour un fichier existant : `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

Journaux

L'exécution d'une applet de commande entraîne la création d'un fichier journal et une entrée dans le fichier journal de l'historique principal. Tous les fichiers journaux d'opérations sont placés dans un dossier de sauvegarde. Tous les noms de fichiers journaux commencent par `CitrixLog`, puis affichent l'opération de configuration automatique ainsi que l'horodatage de l'exécution de l'applet de commande. Les journaux ne sont pas supprimés automatiquement.

Le journal de l'historique principal se trouve dans `*%HOMEPATH%\Documents\Citrix\AutoConfig*`, dans le fichier **History.Log**. Chaque exécution de l'applet de commande entraîne

une entrée de journal principal contenant la date, l'opération, le résultat, la sauvegarde et les emplacements du fichier journal de l'exécution.

Vous pouvez également utiliser l'applet de commande `New-CvadAcZipInfoForSupport` pour collecter des journaux à envoyer à Citrix pour obtenir de l'aide. Cette applet de commande compresse tous les fichiers journaux et .yml dans un seul fichier zip. Les informations sensibles du client (CustomerInfo.yml et CvadAcSecurity.yml) ne sont pas incluses dans le zip. Le fichier Icon.yml est également exclu en raison de sa taille. Le fichier zip est placé dans *%HOMEPATH%\Documents\Citrix\AutoConfig* et nommé *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, en fonction de la date et de l'horodatage. Ce fichier zip peut également servir de sauvegarde.

Chaque fichier journal comprend les éléments suivants :

- Nom de l'opération et si le mode de vérification est activé
- Date et heure de début et de fin
- Entrées multiples pour les actions et les notifications de réussite/échec de chaque composant
- Résumé des actions effectuées, y compris les différents dénombrements d'objets créés
- Corrections suggérées, le cas échéant
- Emplacement du dossier de sauvegarde, le cas échéant
- Emplacement du journal principal
- Durée

Fichiers de diagnostic

Les fichiers de diagnostic vous aident à déterminer et à résoudre les problèmes. Les fichiers suivants sont créés lors de l'exécution de leur opération. Ils se trouvent dans le sous-dossier spécifique à l'action sous *%HOMEPATH%\Documents\Citrix\AutoConfig*. Incluez ces fichiers lorsque vous fournissez des informations à l'équipe d'assistance pour la résolution de problèmes.

Exporter

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

Ce fichier compte tous les appels SDK PowerShell de Broker effectués pour exporter la configuration du site vers des fichiers.

Import, Merge, Restore, Sync, Backup, Compare

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

Ce fichier documente chaque appel d'API Rest et les informations connexes.

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

Ce fichier contient tout le contenu de l'API Rest `Add`, `Update` et `Delete`.

Problèmes résultant des dépendances

Les importations et les fusions peuvent échouer en raison de dépendances manquantes. Voici quelques problèmes courants :

1. Des filtres de groupe de mise à disposition manquent dans les stratégies de groupe. C'est en général parce que des groupes de mise à disposition n'ont pas été importés.
2. Échec de l'importation ou de la fusion des applications. C'est en général parce que des groupes de mise à disposition manquent ou des groupes d'applications n'ont pas été importés.
3. Il manque un RestrictToTag dans les groupes d'applications. C'est en général parce que des balises n'ont pas été importées.
4. Les connexions d'hôte échouent. C'est en général parce que des informations de sécurité manquent dans le fichier CvadAcSecurity.yml.
5. Les catalogues de machines échouent. C'est en général parce que des connexions d'hôte n'ont pas été importées.
6. Machines manquantes dans des catalogues de machines et des groupes de mise à disposition. C'est en général parce que des machines n'ont pas été trouvées dans Active Directory.
7. Utilisateurs manquants dans des groupes de mise à disposition. C'est en général parce que des utilisateurs sont introuvables dans Active Directory.

Recommandations

- N'exécutez pas plus d'une instance de l'outil de configuration automatisée à la fois. L'exécution de plusieurs instances simultanées produit des résultats imprévisibles sur le site cloud. Si cela se produit, réexécutez une instance de l'outil de configuration automatisée pour amener le site à l'état attendu.
- Ne modifiez pas les données dans l'onglet Gérer de l'interface Configuration complète pendant l'exécution de la configuration automatisée.
- Vérifiez toujours visuellement les résultats de fusion, d'importation ou de restauration dans l'interface Configuration complète pour vous assurer que le site cloud répond aux attentes.

Dossiers

Emplacement racine du dossier par défaut

Toutes les opérations de l'outil de configuration automatisée s'effectuent dans le dossier racine ou dans les sous-dossiers qu'il contient. Le dossier racine se trouve sous *%HOMEPATH%\Documents\Citrix\AutoConfig*.

Exporter

Tous les fichiers exportés sont placés dans deux emplacements de dossier, ce qui offre une facilité d'utilisation et un historique des exportations. Les exportations sont toujours placées dans le dossier racine. Les copies sont placées dans un sous-dossier nommé **Export** avec la date et l'heure de l'exportation.

Le dossier racine contient toujours la configuration de site locale exportée la plus récente. Chaque sous-dossier **Export** contient l'exportation effectuée à la date et à l'heure indiquées, ce qui permet de conserver un historique des exportations. Vous pouvez utiliser n'importe quel sous-dossier **Export** pour configurer le site cloud. L'outil de configuration automatisée ne supprime pas et ne modifie pas les sous-dossiers d'exportation existants.

Import/Merge/Sync/Compare

Les opérations `Import`, `Merge` et `Compare` proviennent toujours de fichiers situés dans le dossier racine. Chaque opération entraîne la création d'un sous-dossier dans lequel les fichiers du dossier racine sont copiés, fournissant ainsi un historique des modifications des fichiers source du site cloud.

Restaurer

L'opération `Restore` utilise un sous-dossier existant pour configurer le site cloud. Le dossier source est spécifié sur le paramètre `-RestoreFolder` requis. Contrairement aux autres commandes, aucun nouveau sous-dossier n'est créé car l'opération `Restore`utilise un sous-dossier existant. Le dossier de restauration peut être le dossier racine mais doit toujours être spécifié sur le paramètre `-RestoreFolder`.

Sauvegardes

L'outil de configuration automatisée initialise, met à jour et sauvegarde la configuration d'un site cloud. Au fil du temps, de nombreuses configurations différentes peuvent changer sur le site cloud. Pour faciliter l'utilisation à long terme et préserver l'historique des changements, l'outil de configuration automatisée utilise un schéma de conservation pour sauvegarder cet historique et fournir une méthode pour restaurer les états antérieurs.

Les sauvegardes de configuration de site cloud sont toujours effectuées dans un sous-dossier nommé **Backup** avec les données et l'heure de la sauvegarde. L'outil de configuration automatisée ne supprime pas et ne modifie pas les sous-dossiers d'exportation existants.

Vous pouvez utiliser les sauvegardes pour restaurer des composants spécifiques ou l'intégralité de votre configuration. Pour restaurer l'ensemble des composants Groupe de mise à disposition et Catalogue de machines, utilisez l'applet de commande :

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **Remarque :**
>
> Les informations du fichier de sauvegarde de l'applet de commande précédente sont basées sur vos propres sauvegardes.

Pour restaurer l'intégralité de la configuration du site cloud, utilisez l'applet de commande :

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

> **Remarque :**
>
> Les informations du fichier de sauvegarde de l'applet de commande précédente sont basées sur vos propres sauvegardes.

Modification du dossier racine par défaut

Les opérations `Export`, `Import`, `Merge`, `Sync` et `Compare` peuvent modifier le dossier racine par défaut à l'aide du paramètre `–AlternateFolder`. La création et la gestion des sous-dossiers par opération restent les mêmes que celles décrites précédemment.

Fichiers copiés dans des sous-dossiers

Tous les fichiers ayant une extension « .yml » sont copiés dans les sous-dossiers d'opération, à l'exception des éléments suivants :

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

Sauvegardes automatisées de site cloud en mode sans échec

Une sauvegarde de la configuration actuelle du site cloud est effectuée avant d'exécuter les opérations qui modifient la configuration. Cela inclut les paramètres `Import`, `Merge`, `Sync` et `Restore`. La sauvegarde se trouve toujours dans un sous-dossier situé sous le sous-dossier opérationnel.

Dans le cas de `Restore`, le dossier de sauvegarde est un sous-dossier du dossier spécifié sur le paramètre `-RestoreFolder`.

Automatisation

Les applets de commande de l'outil configuration automatisée peuvent être exécutées dans des scripts d'automatisation sans intervention de l'administrateur en supprimant les invites et l'affichage des résultats du journal à la fin de l'applet de commande. Vous pouvez également définir des paramètres pour faire de même à l'aide du fichier CustomerInfo.yml.

Ajoutez le paramètre suivant aux applets de commande de modification du cloud pour supprimer l'affichage des invites.

```
-Confirm $false
```

Ajoutez le paramètre suivant aux applets de commande pour supprimer l'affichage du journal à la fin de l'applet de commande.

```
-DisplayLog $false
```

Ajoutez le paramètre suivant aux applets de commande pour supprimer la journalisation dans la fenêtre de commande PowerShell.

```
-Quiet
```

Une autre méthode consiste à placer les paramètres suivants dans le fichier CustomerInfo.yml.

```
Confirm: False
```

```
DisplayLog: False
```

Exportation à partir d'ordinateurs autres que le Delivery Controller

L'outil de configuration automatisée utilise plusieurs SDK PowerShell Citrix pour exporter la configuration de site local vers des fichiers. Ces SDK sont automatiquement installés sur le Delivery Controller, ce qui permet à l'outil de s'exécuter sur le Delivery Controller sans actions supplémentaires. Lors de l'exécution sur des machines non Delivery Controller, il est nécessaire d'installer l'ensemble de SDK PowerShell Citrix requis par l'outil. Cet ensemble de SDK fait partie de Citrix Studio qui peut être installé à partir du support d'installation Citrix Virtual Apps and Desktops.

> **Remarque :**
>
> L'outil de configuration automatisée ne peut pas être exécuté sur le Cloud Connector.

Migration vers Citrix Cloud Government et Japan Control Plane

Les environnements Citrix Cloud Government et Japan Control Plane utilisent différents points d'accès pour authentifier et allouer des jetons d'accès. Cette exigence unique s'applique à tout outil de configuration automatisée accédant au cloud. Effectuez la procédure suivante pour utiliser la configuration automatisée dans ces environnements.

1. Dans le dossier *%CHEMINDEBASE%\Documents\Citrix\AutoConfig*, modifiez CustomerInfo.yml.
2. Ajoutez l'une des lignes suivantes, en fonction de l'environnement auquel vous souhaitez vous connecter, à CustomerInfo.yml (ou modifiez-la, si elle est déjà présente).

   ```
   Environment: 'ProductionGov'
   ```

   ou

   ```
   Environment: 'ProductionJP'
   ```

La configuration automatisée peut désormais être utilisée dans ces environnements.

Collecte de données Citrix Cloud

Pour en savoir plus sur les informations collectées par Citrix Cloud, consultez la section Gestion du contenu client et des journaux de Citrix Cloud Services.

Ressources supplémentaires

Forum de discussion

Visitez le Forum de discussion Citrix pour la configuration automatisée.

Vidéo

Regardez Under the Hood of the Automated Configuration Tool for Citrix Virtual Apps and Desktops sur YouTube.

Formation

Le Cloud Learning Center contient des guides vidéo étape par étape sur la création d'un déploiement de services, y compris les tâches décrites dans cet article. Voir Migrating Citrix Virtual Apps and Desktops to Citrix Cloud Learning Path.

Migrer les charges de travail entre les emplacements de ressources à l'aide du service de portabilité des images

May 17, 2024

Le service de portabilité des images simplifie la gestion des images sur toutes les plateformes. Les API REST Citrix Virtual Apps and Desktops peuvent être utilisées pour automatiser l'administration des ressources au sein d'un site Citrix Virtual Apps and Desktops.

Le flux de travail de portabilité des images commence lorsque vous utilisez Citrix Cloud pour démarrer la migration d'une image entre deux emplacements de ressources. Après avoir exporté votre image, le service de portabilité des images vous aide à transférer et à préparer l'image en vue de son exécution sur l'hyperviseur ou le cloud public cible. Enfin, Citrix Provisioning ou Machine Creation Services provisionne l'image dans l'environnement cible.

Composants

Les composants du service de portabilité des images incluent :

- Citrix Cloud Services
- Citrix Credential Wallet
- Appliance Connector Citrix
- VM du moteur de composition
- Exemples de scripts PowerShell

Citrix Cloud Services

L'API Citrix Cloud Services est un service d'API REST qui interagit avec le service de portabilité des images. À l'aide du service d'API REST, vous pouvez créer et surveiller les tâches de portabilité des images. Par exemple, vous effectuez un appel d'API pour démarrer une tâche de portabilité des images, comme exporter un disque, puis effectuez des appels pour obtenir l'état de la tâche.

Citrix Credentials Wallet

Le service Citrix Credentials Wallet gère en toute sécurité les informations d'identification système, ce qui permet au service de portabilité des images d'interagir avec vos ressources. Par exemple, lors de l'exportation d'un disque de vSphere vers un partage SMB, le service de portabilité des images a besoin d'informations d'identification pour ouvrir une connexion au partage SMB afin d'écrire sur

le disque. Si les informations d'identification sont stockées dans le Credentials Wallet, le service de portabilité d'images peut récupérer et utiliser ces informations d'identification.

Ce service vous permet de gérer entièrement vos informations d'identification. L'API Cloud Services agit en tant que point d'accès, vous donnant la possibilité de créer, de mettre à jour et de supprimer des informations d'identification.

Moteur de composition

Le moteur de composition est le cœur du service de portabilité des images. Le moteur de composition (CE) est une machine virtuelle unique créée au début d'une tâche d'exportation ou de préparation de portabilité des images. Ces machines virtuelles sont créées dans le même environnement que celui dans lequel la tâche a lieu. Par exemple, lors de l'exportation d'un disque à partir de vSphere, le CE est créé sur le serveur vSphere. De même, lors de l'exécution d'une tâche de préparation dans Azure, AWS ou Google Cloud, le CE est créé dans Azure, AWS ou Google Cloud, respectivement. Le CE monte votre disque sur lui-même, puis effectue les manipulations nécessaires sur le disque. À la fin de la tâche de préparation ou d'exportation, la machine virtuelle CE et tous ses composants sont supprimés.

Appliance Connector

L'appliance Connector, qui exécute le logiciel du fournisseur pour gérer les ressources IPS, s'exécute dans votre environnement (à la fois sur site et dans votre abonnement Azure, AWS ou Google Cloud) et agit en tant que contrôleur pour les tâches individuelles. Elle reçoit les instructions de tâche du service cloud et crée et gère les machines virtuelles du moteur de composition. La machine virtuelle de l'appliance Connector agit comme un point de communication unique et sécurisé entre les services cloud et vos environnements. Déployez une ou plusieurs appliances Connector dans chacun de vos emplacements de ressources (sur site, Azure, AWS ou Google Cloud). Une appliance Connector est déployée sur chaque emplacement de ressources pour des raisons de sécurité. En co-localisant l'appliance Connector et le moteur de composition, vous augmentez considérablement la posture de sécurité du déploiement, car tous les composants et les communications sont conservés dans votre emplacement de ressources.

Modules PowerShell

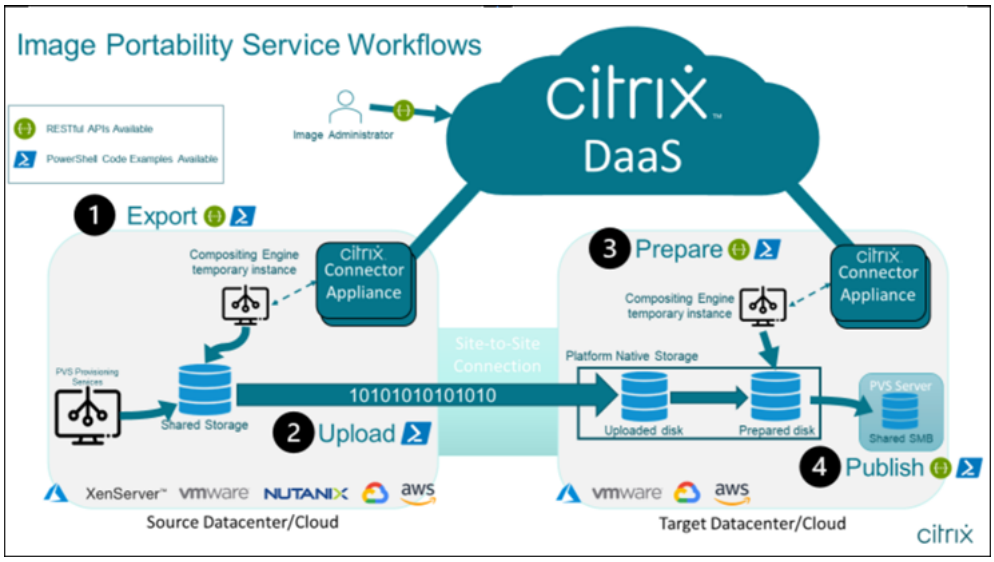
Nous fournissons un ensemble de modules PowerShell à utiliser dans des scripts comme point de départ pour développer votre propre automatisation personnalisée. Les modules fournis sont pris en charge tels quels, mais vous pouvez les modifier si nécessaire pour votre déploiement.

L'automatisation PowerShell utilise les paramètres de configuration fournis pour composer un appel REST vers le service d'API Citrix Cloud afin de démarrer la tâche, puis vous fournir des mises à jour périodiques au fur et à mesure de l'avancement de la tâche.

Si vous souhaitez développer votre propre solution d'automatisation, vous pouvez envoyer des appels directement au service cloud en utilisant le langage de programmation de votre choix. Consultez le portail des API pour obtenir des informations détaillées sur la configuration et l'utilisation des points de terminaison REST et des modules PowerShell du service de portabilité des images.

Workflows

Le service de portabilité des images utilise un flux de travail en plusieurs phases pour préparer une image de catalogue principal à partir d'un emplacement de ressources sur site pour votre abonnement à un cloud public. Le service exporte l'image à partir de la plate-forme de l'hyperviseur local et vous la téléchargez sur votre abonnement cloud (l'utilitaire de téléchargement PowerShell que nous fournissons peut vous aider à automatiser cela). Ensuite, la portabilité des images prépare l'image pour qu'elle soit compatible avec votre plateforme de cloud public. Enfin, l'image est publiée et prête à être déployée en tant que nouveau catalogue de machines au sein de votre emplacement de ressources cloud.



Ces flux de travail de haut niveau sont basés sur la configuration de provisioning source et cible de l'image (Machine Creation ou Citrix Provisioning). Le flux de travail choisi détermine les étapes des tâches de portabilité des images requises.

Reportez-vous au tableau suivant pour savoir quelles tâches sont requises pour chacun des flux de travail IPS pris en charge.

Flux de travail (de la source à la cible)	Exporter	Charger	Préparer	Publier
MCS vers MCS	O	O	O	N

Flux de travail (de la source à la cible)	Exporter	Charger	Préparer	Publier
PVS vers MCS*	N	O	O	N
PVS vers PVS	S/O	O	O	O
MCS vers PVS	O	O	O	O

*Suppose que vous disposez de l'image d'origine en tant que Citrix Provisioning vDisk et que vous n'avez pas besoin de l'exporter directement hors de l'hyperviseur de la plate-forme source.

Exigences

Pour commencer à utiliser la portabilité des images, vous devez répondre aux exigences suivantes.

Une image du catalogue de machines Citrix

L'IPS nécessite l'utilisation d'images ayant l'une des configurations testées suivantes :

- Windows Server 2016, 2019 et 2022H2
- Windows 10 ou 11
- Provisioning à l'aide de Machine Creation Services ou Citrix Provisioning
- Citrix Virtual Delivery Agent :
  - Les deux dernières mises à jour cumulatives pour 1912 et 2203 LTSR
  - Les deux dernières versions actuelles
- Services Bureau à distance activés pour l'accès à la console dans Azure

Le service de portabilité des images prend en charge les hyperviseurs et les plates-formes cloud suivants :

Plates-formes sources :

- VMware vSphere 7.0 et 8.0
- XenServer 8/Citrix Hypervisor 8.2
- Nutanix AHV (Prism Element uniquement)
- Microsoft Azure
- Google Cloud Platform

Plates-formes de destination :

- VMware vSphere 8.0
- XenServer 8/Citrix Hypervisor 8.2
- Nutanix AHV (Prism Element uniquement)
- Microsoft Azure
- AWS
- Google Cloud Platform

Appliance Connector Citrix

Vous devez disposer d'une appliance Connector Citrix installée et configurée dans chaque emplacement de ressources où vous prévoyez d'utiliser la portabilité des images. Par exemple, si vous utilisez la portabilité des images pour déplacer une image de vSphere vers Azure, AWS et Google Cloud, vous avez besoin d'au moins trois Citrix Connector Appliances :

Consultez Déployer des appliances Connector pour obtenir des instructions détaillées.

Un partage de fichiers SMB (Windows)

Vous avez besoin d'un **partage de fichiers SMB** Windows pour le stockage de la sortie des tâches d'exportation. Le partage doit être accessible à la machine virtuelle du moteur de composition qui sera créée dans l'emplacement des ressources où vous utilisez le service de portabilité des images. Assurez-vous que l'espace libre disponible sur le partage est au moins le double de la taille configurée du système de fichiers de votre image.

Une machine pour exécuter des scripts PowerShell

Assurez-vous que votre machine exécutant les scripts PowerShell présente les caractéristiques suivantes :

- PowerShell version 5.1.
- Une connexion réseau rapide au partage de fichiers SMB. Il peut s'agir de la machine qui héberge le partage de fichiers.
- Une connexion réseau rapide aux plateformes de cloud public sur lesquelles vous prévoyez d'utiliser la fonctionnalité de portabilité des images. Par exemple, Azure, AWS ou Google Cloud.

  Consultez la section Préparer une machine pour PowerShell pour plus d'informations sur la façon de télécharger et de configurer les modules de portabilité des images à partir de la galerie PowerShell.

Votre numéro client Citrix Cloud

Vérifiez que vous disposez d'un abonnement Citrix DaaS valide.

Pour continuer, vous devez accéder à Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Si vous n'y avez pas accès, contactez votre représentant Citrix.

Reportez-vous à la documentation API Getting Started pour obtenir des instructions sur la création et la configuration d'un client API à utiliser avec la portabilité des images.

Autorisations et configuration requises pour Azure

Pour que le service de portabilité des images effectue des actions dans votre ressource Azure, vous devez accorder des autorisations sur certaines fonctionnalités Azure au principal du service Azure utilisé par le service de portabilité des images. Pour obtenir la liste détaillée, consultez Autorisations requises par Microsoft Azure.

Vous pouvez attribuer le rôle **Contributeur** au principal de service dans la ressource associée. Ou, pour attribuer les autorisations minimales requises, vous pouvez créer des rôles personnalisés avec les autorisations requises et les attribuer au principal de service défini pour les ressources appropriées.

Reportez-vous à la documentation Azure pour configurer les rôles de sécurité pour votre principal de service Azure et pour créer des rôles personnalisés.

Autorisations et configuration requises pour Google Cloud

Pour que le service de portabilité des images effectue des actions dans votre projet Google Cloud, vous accordez des autorisations sur certaines fonctionnalités au principal du service Google Cloud utilisé par le service de portabilité des images.

Pour obtenir la liste détaillée, consultez Autorisations requises pour Google Cloud.

Vous pouvez attribuer ces autorisations à l'aide des rôles suivants :

- Éditeur Cloud Build
- Administrateur informatique
- Administrateur de l'espace de stockage
- Utilisateur du compte de service

Consultez la documentation Google Cloud pour plus d'informations sur la configuration des autorisations de compte de service.

Autorisations et configuration requises pour Amazon Web Services

Afin d'effectuer des flux de travail de service de portabilité des images avec un compte Amazon Web Services (AWS), l'utilisateur IAM (Identity and Access Management) doit disposer des autorisations appropriées.

Pour obtenir la liste détaillée, consultez la section Autorisations requises par AWS.

Configurer le service de portabilité des images

Pour configurer le service de portabilité des images, vous devez :

- Déployer des appliances Connector
- Préparer une machine pour PowerShell
- Ajouter des informations d'identification à Credential Wallet

Déployer des appliances Connector

La portabilité des images nécessite que les appliances Citrix Connector créent des tâches de portabilité des images. Les appliances Connector permettent de sécuriser les interactions avec vos environnements cloud publics et locaux. Les appliances Connector communiquent avec le service de portabilité des images pour générer des rapports sur l'état de la tâche et l'état général du service.

Pour déployer et configurer une appliance Connector dans votre environnement, suivez les étapes décrites dans Appliance Connector pour les services cloud.

Notez la configuration matérielle et l'accès au port réseau requis pour l'appliance lors de la planification de votre déploiement.

Lorsque votre appliance est déployée et enregistrée, les composants nécessaires pour activer la portabilité des images sont automatiquement installés.

Préparer une machine pour PowerShell

Pour vous aider à démarrer et à utiliser la portabilité des images, nous avons créé des modules PowerShell que vous pouvez personnaliser et utiliser avec le service.

Les sections suivantes expliquent comment préparer une machine à exécuter les scripts PowerShell. Ces scripts ne sont que quelques exemples. Modifiez-les ou améliorez-les en fonction de vos besoins.

> **Remarque :**
>
> Après l'installation initiale, utilisez **Update-Module** pour mettre à jour le module PowerShell.

Configuration requise pour PowerShell Pour utiliser les scripts PowerShell, vous devez disposer des éléments suivants :

- Un ordinateur Windows pour exécuter les scripts PowerShell qui pilotent les tâches de portabilité des images. La machine :
  - Est dotée de la dernière version de PowerShell.
  - Dispose d'une connexion réseau de 10 Gbit/s au minimum au partage de fichiers SMB sur site et d'une connexion rapide à votre cloud public (Azure, AWS ou Google Cloud, par exemple).
  - Peut être la machine hébergeant le partage de fichiers.
  - Exécute Windows 10, Windows Server 2019 ou Windows Server 2022, avec les derniers correctifs Microsoft.
  - Peut se connecter à la galerie Microsoft PowerShell pour télécharger les bibliothèques PowerShell requises.

Selon votre version de Windows, vous devrez peut-être désactiver la prise en charge de TLS 1.0/1.1. Reportez-vous à la documentation sur la prise en charge de TLS dans Microsoft PowerShell Gallery pour plus d'informations.

Par défaut, PowerShell ne s'authentifie pas automatiquement via un serveur proxy. Assurez-vous d'avoir configuré votre session PowerShell pour utiliser votre serveur proxy, conformément aux meilleures pratiques de Microsoft et de votre fournisseur de proxy.

Si vous constatez des erreurs lors de l'exécution des scripts PowerShell relatives à une version manquante ou ancienne de PowerShellGet, vous devez installer la dernière version comme suit :

```
Install-Module -Name PowerShellGet -Force -Scope CurrentUser -
    AllowClobber
<!--NeedCopy-->
```

Installer des bibliothèques et des modules Le service de portabilité des images s'appuie sur les bibliothèques de la galerie Microsoft PowerShell pour gérer les opérations de portabilité.

> **Important :**
>
> Après l'installation initiale, utilisez **Update-Module** pour installer les nouvelles versions.

1. Exécutez la commande PowerShell suivante pour télécharger les derniers modules :


```
Install-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
    Uploader" -Scope CurrentUser
<!--NeedCopy-->
```

- Pour modifier la variable d'environnement PATH :

  Appuyez sur **Y** et sur **Entrée** pour accepter.

- Pour installer le fournisseur NuGet :

  Appuyez sur **Y** et sur **Entrée** pour accepter.

- Si vous êtes informé d'un référentiel non approuvé :

  Appuyez sur **A** (Yes to All) et sur **Entrée** pour continuer.

2. Confirmez que tous les modules nécessaires ont été téléchargés en exécutant la commande :

```
Get-InstalledModule -Name Citrix.*
<!--NeedCopy-->
```

Cette commande renvoie une sortie similaire à la suivante :

Nom	Référentiel	Description
Citrix.Image.Uploader	PSGallery	Commandes pour télécharger un disque dur virtuel (x) sur un compte de stockage Azure, AWS ou GCP et obtenir des informations sur un disque dur virtuel (x)
Citrix.Workloads.Portability	PSGallery	Cmdlet autonome pour la tâche image du service de portabilité des images Citrix

Mettre à jour les modules vers la dernière version Exécutez la commande suivante pour mettre à jour le script vers la dernière version.

```
Update-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
    Uploader" -Force
<!--NeedCopy-->
```

Installer le SDK Citrix Virtual Apps and Desktops Remote PowerShell Le service de portabilité des images nécessite le SDK Citrix Virtual Apps and Desktops Remote PowerShell pour créer et gérer des tâches de portabilité dans Citrix Cloud.

Téléchargez et installez le SDK Remote PowerShell sur votre machine.

Installer des composants tiers spécifiques à la plateforme Le module PowerShell du service de portabilité des images n'installe pas de dépendances tierces. Par conséquent, vous pouvez limiter l'installation aux seules plateformes que vous ciblez. Si vous utilisez l'une des plateformes suivantes, suivez les instructions correspondantes pour l'installation des dépendances de plate-forme :

VMware Si vous créez des travaux de portabilité des images qui communiquent avec votre environnement VMware, exécutez la commande suivante pour installer les modules VMware PowerShell requis.

```
Install-Module -Name VMWare.PowerCLI -Scope CurrentUser -AllowClobber -
    Force -SkipPublisherCheck
<!--NeedCopy-->
```

Amazon Web Services Si vous créez des travaux de portabilité des images dans AWS, téléchargez et installez l'interface de ligne de commande AWS, puis exécutez ces commandes pour installer les modules Azure PowerShell requis :

```
Install-Module -Name AWS.Tools.Installer
Install-AWSToolsModule AWS.Tools.EC2,AWS.Tools.S3
<!--NeedCopy-->
```

Azure Si vous créez des travaux de portabilité des images dans Azure, téléchargez et installez les utilitaires de ligne de commande Azure, puis exécutez ces commandes pour installer les modules Azure PowerShell requis :

```
Install-Module -Name Az.Accounts -Scope CurrentUser -AllowClobber -
    Force
Install-Module -Name Az.Compute -Scope CurrentUser -AllowClobber -Force
<!--NeedCopy-->
```

Google Cloud Si vous créez des tâches de portabilité des images dans Google Cloud, téléchargez et installez le SDK Google Cloud sur votre machine.

Désinstaller les scripts et les modules Exécutez les commandes suivantes pour désinstaller les modules utilisés par le logiciel de portabilité des images.

> **Remarque :**
>
> Les scripts et composants tiers ne sont pas automatiquement supprimés lors de la désinstalla-

> tion des modules IPS.

Pour désinstaller les modules :

```
Get-InstalledModule -Name "Citrix.Workloads.Portability","Citrix.Images.Uploader" | Uninstall-Module
<!--NeedCopy-->
```

Ajouter des informations d'identification à Credential Wallet

Pour les scénarios d'automatisation de bout en bout, vous pouvez configurer le service de portabilité des images pour s'authentifier de manière non interactive auprès de Citrix Cloud, de votre cloud public et des ressources locales. En outre, le service de portabilité des images utilise les informations d'identification stockées dans Citrix Credential Wallet chaque fois que nos API s'authentifient directement auprès de vos ressources locales et dans le cloud public. La définition des informations d'identification telle que décrite dans cette section est une étape obligatoire pour exécuter des tâches d'exportation, de préparation et de publication.

Lors de l'exécution des tâches, le service de portabilité des images a besoin d'accéder à des ressources que vous pouvez contrôler. Par exemple, pour que le service de portabilité des images exporte un disque d'un serveur vSphere vers un partage SMB, le service a besoin d'un accès aux deux systèmes. Pour sécuriser ces informations de compte, le service de portabilité des images utilise le service Citrix Credential Wallet. Ce service stocke vos informations d'identification dans le service Wallet sous un nom défini par l'utilisateur. Lorsque vous souhaitez exécuter un travail, indiquez le nom des informations d'identification à utiliser. En outre, ces informations d'identification peuvent être mises à jour ou supprimées du service Wallet à tout moment.

Les informations d'identification sont souvent stockées pour ces plateformes :

- Microsoft Azure
- AWS
- Google Cloud
- Partage SMB
- VMware vSphere
- Nutanix AHV
- XenServer

Pour gérer les informations d'identification, reportez-vous à la section API du service de portabilité des images et Credentials Management du portail Developer API.

Utiliser le service de portabilité des images

La préparation d'images dans vos emplacements de ressources locaux pour votre abonnement à un cloud public nécessite la création de travaux de portabilité des images au sein de Citrix Cloud. Vous pouvez créer une tâche pour envoyer des appels d'API directs au service au sein de votre script ou programme, ou en utilisant les exemples de modules PowerShell que nous avons développés pour automatiser les appels d'API. Pour plus d'informations sur l'utilisation des API REST et des modules PowerShell pour créer des tâches IPS, reportez-vous au portail Image Portability Service Developer API.

Publier des catalogues de machines à l'aide de Citrix Provisioning

Le service de portabilité des images (IPS) est utilisé avec Machine Creation Services (MCS) dans Azure, AWS, Google Cloud, Nutanix, vSphere et XenServer, ou avec Citrix Provisioning (PVS) dans Azure, Google Cloud, vSphere et XenServer. Vous pouvez combiner les solutions PowerShell et REST décrites dans ce guide avec les outils de votre plateforme, les API de votre plate-forme ou les SDK Citrix DaaS pour créer un flux de travail de bout en bout transparent et automatisé permettant de créer un catalogue de machines basé sur l'image préparée. Selon la plate-forme cloud que vous avez choisie, des étapes intermédiaires peuvent être nécessaires entre la réalisation d'une tâche de préparation IPS et la création d'un catalogue ou d'une attribution à une cible PVS.

AWS Les tâches de préparation IPS sur AWS produisent un volume. Machine Creation Services nécessite une Amazon Machine Image (AMI) lors de la création du catalogue. Pour générer une AMI à partir de votre image migrée, vous devez d'abord créer un instantané d'image à partir du volume obtenu, puis créer une AMI basée sur cet instantané. Cela peut être effectué à l'aide de l'interface de ligne de commande (CLI) AWS :

```
1 > aws ec2 create-snapshot --volume-id <VolumeId>
2 > aws ec2 register-image --name <AmiName> --architecture 'x86_64' --
    root-device-name '/dev/sda1 --boot-mode uefi --ena-support --
    virtualization-type 'hvm' --block-device-mappings 'DeviceName=/dev/
    sda1,Ebs={
3  SnapshotId=<SnapshotID> }
4  '
5 <!--NeedCopy-->
```

<VolumeId> est le résultat de la tâche de préparation IPS. L'AMI qui en résulte peut être utilisée comme image principale MCS.

Un exemple de script PowerShell pour automatiser cette partie du flux de travail est fourni dans le module Citrix.Workloads.Portability sous la forme d'un script nommé New-IpsAwsImage.ps1.

Azure Sur Azure, IPS produit des disques gérés qui sont directement utilisables en tant qu'images principales MCS. Pour attribuer l'image résultante à des cibles PVS, IPS propose une opération « publish » permettant de copier le disque géré dans un fichier VHD (x) de votre magasin PVS.

Google Cloud Les tâches de préparation IPS sur Google Cloud produisent un disque. MCS nécessite un modèle d'instance Google Cloud. Le processus de création d'un modèle d'instance MCS à partir d'un disque est décrit en détail dans Préparer une instance de VM principale et un disque persistant.

Pour les cibles PVS sur Google Cloud, IPS propose une opération « publish » permettant de copier le disque dans un fichier VHD (x) de votre magasin PVS.

Automatiser la configuration du VDA

Lors de la préparation d'une image gérée par Citrix dont l'origine est locale, vous pouvez reconfigurer le VDA au sein de l'image pour prendre en charge l'environnement cible pour lequel l'image est en cours de préparation. Le service de portabilité des images peut appliquer les modifications de configuration du VDA à la volée pendant la phase de préparation du flux de travail. Les paramètres de configuration suivants définissent le mode de fonctionnement du VDA dans l'image migrée : **InstallMisa**, **XdReconfigure** et **InstallMcsio**. Consultez les exemples PowerShell du service de portabilité des images pour définir ces paramètres lors de la création de tâches de service de portabilité des images (IPS, Image Portability Service).

Configurations

- La configuration de **InstallMisa** sur `true` permet au service de portabilité des images d'installer tous les composants VDA manquants qui sont nécessaires pour provisionner l'image à l'aide de MCS.
- La configuration d'**InstallMisa** sur `true` ou d'**InstallMcsio** sur `true` nécessite également la configuration de **CloudProvisioningType** sur `Mcs`.
- Définissez **InstallPvs** sur la version du serveur PVS sur lequel l'image est déployée. Lorsque **InstallPvs** est défini, le service de portabilité des images (IPS) installe automatiquement la version spécifiée du logiciel de la machine cible PVS dans l'image pendant les tâches de préparation. IPS prend en charge les deux derniers builds (version de base ou mises à jour cumulatives) pour les deux dernières versions LTSR et CR.

Pour **InstallMisa** et **InstallMcsio**, notez les points suivants :

- Ces fonctionnalités ne sont prises en charge que pour les versions LTSR et CR récentes du VDA.
- Si les composants nécessaires sont déjà présents pour le VDA installé, aucune modification n'est apportée, même si les paramètres sont configurés.

- Pour les versions prises en charge du VDA, la portabilité des images installe la version appropriée des composants requis, même si les composants VDA nécessaires ne sont pas présents.
- Pour les versions non prises en charge du VDA, la reconfiguration échoue et un message est généré si les composants VDA nécessaires ne sont pas présents. La tâche de préparation se termine même si la reconfiguration du VDA n'est pas terminée.

XdReconfigure nécessite l'une des valeurs suivantes : `controllers` ou `site_guid`. Voici des exemples de paramètres de configuration utilisant chaque valeur :

Utilisation de **controllers** :

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'controllers'
        ParameterValue = 'comma-separated-list-of-your-cloud-connectors
           -fqdns'
     }

)
<!--NeedCopy-->
```

où **ParameterValue** est la liste des noms de domaine complets des nouveaux DDC vers lesquels vous souhaitez pointer le VDA. Plusieurs DDC peuvent être spécifiés dans un format séparé par des virgules.

Utilisation de **site_guid** :

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'site_guid'
        ParameterValue = 'active-directory-site-guid'
     }

)
<!--NeedCopy-->
```

XdReconfigure accepte également les valeurs prises en charge lors de l'exécution du programme d'installation de ligne de commande du VDA avec le commutateur d'installation **/reconfigure**, par exemple, **XenDesktopVdaSetup.exe /reconfigure**. Parmi ces valeurs, citons **wem_agent_port**, **wem_cached_data_sync_port**, **wem_cloud_connectors** ou **wem_server**. Pour obtenir la liste complète des options de ligne de commande de reconfiguration de VDA, reportez-vous à la documentation VDA Citrix DaaS.

Configurer **InstallMcsio** sur **`true`** installe automatiquement MCSIO sur l'image. Pour désactiver l'installation automatique de MCSIO sur l'image, configurez **InstallMcsio** sur **`false`**.

> **Remarque :**
>
> Lors de l'exécution de vos commandes, vous pouvez utiliser `-DryRun` pour valider votre configuration et les paramètres réseau de votre Connector Appliance.

Référence

Cette section détaille les informations de référence techniques, en fonction de vos besoins.

Autorisations requises par les services de portabilité des images

Cette section détaille les autorisations requises par le service de portabilité des images sur chacune des plateformes locales et cloud prises en charge.

Autorisations requises pour Connector Appliance Connector Appliance doit accéder aux URL suivantes pour préparer des images dans le service de portabilité des images :

```
api-ap-s.cloud.com
api-eu.cloud.com
api-us.cloud.com
credentialwallet.citrixworkspaceapi.net
graph.microsoft.com
login.microsoftonline.com
management.azure.com
*.blob.storage.azure.net
<!--NeedCopy-->
```

Autorisations requises pour VMware vCenter Les autorisations vCenter suivantes sont nécessaires pour exécuter la tâche d'exportation sur disque IPS dans un environnement VMware. Ces autorisations se trouvent sous **Rôles** dans la section **Contrôle d'accès** du panneau d'administration de vCenter.

```
-  Cryptographic operations
    -  Direct Access

-  Datastore
    -  Allocate space
    -  Browse datastore
    -  Low level file operations
    -  Remove file

-  Folder
    -  Create folder
    -  Delete folder

```



```
- Network
    - Assign network

- Resource
    - Assign virtual machine to resource pool

- Virtual machine
    - Change Configuration
        - Add existing disk
        - Add new disk
        - Remove disk

    - Edit Inventory
        - Create from existing
        - Create new
        - Remove

    - Interaction
        - Power off
        - Power on
<!--NeedCopy-->
```

Autorisations requises pour Microsoft Azure Le service de portabilité des images nécessite que votre compte de service Azure dispose des autorisations suivantes :

Lorsque le groupe de ressources à utiliser pour le moteur de composition est spécifié (c'est-à-dire dans la propriété *resourceGroup* dans une requête REST ou dans le paramètre *-AzureVmResourceGroup* lors de l'utilisation des commandes PowerShell Citrix.Workloads.Portability), les autorisations suivantes sont requises au niveau du groupe de ressources.

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/delete
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
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.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/read
```



```
<!--NeedCopy-->
```

Lorsque le groupe de ressources à utiliser pour le moteur de composition n'est pas spécifié, les autorisations suivantes sont requises dans le cadre de l'abonnement.

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/write
Microsoft.Network/networkInterfaces/join/action
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkInterfaces/write
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/networkSecurityGroups/write
Microsoft.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Authorization/roleAssignments/read
Microsoft.Authorization/roleDefinitions/read
<!--NeedCopy-->
```

Les autorisations suivantes sont requises au niveau du groupe de ressources cible spécifié (c'est-à-dire le groupe de ressources spécifié dans la propriété *targetDiskResourceGroupName* dans une requête REST ou dans le paramètre *-TargetResourceGroup* lors de l'utilisation de PowerShell).

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/snapshots/delete
Microsoft.Compute/snapshots/read
Microsoft.Compute/snapshots/write
<!--NeedCopy-->
```

Les autorisations suivantes sont requises au niveau du groupe de ressources du réseau virtuel spécifié (c'est-à-dire le groupe de ressources spécifié dans la propriété *virtualNetworkResourceGroupName* dans une requête REST ou dans le paramètre *-AzureVirtualNetworkResourceGroupName* lors de l'utilisation de PowerShell).

```
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/subnets/join/action
<!--NeedCopy-->
```


> **Important :**
>
> L'option `ceVmSku` pour les tâches « prepare » et « prepareAndPublish » contrôle le type de machine virtuelle Azure auquel le disque géré obtenu est adapté. Vous devez sélectionner un ceVmSku de la même famille et de la même version que les machines virtuelles que vous souhaitez provisionner à partir de l'image de sortie. La valeur par défaut de `Standard_D2S_v3` convient à toutes les machines de la famille v3 D. La spécification de SKU de machines non dotées d'un disque temporaire n'est pas prise en charge.

Autorisations requises pour Google Cloud La portabilité des images nécessite que votre compte de service Google Cloud dispose des autorisations suivantes :

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.stop
compute.instances.updateDisplayDevice
compute.networks.get
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
iam.serviceAccounts.get
iam.serviceAccounts.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.objects.create
```



```
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

Autorisations requises par AWS La portabilité des images nécessite de joindre un document de stratégie JSON avec la configuration suivante à l'utilisateur IAM (Identity and Access Management) :

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ec2:CreateTags",
                "ec2:CreateImage",
                "ec2:DeleteSnapshot",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:RebootInstances",
                "ec2:RegisterImage",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

> **Remarque :**
>
> Vous pouvez réduire l'étendue de la ressource selon vos besoins.

Autorisations requises pour Nutanix AHV La portabilité des images nécessite que vous soyez administrateur de cluster dans votre configuration Nutanix AHV.

Autorisations requises pour XenServer La portabilité des images nécessite que vous disposiez au minimum du rôle « Administrateur de machine virtuelle » pour le pool dans lequel se trouve l'hôte XenServer.

Réseau Le service de portabilité des images (Image Portability Service, IPS) crée une machine virtuelle de travail appelée moteur de composition (CE) pour effectuer des opérations sur les images. Tous les Connector Appliance situés dans l'emplacement de ressources associé doivent être capables de communiquer via HTTPS avec le CE.
Toutes les communications entre un Connector Appliance (CA) et le CE sont initiées par le CA, sauf une seule exception dans le cas de vSphere où il existe une communication HTTPS bidirectionnelle entre le CE et le CA.

Dans les environnements cloud (Azure, AWS, Google Cloud), le CE est créé avec une adresse IP privée. Le CE doit donc se trouver sur le même réseau virtuel que le CA ou sur un réseau virtuel accessible depuis le CA.

En outre, pour les tâches impliquant des fichiers sur un partage SMB (par exemple, les tâches d'exportation), le CE doit se trouver sur un réseau connecté au partage SMB.

Consultez la documentation de l'API Image Portability Service pour savoir comment spécifier le réseau à utiliser pour le CE sur chaque plate-forme prise en charge.

Avec les tâches « prepare », le système d'exploitation contenu dans l'image est démarré (sur le CE) pour effectuer des tâches de spécialisation et d'autres tâches. Si l'image contient des agents de gestion ou de sécurité qui contactent un serveur de contrôle par téléphone, ces processus peuvent interférer avec le processus de préparation.

Si l'option de dissociation du domaine est spécifiée, la connectivité réseau peut affecter les résultats. Si la machine virtuelle du moteur de composition peut accéder au contrôleur de domaine Active Directory via le réseau, la dissociation supprime le compte d'ordinateur du domaine. Cela annule l'appartenance au domaine pour la machine virtuelle source à partir de laquelle l'image a été extraite.

Nous recommandons donc d'isoler le réseau fourni pour l'opération des autres ressources réseau. Cela peut se faire en isolant le sous-réseau ou en utilisant des règles de pare-feu. Voir Isolation du réseau pour plus de détails.

Dans certains environnements d'hyperviseur locaux, l'hyperviseur peut être configuré avec un certificat de serveur TLS, qui n'est pas approuvé par l'ensemble des certificats racines fiables de l'autorité de certification ou qui ne correspond pas au nom d'hôte du serveur. Dans de telles situations, **IPS fournit des propriétés de demande de tâches** qui peuvent être utilisées pour contourner le problème. Consultez les certificats TLS pour plus de détails.

Proxys réseau Si le trafic réseau entre l'autorité de certification et Internet passe par un proxy qui effectue une introspection TLS, il peut être nécessaire d'ajouter à l'autorité de certification racine

du proxy (c'est-à-dire le certificat que le proxy utilise pour signer les certificats TLS qu'il génère) à l'ensemble des autorités de certificat racine de l'autorité de certification. Consultez Enregistrer votre Connector Appliance auprès de Citrix Cloud pour plus d'informations.

Isolation du réseau

- Azure

  Dans Azure, le CE est créé par défaut avec un groupe de sécurité réseau (NSG) attaché à sa carte réseau si le principal de service Azure utilisé dans l'opération dispose des autorisations Azure nécessaires [1].

  - Microsoft.Network/networkSecurityGroups/join/action
  - Microsoft.Network/networkSecurityGroups/read
  - Microsoft.Network/networkSecurityGroups/write

    Sinon, les autorisations suivantes définies dans l'étendue de l'abonnement si aucun groupe de ressources explicite n'est utilisé :

    * Microsoft.Network/networkSecurityGroups/delete
    * Microsoft.Network/networkSecurityGroups/join/action
    * Microsoft.Network/networkSecurityGroups/read
    * Microsoft.Network/networkSecurityGroups/write

  Ce NSG est configuré pour bloquer tout le trafic entrant/sortant du CE, à l'exception de :

  - SMB (port 445) sortant
  - HTTPS (port 443) entrant
  - requis pour les services Azure internes

  L'utilisation du NSG peut être forcée en définissant la propriété *networkIsolation* sur *true* dans la demande de tâche. Dans ce cas, la tâche échoue si le principal de service utilisé dans l'opération ne dispose pas des autorisations nécessaires. L'utilisation du NSG peut être désactivée en définissant la propriété *networkIsolation* sur *false*.

- AWS

Dans AWS, pour isoler le CE sur le réseau, vous pouvez créer un ou plusieurs groupes de sécurité réseau qui bloquent tout trafic indésirable, puis, dans la demande de tâche, attribuer les groupes de sécurité à l'instance CE à l'aide du paramètre de demande *securityGroupIds* qui prend comme valeur une liste d'identifiants de groupes de sécurité.

- Google Cloud

Dans Google Cloud, pour isoler le CE sur le réseau, vous pouvez créer des règles de pare-feu qui bloquent tout trafic indésirable, puis appliquer ces règles au CE via des balises réseau. IPS crée le CE avec la balise réseau *compositing-engine* et vous pouvez lui attribuer d'autres balises réseau à l'aide du paramètre de demande de tâche *networkTags* qui prend une liste de balises comme valeur.

Certificats TLS Si le certificat de serveur de l'hyperviseur est signé par une autorité non approuvée par l'autorité de certification, deux approches alternatives peuvent être utilisées pour résoudre le problème.

1. Spécifiez dans la demande de tâche un certificat d'autorité de certification racine supplémentaire à utiliser pour la vérification des certificats. Ce certificat doit être l'autorité de certification racine utilisée pour signer le certificat de serveur de l'hyperviseur.
2. Spécifiez dans la demande de tâche l'empreinte SHA-1 du certificat de serveur de l'hyperviseur. Dans ce cas, la validation du certificat est effectuée en vérifiant que l'empreinte SHA-1 du certificat renvoyé par l'hyperviseur correspond à celle fournie dans la demande de tâche. Cette méthode peut ne pas fonctionner s'il existe un proxy d'interception TLS entre le CE et l'hyperviseur.

Les paramètres de demande de tâche pour ce qui précède, indiqués respectivement ci-dessous pour chaque plateforme, sont les suivants :

- vSphere
    1. vCenterSslCaCertificate
    2. vCenterSslFingerprint
- Nutanix
    1. prismSslCaCertificate
    2. prismSslFingerprint
- XenServer
    1. xenSslCaCertificate
    2. xenSslFingerprint

Pour plus d'informations, consultez la documentation de l'API du service de portabilité des images.

Des erreurs de validation de certificat peuvent également se produire en cas de non-concordance entre le nom d'hôte du serveur de l'hyperviseur et le nom d'hôte figurant dans son certificat. Dans ce cas, la correspondance des noms d'hôte peut être désactivée en définissant le paramètre suivant sur *true* dans la demande de tâche :

- vSphere
    - vCenterSslNoCheckHostname

- Nutanix
  - prismSslNoCheckHostname
- XenServer
  - xenSslNoCheckHostname

Documentation associée

- Documentation de l'API du service de portabilité des images
- Connector Appliance pour Cloud Services
- Documentation Google Cloud
- Comptes de service Google Cloud
- Enregistrement et authentification d'applications Microsoft Azure

1. If Un groupe de ressources explicite est utilisé pour l'opération, puis les autorisations suivantes dans l'étendue du groupe de ressources :

Imprimer

April 27, 2022

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.

Pour obtenir des informations complètes sur l'impression dans un environnement Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), commencez par lire l'article Imprimer. Vous pourrez ensuite passer à :

- Exemples de configuration d'impression
- Recommandations
- Stratégies et préférences d'impression
- Provisionner des imprimantes
- Gérer l'environnement d'impression

Installer le serveur d'impression universelle sur vos serveurs d'impression

1. Assurez-vous que Microsoft Virtual C ++ Runtime 2017 32 bits et 64 bits est installé sur chaque serveur d'impression.
2. Accédez à la page de téléchargement du serveur d'impression universel Citrix et cliquez sur **Télécharger le fichier**.
3. Exécutez l'une des commandes suivantes sur chaque serveur d'impression :
    - Pour un système d'exploitation 32 bits : **UpsServer_x86.msi**.
    - Pour un système d'exploitation 64 bits : **UpsServer_x64.msi**.

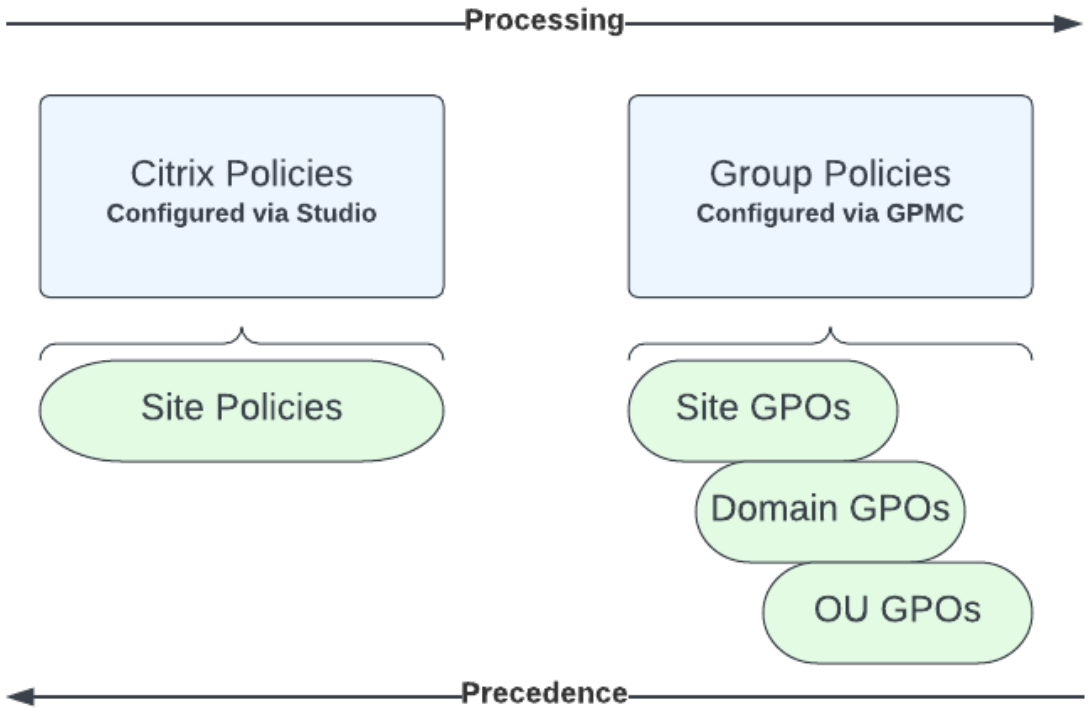
Après avoir installé le serveur d'impression universel, configurez ce dernier à l'aide des instructions de la section Provisionner les imprimantes.

Stratégies

April 17, 2023

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 VDA ou à des utilisateurs. Vous pouvez modifier les paramètres dans Web Studio ou dans les objets de stratégie de groupe (GPO) d'Active Directory. Vous pouvez spécifier des filtres (attributions d'objets) pour les stratégies. Si vous n'attribuez pas de stratégies spécifiques aux filtres, les paramètres sont appliqués à toutes les sessions utilisateur.



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 de site 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.

Web 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 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 Web Studio 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. À partir de l'application Citrix Workspace, l'utilisateur final se connecte à un VDA à l'aide des informations d'identification du domaine.
2. Les stratégies Citrix sont traitées pour l'utilisateur final et pour le VDA
3. Les stratégies sont appliquées dans l'ordre suivant :

    a) Stratégies locales
    b) Stratégies de site
    c) Stratégies de domaine
    d) Stratégies d'UO (unité organisationnelle)

> **Remarque :**
>
> - Toutes les stratégies peuvent ne pas être présentes aux quatre niveaux. Pour la plupart des clients, seules les stratégies du site sont utilisées. Les stratégies locales exigent que l'utilisateur se connecte au VDA pour modifier les stratégies. Par conséquent, ces stratégies ne sont presque jamais utilisées.
> - Nous ne prenons pas en charge le mélange de stratégies Windows et Citrix dans le même objet de stratégie de groupe.

Pour des informations complètes sur les stratégies Citrix, consultez les rubriques suivantes :

- Utiliser les stratégies
- Modèles de stratégie
- Créer des stratégies
- Donner un ordre de priorité, modéliser, comparer et résoudre les problèmes de stratégies
- Paramètres de stratégie par défaut
- Référence des paramètres de stratégie

  > **Remarque :**
  >
  > Les références de paramètres de stratégie pour Citrix DaaS sont les mêmes que les paramètres de stratégie pour Citrix Virtual Apps and Desktops. Vous pouvez donc également consulter la section Référence des paramètres de stratégie dans la documentation Citrix Virtual Apps and Desktops pour Citrix DaaS.

Utiliser les stratégies

May 23, 2023

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

- Studio - Les stratégies créées à l'aide de Studio sont stockées dans la base de données du site et les mises à jour sont transmises au VDA dans l'une des situations suivantes :
  - Lorsque ce VDA s'enregistre auprès du Controller
  - Lorsqu'un utilisateur lance une session
- Console de gestion des stratégies de groupe : si votre environnement réseau utilise Active Directory et que vous êtes autorisé à gérer les stratégies de groupe, vous pouvez utiliser la console de gestion des stratégies de groupe (GPMC) pour créer et modifier des stratégies pour votre site. Dans la console, vous pouvez configurer des objets de stratégie de groupe (GPO) avec les paramètres et les filtres souhaités. Ces stratégies auront priorité sur les stratégies configurées dans Studio. Pour plus d'informations, veuillez consulter l'article CTX238166.

Ordre de traitement et priorité des stratégies

Les paramètres de stratégie de groupe sont traités dans l'ordre suivant :

1. GPO du site Citrix DaaS (stocké dans la base de données du site)
2. GPO au niveau du domaine
3. Unités d'organisation

Toutefois, si des paramètres différents sont appliqués à la même stratégie dans deux GPO, les paramètres de stratégie traités en dernier remplacent les paramètres traités précédemment. Cette configuration signifie que les paramètres de stratégie sont prioritaires dans l'ordre suivant :

1. Unités d'organisation
2. GPO au niveau du domaine
3. GPO du site Citrix DaaS (stocké dans la base de données du site)

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 Donner un ordre de priorité, modéliser, comparer et résoudre les problèmes de 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 le volet **Actions**. L'onglet **Modélisation** est disponible dans Web Studio hébergé dans Citrix Cloud à la demande du client.

Naviguer vers les stratégies et paramètres Citrix

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. Les paramètres utilisateur sont appliqués lorsqu'un utilisateur se connecte ou se reconnecte

Pour accéder aux stratégies, paramètres ou modèles, sélectionnez **Stratégies** dans le panneau de navigation 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 : groupe de mise à disposition. Vous pouvez modifier ou supprimer les paramètres d'attribution. Appliquez la stratégie basée sur l'appartenance au groupe de mise à disposition du bureau exécutant la session. 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 Donner un ordre de priorité, modéliser, comparer et résoudre les problèmes de stratégies.
  - À partir de l'onglet **Modélisation**, vous pouvez simuler des scénarios de connexion avec les stratégies Citrix. Pour plus d'informations, consultez la section Donner un ordre de priorité, modéliser, comparer et résoudre les problèmes de stratégies.

  Pour rechercher un paramètre dans une stratégie ou un modèle :

  1. Sélectionnez la stratégie ou le modèle.
  2. Sélectionnez l'onglet **Modifier la stratégie** ou **Modifier le modèle**.
  3. Sur la page **Sélectionner les paramètres**, commencez à taper le nom du paramètre.

  Vous pouvez affiner votre recherche en sélectionnant :

  - Une catégorie (par exemple, Bande passante)
  - La case à cocher **Afficher sélectionné uniquement**
  - Pour rechercher uniquement les paramètres qui ont été ajoutés à la stratégie sélectionnée.

- Pour rechercher un paramètre dans une stratégie :

  1. Sélectionnez la stratégie.
  2. Sélectionnez l'onglet **Paramètres** et tapez le nom du paramètre.

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.

Modèles de stratégie

November 17, 2022

Les modèles sont utilisés pour créer des stratégies à partir d'un point de départ prédéfini. Les modèles Citrix incorporés, optimisés pour des environnements ou des conditions réseau spécifiques, peuvent être utilisés en tant que :

- Source pour créer vos propres stratégies et modèles à partager entre les sites.
- Référence pour comparer en toute facilité les résultats entre déploiements en vous permettant de faire état des résultats, par exemple, « …lors de l'utilisation du modèle Citrix x ou y… »
- Méthode permettant de transmettre des stratégies au support Citrix ou à des tiers de confiance. Vous pouvez le faire en important ou en exportant des modèles.

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 destiné aux travailleurs de tâches des succursales qui utilisent un réseau étendu partagé ou des sites distants dotés de connexions à faible bande passante. Les travailleurs accèdent à des applications dotées d'interfaces utilisateur graphiquement simples et d'un faible 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**. Ce modèle s' applique uniquement aux VDA exécutant Windows Server 2008 R2 ou Windows 7 et versions

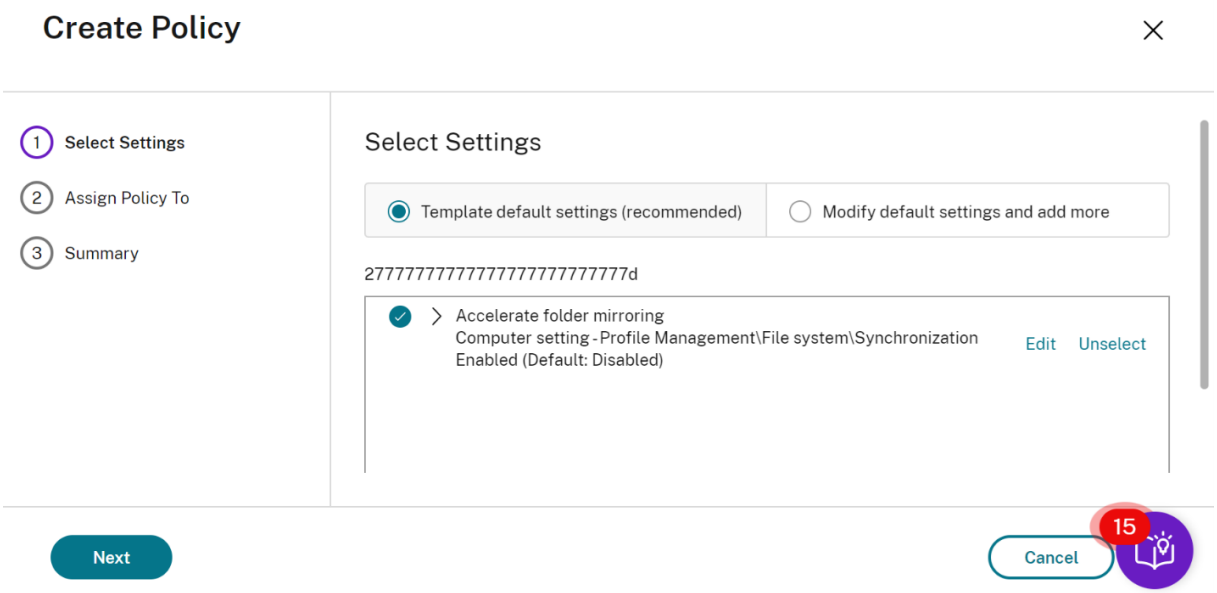
antérieures. Ce modèle s'appuie sur le Mode graphique d'ancienne génération qui est plus efficace pour ces systèmes d'exploitation.

- **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 DaaS. Ce modèle inclut des paramètres qui désactivent l'accès aux éléments suivants :

  - Impression
  - Presse-papiers
  - Périphériques
  - Mappage des lecteurs clients
  - Redirection de port
  - Accélération Flash sur les appareils 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.



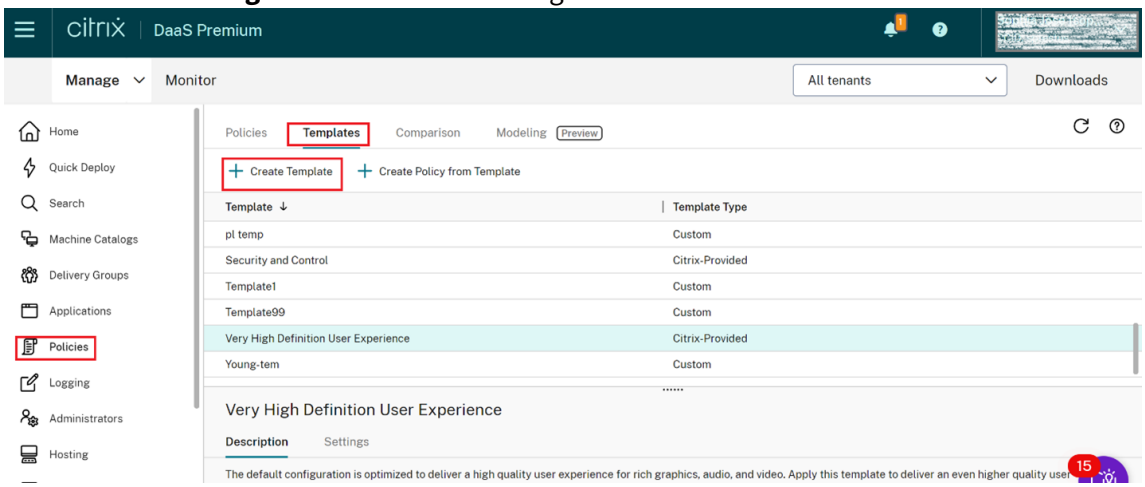
Supposons que vous travaillez avec un déploiement (gestion de stratégie et VDA) antérieur à XenApp et XenDesktop 7.6 FP3. Vous exigez également une capacité élevée des serveurs à monter en charge et une optimisation pour les modèles WAN. Dans ce cas, utilisez les versions OS d'ancienne génération de ces modèles lorsqu'elles s'appliquent.

> **Remarque :**
>
> Citrix crée des modèles incorporés et les met à jour. vous ne pouvez ni modifier ni supprimer ces modèles.

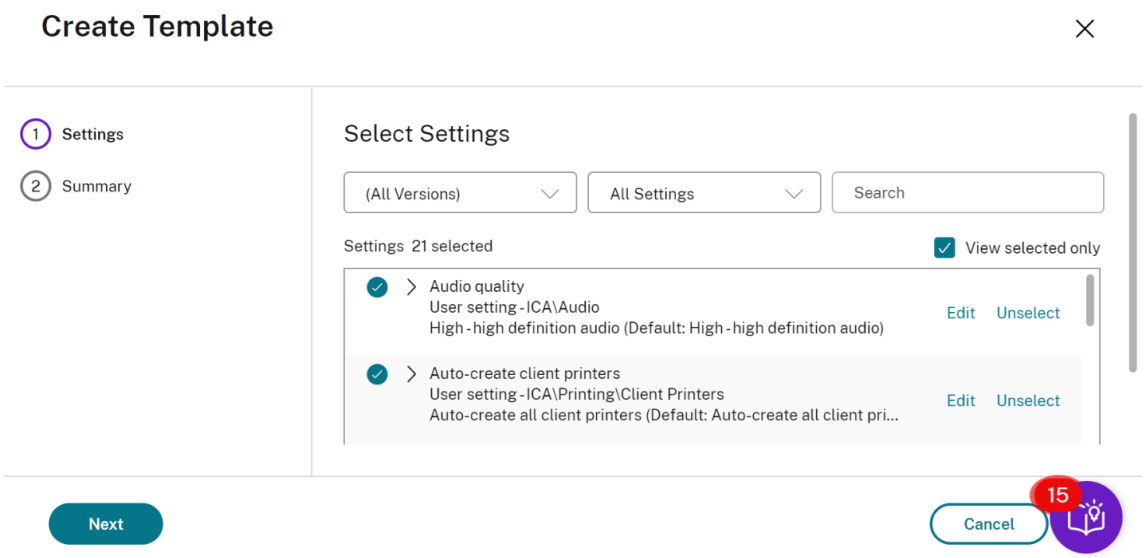
Créer et gérer des modèles à l'aide de Web Studio

Pour créer un modèle à partir d'un autre modèle :

1. Sélectionnez **Stratégies** dans le volet de navigation de Web Studio.



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.



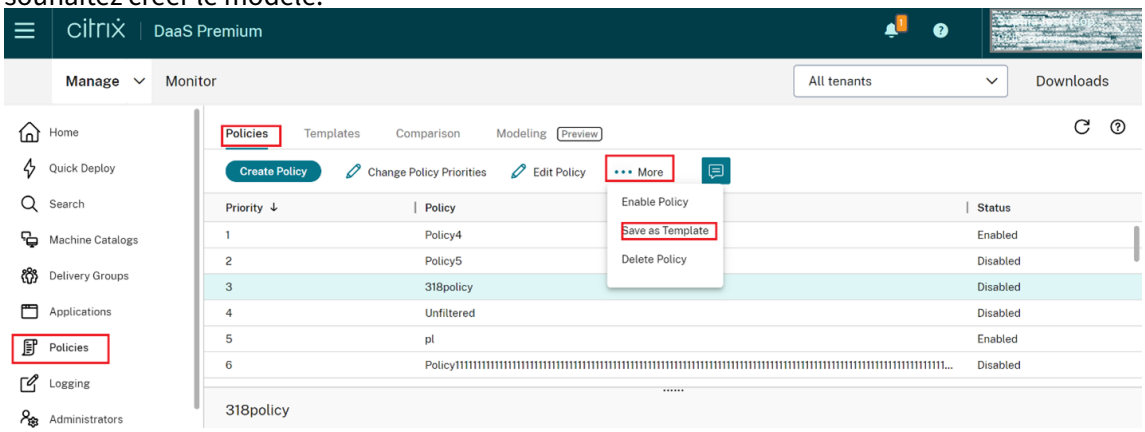
4. Sélectionnez et configurez les paramètres de stratégie que vous souhaitez inclure dans le mod-

èle.

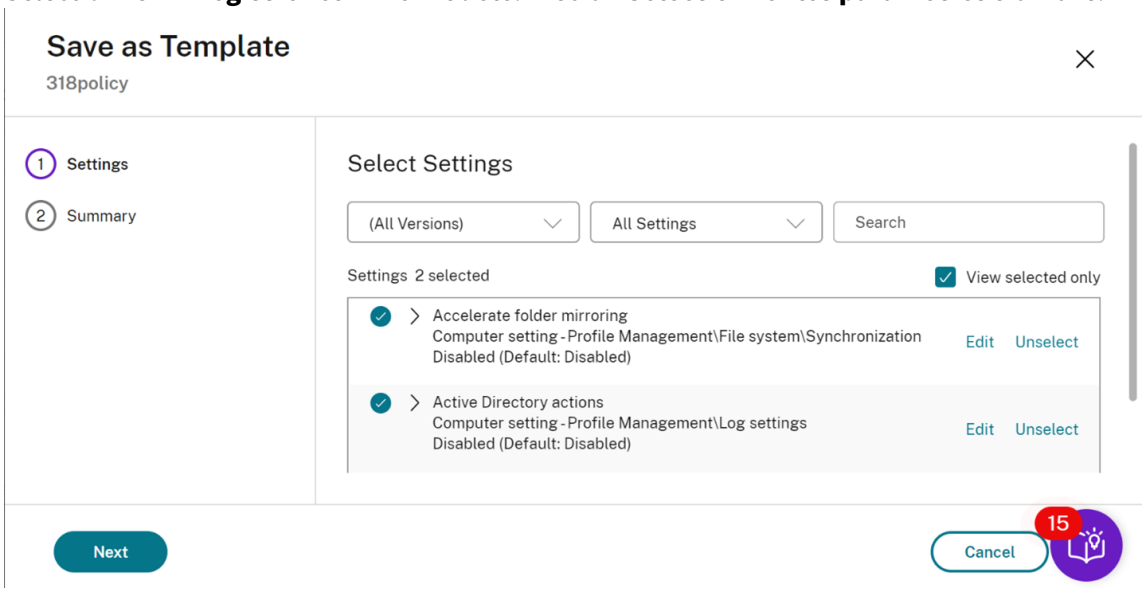
5. Cliquez sur **Suivant**. L'écran **Résumé** s'affiche.
6. Entrez un nom pour le modèle.
7. Cliquez sur **Terminer**. Le nouveau modèle apparaît dans l'onglet Modèles

Pour créer un modèle à partir d'une stratégie :

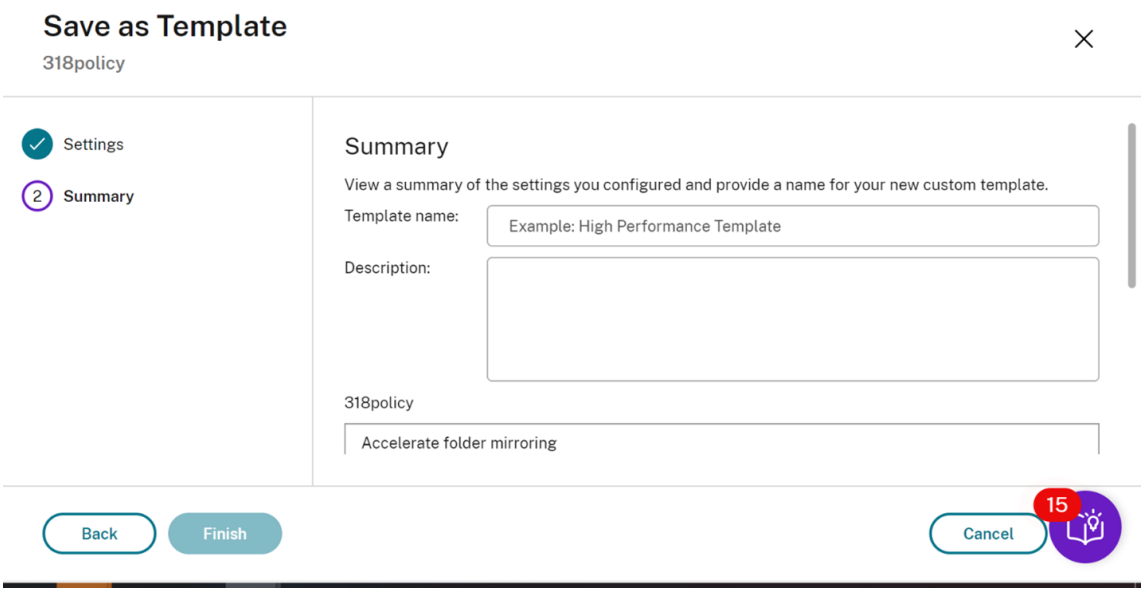
1. Sélectionnez **Stratégies** dans le volet de navigation de Web Studio.
2. Sélectionnez l'onglet **Stratégies**, puis sélectionnez la stratégie à partir de laquelle vous souhaitez créer le modèle.



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**.

Créer des stratégies

November 2, 2023

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.

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 Citrix Studio, les nouvelles stratégies créées sont réglées 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 pour toutes les versions de VDA

- Paramètres actuels uniquement - Afficher les paramètres uniquement pour les versions actuelles de VDA
- Anciens paramètres uniquement - Afficher les paramètres uniquement pour les versions de VDA obsolètes

Pour afficher les paramètres lors de leur configuration, procédez comme suit :

1. Connectez-vous à DaaS Premium.
2. Dans le volet de navigation de gauche, cliquez sur **Stratégies**.
3. Dans l'onglet **Stratégies**, cliquez sur **Créer une stratégie**.
4. Dans le tableau **Sélectionner les paramètres**, cliquez sur le menu déroulant situé à côté de **Paramètres**.
5. Sélectionnez l'une des options suivantes dans le menu déroulant :

    - Tous les paramètres - Afficher tous les paramètres pour toutes les versions de VDA
    - Paramètres actuels uniquement - Afficher les paramètres uniquement pour les versions actuelles de VDA
    - Anciens paramètres uniquement - Afficher les paramètres uniquement pour les versions de VDA obsolètes

6. Le tableau des 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.

Lors de la configuration des paramètres pour la création ou la modification d'une stratégie, si tous les groupes de mise à disposition sont désactivés, le système affiche un signe de notification d'avertissement **Aucun des éléments de ce filtre n'est activé**. Si au moins un groupe de mise à disposition est activé, le système n'affiche pas le signe d'avertissement.

Pour voir l'avertissement lors de la création d'une stratégie, procédez comme suit :

1. Connectez-vous à DaaS Premium.
2. Dans le volet de navigation de gauche, cliquez sur **Stratégies**.
3. Dans l'onglet **Stratégies**, cliquez sur **Créer une stratégie**.
4. Dans le tableau **Sélectionner les paramètres**, sélectionnez un paramètre et cliquez sur **Suivant**.

5. Dans le tableau **Attribuer une stratégie à**, sélectionnez un filtre dans le menu déroulant.
6. Décochez la case **Activer** et cliquez sur **Enregistrer**.

> **Remarque :**
>
> Tous les filtres ne permettent pas de désélectionner la case **Activer**.
> Dans le tableau **Filtres**, le filtre affiche l'avertissement.

Pour voir l'avertissement lors de la modification d'une stratégie, procédez comme suit :

1. Connectez-vous à DaaS Premium.
2. Dans le volet de navigation de gauche, cliquez sur **Stratégies**.
3. Dans l'onglet **Stratégies**, sélectionnez l'une des stratégies répertoriées et cliquez sur **Modifier la stratégie**.
4. Sur la page **Modifier la stratégie**, cliquez sur **Attribuer la stratégie à** dans le volet de navigation de gauche.
5. Dans le tableau **Filtre**, sélectionnez ou cliquez sur **Modifier** pour le filtre requis :
   - Si le bouton **Modifier** n'apparaît pas pour un filtre, sélectionnez le filtre.
   - Si le bouton Modifier est disponible pour le filtre, cliquez sur **Modifier**.
6. Désélectionnez l'option **Activer** et cliquez sur **Enregistrer**.

> **Remarque :**
>
> Tous les filtres ne permettent pas de désélectionner la case **Activer**.
> Dans le tableau **Filtres**, le filtre affiche l'avertissement.

Les paramètres de stratégie peuvent affichés l'un des états suivants :

```
- Allowed or Prohibited allows or prevents the action controlled by
  the setting. Sometimes users are allowed or prevented from managing
  the setting's action in a session. For example, if the menu
  animation setting is set to Allowed, users can control menu
  animations in their client environment
- Enabled or Disabled turns the setting on or off. If you disable a
  setting, it is not enabled in lower-ranked policies.
```

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.

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.

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.
- 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 pas les attributions, la stratégie est appliquée à toutes les connexions.

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.
Citrix SD-WAN	Si une session utilisateur est lancée via Citrix SD-WAN. **Remarque :** vous pouvez ajouter une seule attribution Citrix 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.
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 plus d'informations, consultez 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.
- 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.

Jeux de stratégies (Technical Preview)

May 17, 2024

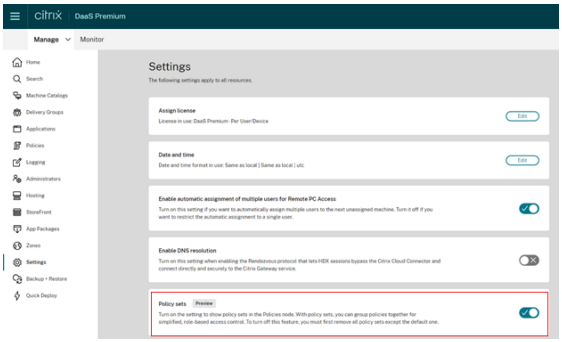
Les jeux de stratégies sont des objets de Citrix DaaS qui regroupent des stratégies pour permettre un accès simplifié basé sur les rôles et une gestion aisée. Vous pouvez créer des jeux de stratégies reflétant les divisions logiques au sein de votre équipe d'administrateurs et de votre entreprise. Par 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.

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 Citrix DaaS, accédez à **Paramètres** et activez le paramètre **Jeux de stratégies**.



> **Remarque :**
>
> avant de créer un jeu de stratégie, vous devez activer le paramètre "Jeux 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.

Fonctionnement des 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

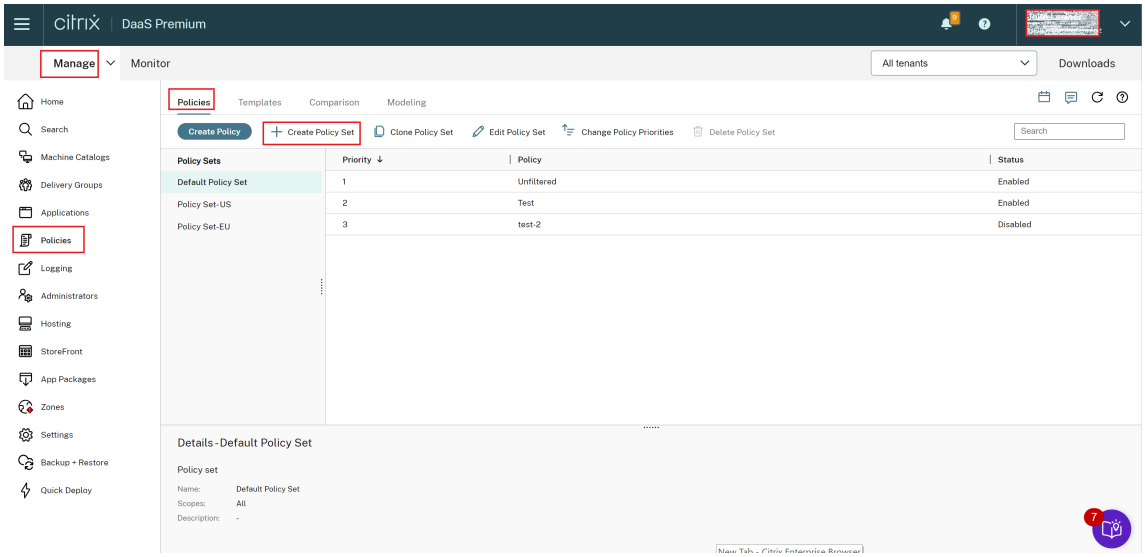
Création d'un jeu de stratégies

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. Sur la page de configuration de Citrix DaaS, cliquez sur l'onglet **Gérer**.
2. Cliquez sur l'onglet **Stratégies**.



3. Sélectionnez **Créer un jeu de stratégies**. L'onglet **Introduction** apparaît.
4. Cliquez sur **Suivant** ou sur l'onglet **Nom et description**.
5. Entrez le nom et la description du jeu de stratégies.
6. Cliquez sur **Suivant** ou sur l'onglet **Attributions**.
7. Sélectionnez un ou plusieurs groupes de mise à disposition auxquels vous souhaitez attribuer le jeu de stratégies.
8. Cliquez sur **Suivant** ou sur l'onglet **Étendues**.
9. Sélectionnez les étendues du jeu de stratégies.
10. Cliquez sur **Créer**. Le jeu de stratégies est créé avec l'affectation et l'étendue définies.

Cloner un jeu de stratégies

1. Sur la page de configuration de Citrix DaaS, cliquez sur l'onglet **Gérer**.
2. Cliquez sur l'onglet **Stratégies**.
3. Sélectionnez **Cloner jeu de stratégies**.
4. Modifiez le nom du jeu de stratégies.
5. Modifiez ou créez des attributions pour le jeu de stratégies et cliquez sur **Suivant**.
6. Sélectionnez ou désélectionnez les stratégies à inclure dans le jeu de stratégies cloné.
7. Modifiez l'étendue de la stratégie.
8. Cliquez sur **Créer**. Le jeu de stratégies est créé.

Modifier des jeux de stratégies

1. Sur la page de configuration de Citrix DaaS, cliquez sur l'onglet **Gérer**.
2. Cliquez sur l'onglet **Stratégies**.
3. Sélectionnez **Modifier jeu de stratégies**.
4. Modifiez le nom du jeu de stratégies et cliquez sur **Suivant**.

5. Modifiez ou créez des attributions pour le jeu de stratégies et cliquez sur **Suivant**.
6. Modifiez l'étendue de la stratégie.
7. Cliquez sur **Créer**.

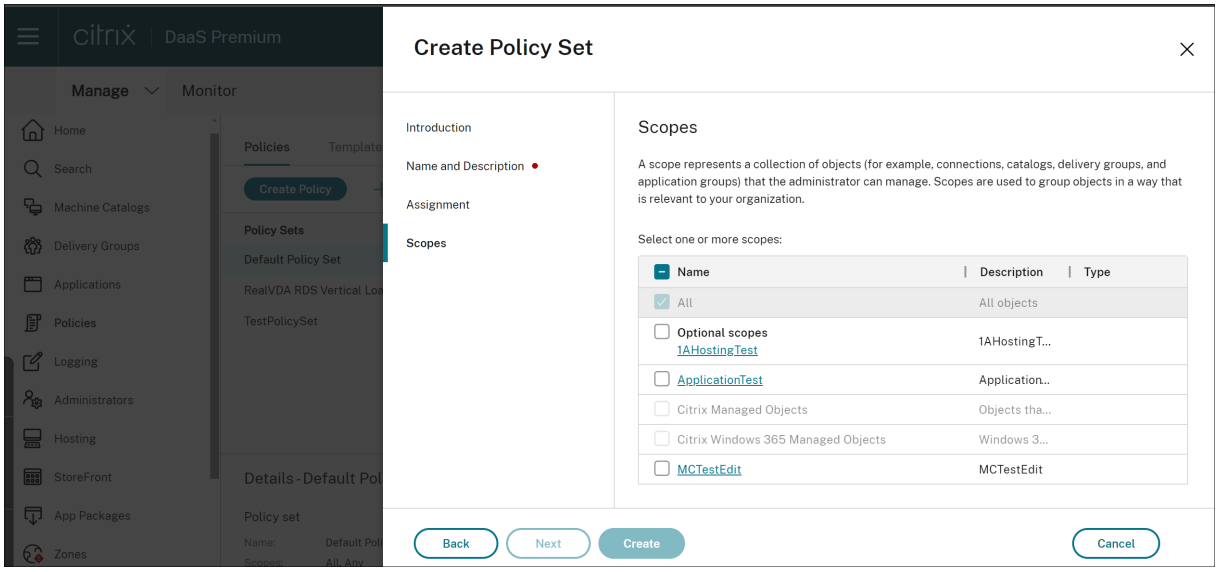
Attribution d'un jeu de stratégies

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.



Donner un ordre de priorité, modéliser, comparer et résoudre les problèmes de stratégies

June 8, 2023

Vous pouvez utiliser des stratégies pour personnaliser votre environnement afin de répondre aux besoins des utilisateurs sur la base des éléments suivants :

- Fonctions professionnelles
- Emplacements géographiques
- 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. Vous pouvez créer une autre stratégie pour les utilisateurs du groupe d'utilisateurs qui ont besoin d'accéder à leurs lecteurs locaux. Vous pouvez ensuite définir l'ordre de ces deux stratégies afin de définir laquelle des deux est prioritaire. Lorsque vous utilisez de nombreuses stratégies, vous devez déterminer :

- Comment hiérarchiser les stratégies
- Comment créer des exceptions
- Comment afficher la stratégie effective en cas de conflit entre les stratégies

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. L'identification de toutes les stratégies qui correspondent aux attributions de la connexion se produit lorsqu'un utilisateur se connecte au système. Les stratégies identifiées et les paramètres qui leur sont associés sont triés par ordre de priorité. Chaque paramètre est appliqué selon l'ordre de priorité de la stratégie.

Vous pouvez définir la priorité des stratégies en leur donnant des numéros de priorité différents dans **Web Studio**. Par défaut, la priorité d'une nouvelle stratégie est plus faible que celle d'une stratégie déjà existante. En cas de conflit entre les paramètres des stratégies, une stratégie avec une priorité plus élevée remplace une stratégie avec une priorité inférieure. Une stratégie dont le numéro de priorité est 1 est la stratégie ayant la priorité la plus élevée. Les paramètres de stratégie sont fusionnés comme suit :

- Priorités des stratégies
- Conditions spécifiées dans les filtres des stratégies

Pour hiérarchiser les stratégies, procédez comme suit :

1. Sélectionnez **Stratégies** dans le volet de gauche.
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 et utilisé des filtres pour les attribuer à 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 des membres de groupe spécifiques 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 dont les adresses IP se trouvent dans la plage spécifiée dans l'*attribution A*. Toutefois, la stratégie ne s'applique pas à l'utilisateur qui se connecte au site avec le compte utilisateur spécifié dans l'*attribution B*.

> **Remarque :**
>
> Au cours de l'étape **Attribuer une stratégie**, si vous désélectionnez la case Activer, l'attribution est désactivée pour la stratégie. Si la seule attribution pour la stratégie est désactivée, cela revient à ne pas avoir d'attribution et, par conséquent, la stratégie s'applique à tous les objets du

> site.

Déterminer les stratégies qui s'appliquent à une connexion

Il arrive parfois 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 :
  - Utilisateurs
  - Valeurs d'évidence d'attribution de stratégie Citrix
- Utilisez l'outil **Résultats de stratégie de groupe** pour créer un rapport décrivant les stratégies Citrix en vigueur pour un utilisateur et un VDA.

Les paramètres de stratégie de site créés à l'aide de **Web Studio** ne sont pas inclus dans l'**ensemble de stratégies résultant** lorsque vous exécutez l'assistant **Modélisation de stratégie de groupe Citrix** 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**.

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. Dans Configuration complète, sélectionnez **Stratégies**.
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 **Next**.
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 **Next**.
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 vouliez 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.

1. Sélectionnez **Stratégies** dans le volet de navigation de **Web Studio**.
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**.

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**, 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.

> **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.

Director

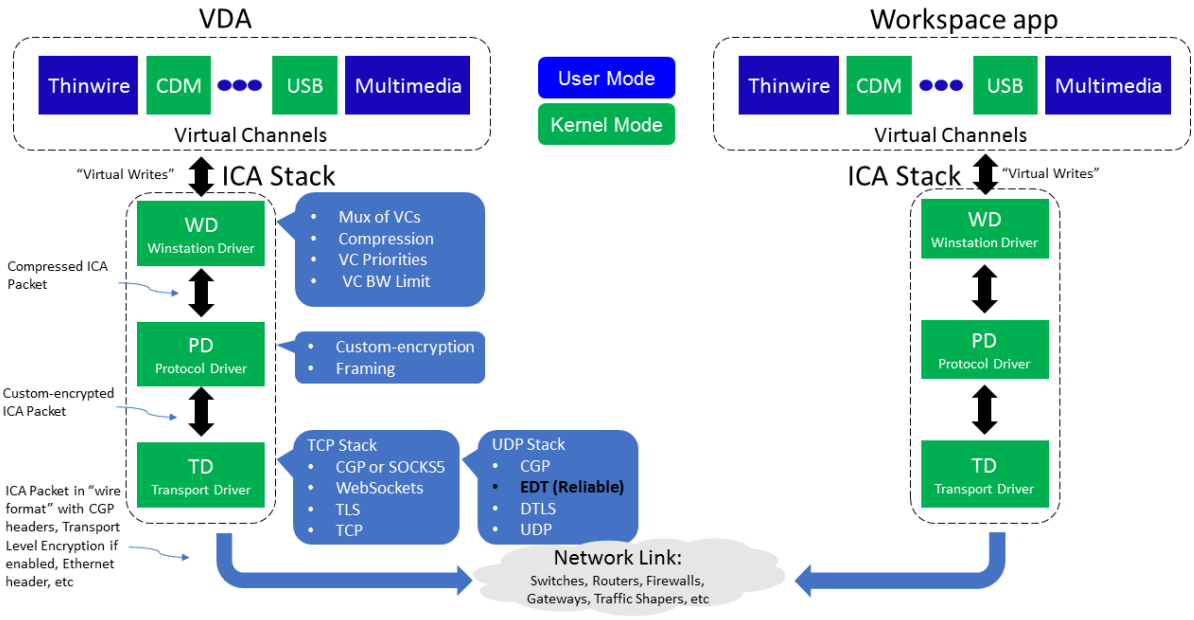
Les non-administrateurs peuvent utiliser le Director pour vérifier les stratégies qui s'appliquent à une session utilisateur.

Présentation de HDX

April 18, 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.

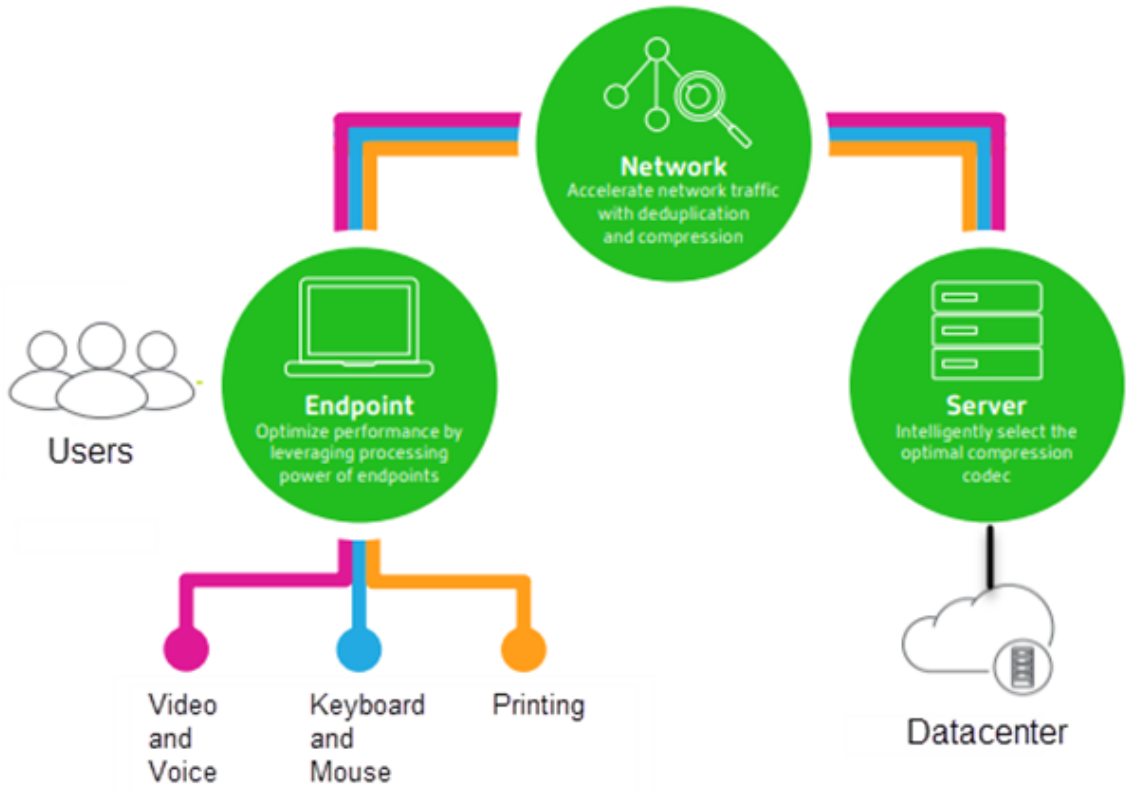


HDX est conçu autour de trois principes techniques :

- 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 offre 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.

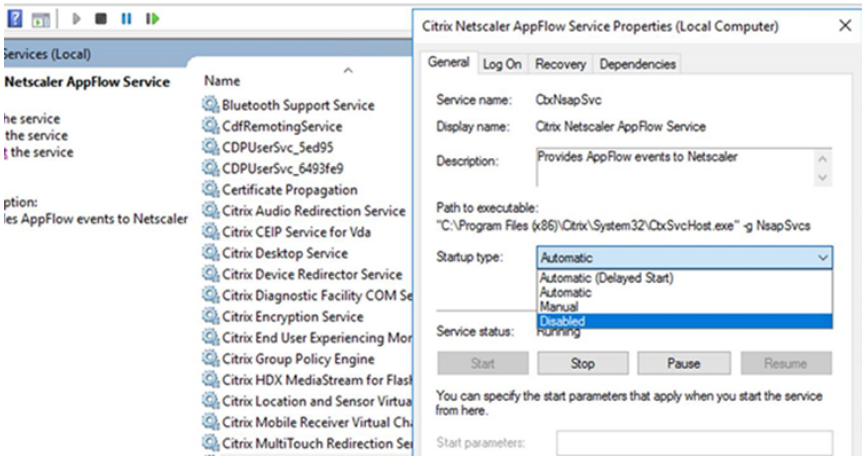
Vous pouvez activer NetScaler pour utiliser le canal virtuel HDX Insight afin de déplacer tous les points de données requis dans un format non compressé. Si vous désactivez cette fonctionnalité, l'appareil NetScaler déchiffre et décompresse la propagation du trafic ICA sur différents canaux virtuels.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

Configuration minimale requise :

- Citrix Virtual Apps and Desktops 7 v1808
- XenApp et XenDesktop 7.17
- 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 rapide-

ment 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 prob-

lèmes 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 comme suit :

- **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 pendant que la reconnexion automatique des clients 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 zone de notification.

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 immédiatement 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 zone de notification 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.

Améliorer les performances de conférence vidéo

Plusieurs applications de visioconférence populaires sont optimisées pour la mise à disposition à partir de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) 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
- Redirection Windows Media

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 et Windows 8. Travaillez avec votre administrateur réseau pour vous assurer que les ports CGP configurés dans le paramètre Stratégie Multi-Port 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 Branch Repeater 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 du Registre, accédez à `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI`.
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, utilisez 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

March 7, 2024

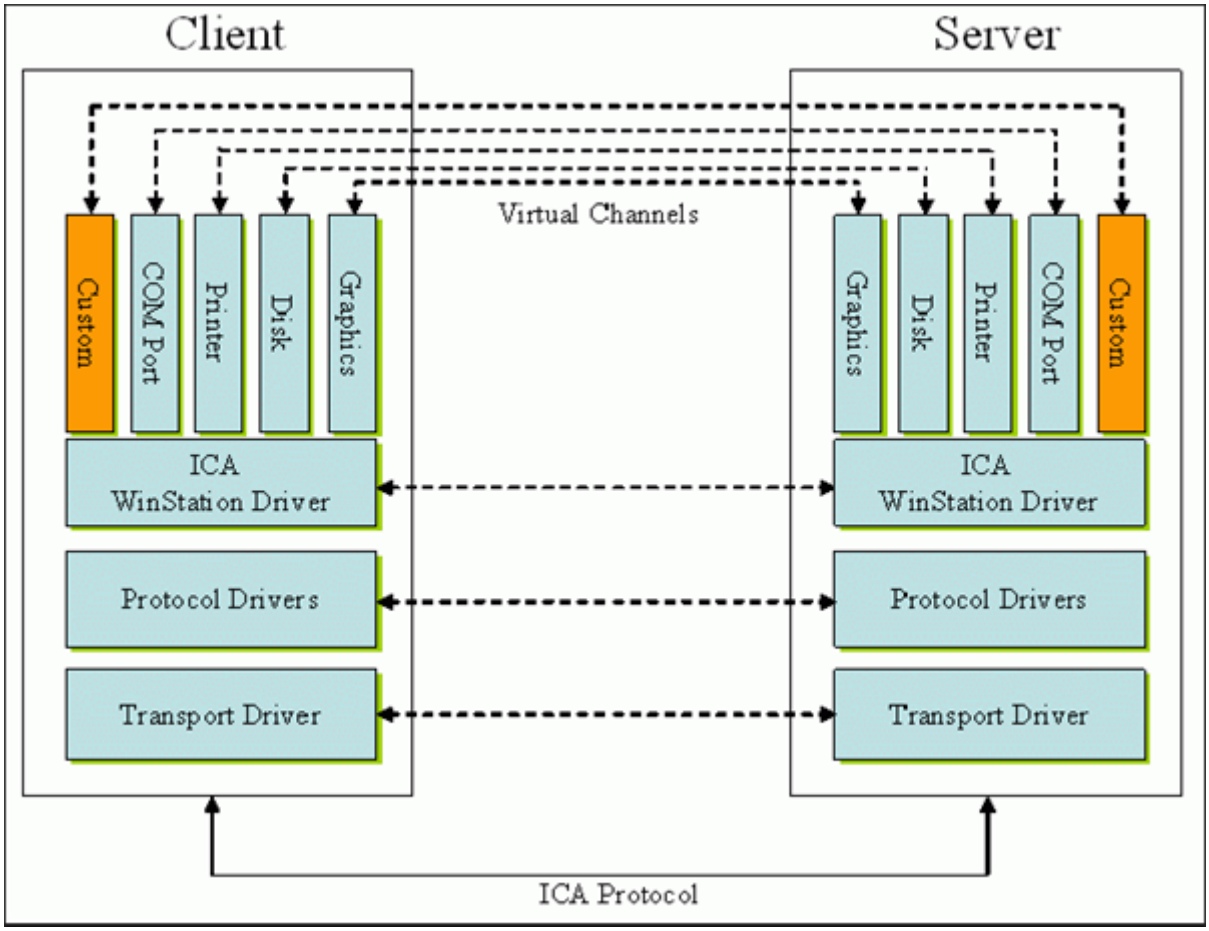
> **Avertissement :**
>
> Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Vous utilisez l'Éditeur du Registre à vos propres risques. 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 DaaS (anciennement Citrix Virtual Apps and Desktops Service) se produit sur des canaux virtuels. Les canaux virtuels font partie intégrante de l'expérience à distance avec les serveurs Citrix DaaS. 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 produits de l'application Citrix DaaS et Citrix Workspace pour fournir davantage de fonctionnalités.



Un canal virtuel consiste en un pilote virtuel côté client qui communique avec une application côté serveur. Citrix DaaS 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

À partir de XenApp 7.0 et XenDesktop7.0, `ctxgfx.exe` héberge le canal virtuel graphique pour les sessions basées sur station 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 station 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

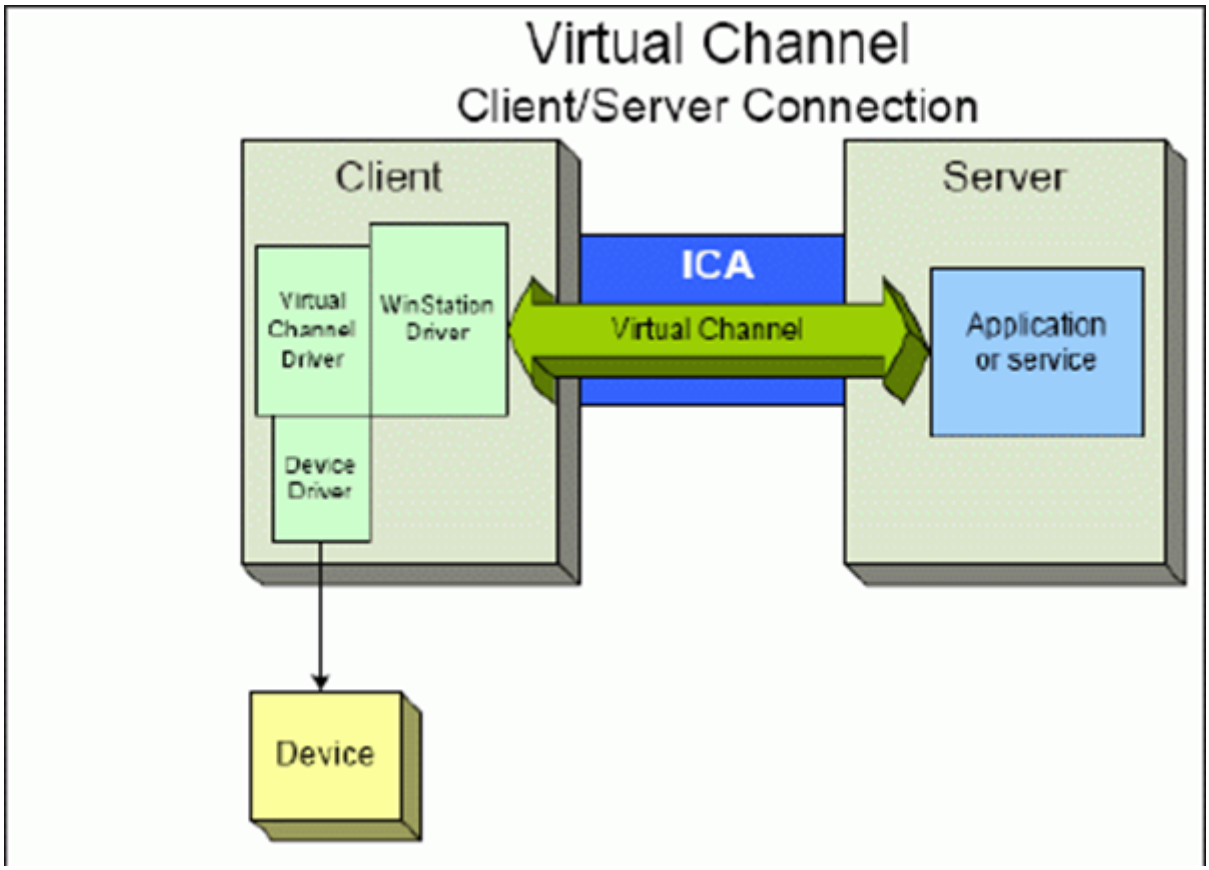
Sur les serveurs DaaS Citrix, différents canaux sont hébergés sous forme de services Windows. Ce type d'hébergement fournit une sémantique « one-to-many » pour plusieurs applications dans une session et plusieurs sessions sur le serveur. Voici des exemples de ces services :

- 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 DaaS. 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

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 DaaS, 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.

Pour plus d'informations, consultez le document Client Object API Specification Programmer's Guide.

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 du 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

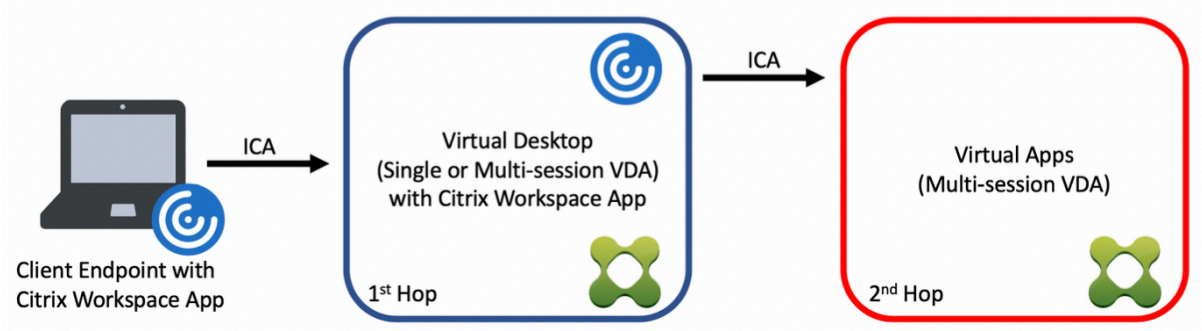
- SDK du canal virtuel ICA
- Le réseau Citrix Developer Network héberge toutes les ressources techniques et toutes les discussions impliquant l'utilisation de SDK Citrix. Dans ce réseau, vous pouvez accéder aux SDK, obtenir des exemples de code et de scripts ainsi que des extensions et plug-ins et consulter 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 DaaS

May 17, 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 DaaS (anciennement Citrix Virtual Apps and Desktops Service) 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 périphériques 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 du contenu du navigateur
- Local App Access

- Pack d'optimisation RealTime pour Skype Entreprise
- Optimisation pour Microsoft Teams

Connectivité HDX

May 17, 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

May 17, 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 :

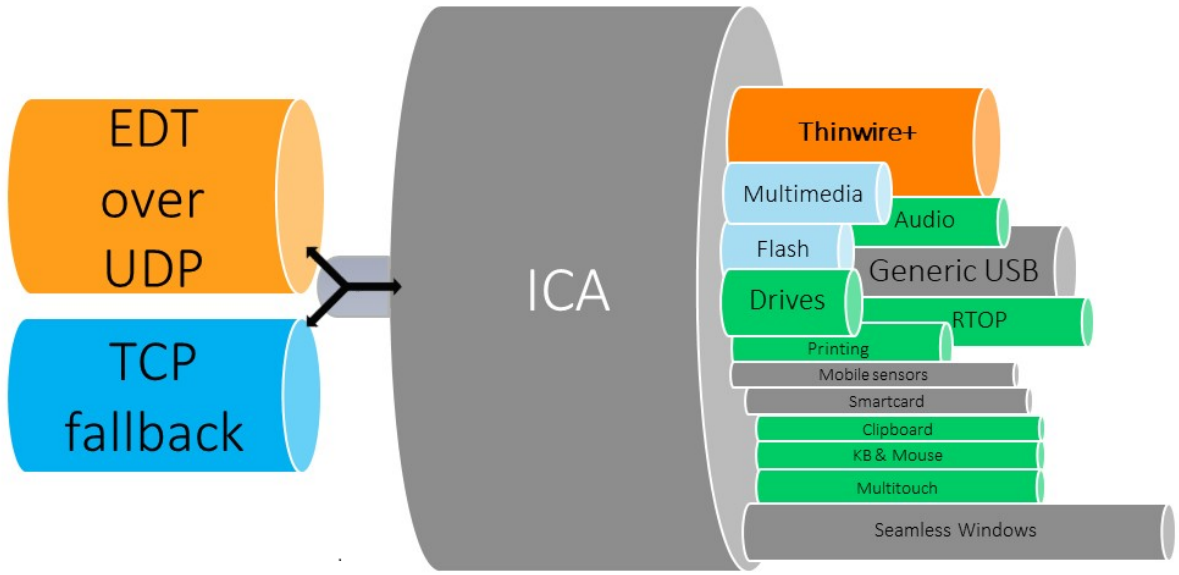
- **Préféré** : (par défaut) le client tente de se connecter avec le protocole préféré et revient au protocole TCP si la connectivité avec le protocole préféré n'est pas disponible.
- **Mode de diagnostic** : le client tente de se connecter uniquement à l'aide du protocole préféré. Le retour vers TCP est désactivé.
- **Désactivé** : le client tente uniquement de se connecter via le protocole TCP.

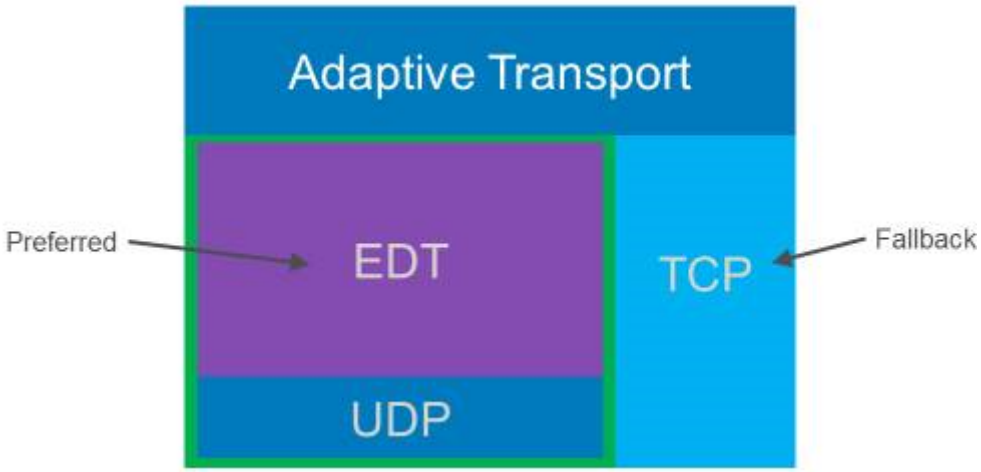
Fonctionnement

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 (2402 ou version ultérieure recommandée)
  - Linux : version actuellement prise en charge (2402 ou version ultérieure recommandée)
- Application Citrix Workspace
  - Windows : version actuellement prise en charge (2402 ou version ultérieure recommandée)
  - Linux : version actuellement prise en charge (2402 ou version ultérieure recommandée)
  - Mac : version actuellement prise en charge (2402 ou version 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

Description	Protocole	Source	Destination	Port de destination
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

Description	Protocole	Source	Destination	Port de destination
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

May 17, 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.

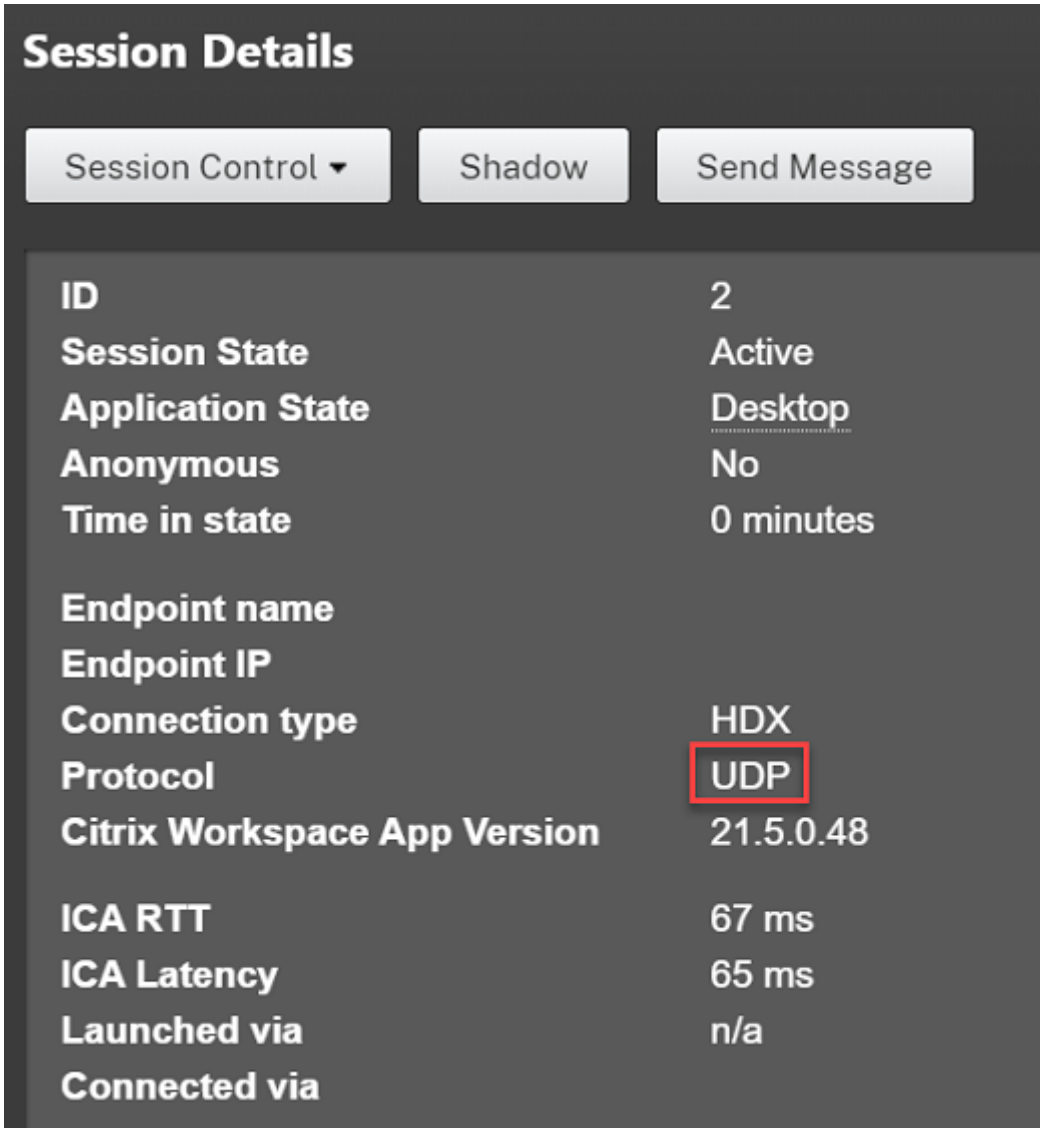
> **Remarque :**
>
> - La **Fiabilité de session** doit être activée pour que la découverte MTU fonctionne.
> - La découverte MTU avec ICA Multi-Stream est disponible avec les versions 2209 et ultérieures du VDA.

Dépannage

May 17, 2024

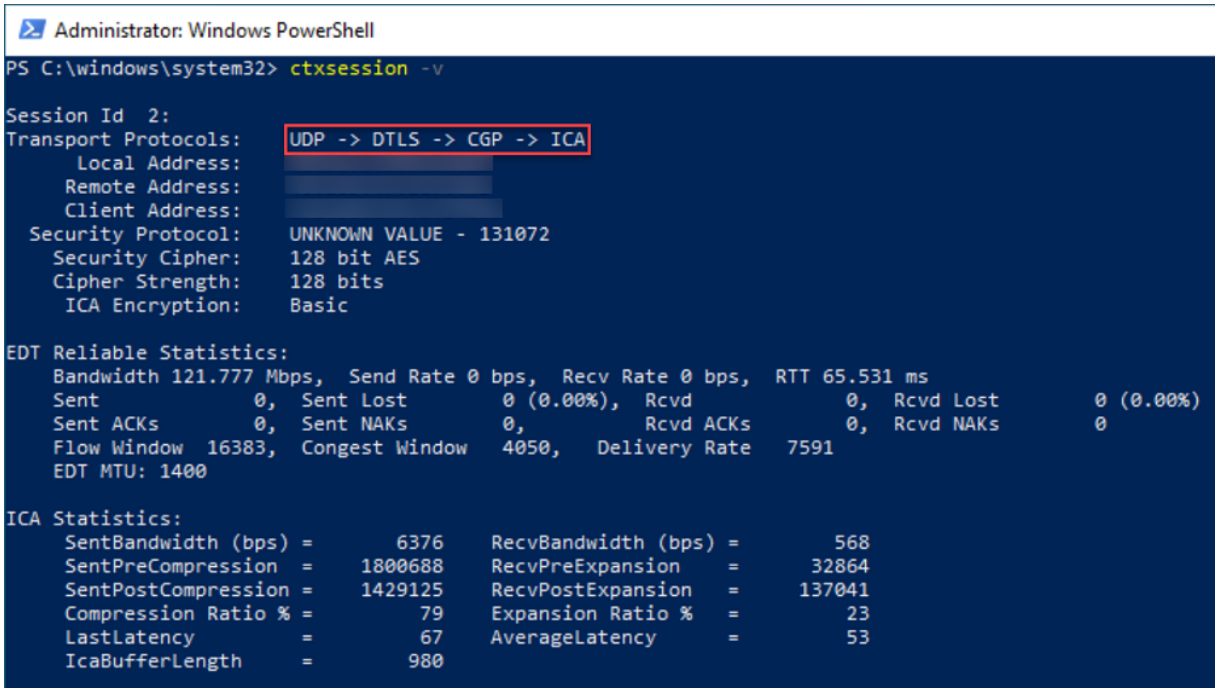
Pour confirmer qu'EDT est utilisé comme protocole de transport pour la session, vous pouvez utiliser Director ou l'utilitaire de ligne de commande `CtxSession.exe` sur le VDA.

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.

Protocole Rendezvous

June 8, 2023

Lors de l'utilisation du service Citrix Gateway, le protocole Rendezvous permet de contourner les Citrix Cloud Connector pour se connecter directement et en toute sécurité au plan de contrôle Citrix Cloud.

Il existe deux types de trafic à prendre en compte :

1. Trafic du contrôle pour l'enregistrement du VDA et la négociation des sessions.
2. Trafic des sessions HDX.

Deux versions de Rendezvous sont disponibles :

- Version 1 (V1) : prend en charge le contournement des Citrix Cloud Connector pour le trafic des sessions HDX uniquement.
- Version 2 (V2) : prend en charge le contournement des Citrix Cloud Connector pour le trafic du contrôle et le trafic des sessions HDX.

Pour plus d'informations sur la configuration requise, les considérations et la configuration de chacune des versions de Rendezvous, consultez leur documentation respective.

Documentation Rendezvous V1

Documentation Rendezvous V2

Rendezvous V1

April 20, 2023

Lors de l'utilisation du service Citrix Gateway, le protocole Rendezvous permet de contourner les Citrix Cloud Connector pour se connecter directement et en toute sécurité au plan de contrôle Citrix Cloud.

Exigences

- Accès à l'environnement à l'aide du service Citrix Workspace et Citrix Gateway.
- Plan de contrôle : Citrix DaaS (Citrix Cloud).
- VDA : Version 1912 ou ultérieure.

  - La version 2012 est la version minimale requise pour EDT Rendezvous.
  - La version 2012 est la version minimale requise pour la prise en charge du proxy non transparent (pas de prise en charge des fichiers PAC).
  - La version 2103 est la version minimale requise pour la configuration du proxy avec un fichier PAC.

- Activez le protocole Rendezvous dans la stratégie Citrix. Pour plus d'informations, consultez la section Paramètre de stratégie de protocole Rendezvous.
- Les VDA doivent avoir accès à `https://*.nssvc.net`, y compris tous les sous-domaines. Si vous ne pouvez pas ajouter tous les sous-domaines à la liste d'autorisation de cette manière, utilisez `https://*.c.nssvc.net` et `https://*.g.nssvc.net` à la place. Pour plus d'informations, reportez-vous à la section Exigences en termes de connexion Internet de la documentation Citrix Cloud (sous Citrix DaaS) et à l'article du centre de connaissances CTX270584.
- Les VDA doivent pouvoir se connecter aux adresses mentionnées précédemment sur TCP 443 et UDP 443 pour TCP Rendezvous et EDT Rendezvous, respectivement.
- Les Cloud Connector doivent obtenir les noms de domaine complets des VDA lors de la négociation d'une session. Ceci peut être fait de l'une de ces deux façons :

  - **Activez la résolution DNS pour le site.** Accédez à **Configuration complète > Paramètres** et activez le paramètre **Activer la résolution DNS**. Vous pouvez aussi utiliser le SDK Remote PowerShell Citrix Virtual Apps and Desktops et exécuter la commande `Set-BrokerSite -DnsResolutionEnabled $true`. Pour plus d'informations sur le SDK Remote PowerShell Citrix Virtual Apps and Desktops, consultez SDK et API.
  - **Zone de recherche inversée DNS avec enregistrements PTR pour les VDA.** Si vous choisissez cette option, nous vous recommandons de configurer les VDA pour toujours tenter d'inscrire les enregistrements PTR. Pour ce faire, utilisez l'Éditeur de stratégie de groupe ou l'Objet de stratégie de groupe, accédez à **Configuration ordinateur > Modèles d'administration > Réseau > Client DNS**, puis définissez **Inscrire les enregistrements PTR** sur **Activé et Inscrire**. Si le suffixe DNS de la connexion ne correspond pas au suffixe DNS du domaine, vous devez également configurer le paramètre du **suffixe DNS spécifique à la connexion** afin que les machines puissent inscrire les enregistrements PTR correctement.

> **Remarque :**
>
> Si vous utilisez l'option de résolution DNS, les Cloud Connector doivent être en mesure de résoudre les noms de domaine complets (FQDN) des machines VDA. Dans le cas où les utilisateurs internes se connectent directement aux machines VDA, les machines clientes doivent également être en mesure de résoudre les noms de domaine des machines VDA.
>
> Si vous utilisez une zone de recherche inversée DNS, les FQDN des enregistrements PTR

> doivent correspondre aux noms de domaine FQDN des machines VDA. Si l'enregistrement PTR contient un FQDN différent, la connexion Rendezvous échoue. Par exemple, si le FQDN de la machine est `vda01.domain.net`, l'enregistrement PTR doit contenir `vda01.domain.net`. Un FQDN différent tel que `vda01.sub.domain.net` ne fonctionne pas.

Configuration du proxy

Le VDA prend en charge les connexions Rendezvous via un proxy.

Considérations relatives au proxy

Prenez les points suivants en considération lors de l'utilisation de proxy avec Rendezvous :

- Les proxy transparents, les proxy HTTP non transparents et les proxy SOCKS5 sont pris en charge.
- Le décryptage et l'inspection des paquets ne sont pas pris en charge. Configurez une exception afin que le trafic ICA entre le VDA et le service de passerelle ne soit pas intercepté, décrypté ou inspecté. Sinon, la connexion est interrompue.
- Les proxies HTTP prennent en charge l'authentification basée sur une machine à l'aide de Negotiate et des protocoles d'authentification Kerberos ou NT LAN Manager (NTLM).

  Lorsque vous vous connectez au serveur proxy, le schéma d'authentification Negotiate sélectionne automatiquement le protocole Kerberos. Si Kerberos n'est pas pris en charge, Negotiate bascule sur NTLM pour l'authentification.

  > **Remarque :**
  >
  > Pour utiliser Kerberos, vous devez créer le nom principal de service (SPN) du serveur proxy et l'associer au compte Active Directory du proxy. Le VDA génère le SPN au format `HTTP/<proxyURL>` lorsqu'il établit une session, où l'URL du proxy est extraite du paramètre de stratégie **proxy Rendezvous**. Si vous ne créez pas de SPN, l'authentification bascule vers NTLM. Dans les deux cas, l'identité de la machine VDA est utilisée pour l'authentification.

- L'authentification avec un proxy SOCKS5 n'est actuellement pas prise en charge. Si vous utilisez un proxy SOCKS5, configurez une exception afin que le trafic destiné aux adresses du service de passerelle (spécifié dans les exigences) puisse contourner l'authentification.
- 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.

Proxy transparent

Si vous utilisez un proxy transparent dans votre réseau, aucune configuration supplémentaire n'est requise sur le VDA.

Proxy non transparent

Si vous utilisez un proxy non transparent sur votre réseau, configurez le paramètre Configuration du proxy Rendezvous. Lorsque le paramètre est activé, spécifiez l'adresse proxy HTTP ou SOCKS5, ou entrez le chemin d'accès au fichier PAC pour que le VDA sache quel proxy utiliser. Par exemple :

- Adresse proxy : `http://<URL or IP>:<port>` ou `socks5://<URL or IP>:<port>`
- Fichier PAC : `http://<URL or IP>/<path>/<filename>.pac`

Si vous utilisez le fichier PAC pour configurer le proxy, définissez le proxy en utilisant la syntaxe requise par le service HTTP Windows : `PROXY [<scheme>=]<URL or IP>:<port>`. Par exemple, `PROXY socks5=<URL or IP>:<port>`.

Validation de Rendezvous

Si vous remplissez toutes les conditions requises, procédez comme suit pour confirmer si Rendezvous est utilisé :

1. Lancez PowerShell ou une invite de commandes dans la session HDX.
2. Exécutez `ctxsession.exe –v`.
3. Les protocoles de transport utilisés indiquent le type de connexion :
    - TCP Rendezvous : **TCP > SSL > CGP > ICA**
    - EDT Rendezvous : **UDP > DTLS > CGP > ICA**
    - Proxy via Cloud Connector : **TCP > CGP > ICA**

Autres considérations

Ordre de la suite de chiffrement Windows

Pour un ordre de suite de chiffrement personnalisé, assurez-vous d'inclure les suites de chiffrement prises en charge par VDA dans la liste suivante :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Si l'ordre de la suite de chiffrement personnalisé ne contient pas ces suites de chiffrement, la connexion Rendezvous échoue.

Zscaler Private Access

Si vous utilisez Zscaler Private Access (ZPA), il est recommandé de configurer des paramètres de contournement pour Gateway Service afin d'éviter une latence accrue et son impact sur les performances. Pour ce faire, vous devez définir des segments d'application pour les adresses Gateway Service (spécifiées dans les conditions requises) et les définir de manière à toujours appliquer le contournement. Pour plus d'informations sur la configuration de segments d'application pour contourner ZPA, reportez-vous à la documentation Zscaler.

Rendezvous V2

May 17, 2024

Lors de l'utilisation du service Citrix Gateway, le protocole Rendezvous permet de contourner les Citrix Cloud Connector pour se connecter directement et en toute sécurité au plan de contrôle Citrix Cloud.

Rendezvous V2 est pris en charge avec des machines jointes à un domaine standard, des machines jointes à Azure AD et des machines non jointes à un domaine.

> **Remarque :**
>
> Actuellement, les déploiements sans connecteur sont possibles uniquement avec des machines *jointes à Azure AD* et *n'appartenant pas à un domaine*. Les machines jointes à un domaine AD standard nécessitent toujours des composants Cloud Connector pour l'enregistrement du VDA et la négociation de session. Cependant, il n'existe pas d'exigences DNS pour utiliser Rendezvous V2.
>
> Les exigences de Cloud Connector pour d'autres fonctions non liées à la communication VDA, telles que la connexion à votre domaine AD sur site, le provisioning MCS sur des hyperviseurs sur site, etc., restent les mêmes.

Exigences

Les conditions requises pour utiliser Rendezvous V2 sont les suivantes :

- Accès à l'environnement à l'aide du service Citrix Workspace et Citrix Gateway.

- Plan de contrôle : Citrix DaaS
- VDA version 2203
- Activez le protocole Rendezvous dans la stratégie Citrix. Pour plus d'informations, consultez la section Paramètre de stratégie de protocole Rendezvous.
- La fiabilité de session doit être activée sur les VDA.
- Les machines VDA doivent avoir accès aux éléments suivants :
  - `https://*.xendesktop.net` sur `TCP 443`. Si vous ne pouvez pas autoriser tous les sous-domaines de cette manière, vous pouvez utiliser `https://<customer_ID>.xendesktop.net`, où <customer_ID> est votre identifiant client Citrix Cloud, affiché sur le portail de l'administrateur Citrix Cloud.
  - `https://*.*.nssvc.net` sur `TCP 443` pour la connexion de contrôle avec Gateway Service.
  - `https://*.*.nssvc.net` sur `TCP 443` et `UDP 443` pour les sessions HDX sur TCP et EDT, respectivement.

> **Remarque :**
>
> 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.

Configuration du proxy

Le VDA prend en charge la connexion via des proxys pour contrôler le trafic et le trafic de session HDX lors de l'utilisation de Rendezvous. Les exigences et les considérations relatives aux deux types de trafic étant différentes, examinez-les attentivement.

Considérations relatives au proxy de trafic

- Seuls les proxys HTTP sont pris en charge.
- Le décryptage et l'inspection des paquets ne sont pas pris en charge. Configurez une exception afin que le trafic de contrôle entre le VDA et le plan de contrôle Citrix Cloud ne soit pas intercepté, décrypté ou inspecté. Sinon, la connexion échoue.
- L'authentification du proxy n'est pas prise en charge.

Considérations relatives au proxy de trafic HD

- Les proxys HTTP et SOCKS5 sont pris en charge.

- EDT ne peut être utilisé qu'avec des proxys SOCKS5.
- Par défaut, le trafic HDX utilise le proxy défini pour le trafic de contrôle. Si vous devez utiliser un proxy différent pour le trafic HDX, qu'il s'agisse d'un autre proxy HTTP ou d'un proxy SOCKS5, utilisez le paramètre de stratégie Configuration du proxy Rendezvous.
- Le décryptage et l'inspection des paquets ne sont pas pris en charge. Configurez une exception afin que le trafic HDX entre le VDA et le plan de contrôle Citrix Cloud ne soit pas intercepté, décrypté ou inspecté. Sinon, la connexion échoue.
- L'authentification basée sur la machine est prise en charge uniquement avec les proxys HTTP et si la machine VDA est jointe à un domaine AD. Elle peut utiliser l'authentification Negotiate/Kerberos ou NTLM.

  > **Remarque :**
  >
  > Pour utiliser Kerberos, créez le nom principal de service (SPN) du serveur proxy et associez-le au compte Active Directory du proxy. Le VDA génère le SPN au format `HTTP/<proxyURL>` lorsqu'il établit une session, où l'URL du proxy est extraite du paramètre de stratégie Configuration du proxy Rendezvous. Si vous ne créez pas de SPN, l'authentification bascule vers NTLM. Dans les deux cas, l'identité de la machine VDA est utilisée pour l'authentification.

- L'authentification avec un proxy SOCKS5 n'est actuellement pas prise en charge. Si vous utilisez un proxy SOCKS5, configurez une exception afin que le trafic destiné aux adresses du service de passerelle (spécifié dans les exigences) puisse contourner l'authentification.
- 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.

Proxy transparent

Si vous utilisez un proxy transparent dans votre réseau, aucune configuration supplémentaire n'est requise sur le VDA.

Proxy non transparent

Si vous utilisez un proxy non transparent dans votre réseau, spécifiez le proxy lors de l'installation du VDA afin que le trafic de contrôle puisse atteindre le plan de contrôle Citrix Cloud. Assurez-vous de prendre en compte les considérations relatives au proxy du trafic de contrôle avant de procéder à l'installation et à la configuration.

Dans l'assistant d'installation du VDA, sélectionnez **Configuration du proxy Rendezvous** sur la page **Composants supplémentaires**. Lorsque vous sélectionnez cette option, la page **Configuration du**

proxy Rendezvous est disponible ultérieurement dans l'assistant d'installation. Une fois sur place, entrez l'adresse du proxy ou le chemin d'accès au fichier PAC pour que le VDA sache quel proxy utiliser. Par exemple :

- Adresse proxy : `http://<URL or IP>:<port>`
- Fichier PAC : `http://<URL or IP>/<path/<filename>.pac`

Comme indiqué dans les considérations relatives au proxy de trafic HDX, le trafic HDX utilise le proxy défini par défaut lors de l'installation du VDA. Si vous devez utiliser un proxy différent pour le trafic HDX, qu'il s'agisse d'un autre proxy HTTP ou d'un proxy SOCKS5, utilisez le paramètre de stratégie Configuration du proxy Rendezvous. Lorsque le paramètre est activé, spécifiez l'adresse proxy HTTP ou SOCKS5. Vous pouvez également entrer le chemin d'accès au fichier PAC afin que le VDA sache quel proxy utiliser. Par exemple :

- Adresse proxy : `http://<URL or IP>:<port>` ou `socks5://<URL or IP>:<port>`
- Fichier PAC : `http://<URL or IP>/<path/<filename>.pac`

Si vous utilisez le fichier PAC pour configurer le proxy, définissez le proxy en utilisant la syntaxe requise par le service HTTP Windows : `PROXY [<scheme>=]<URL or IP>:<port>`. Par exemple, `PROXY socks5=<URL or IP>:<port>`.

Comment configurer Rendezvous

Voici les étapes à suivre pour configurer Rendezvous dans votre environnement :

1. Assurez-vous que toutes les exigences sont respectées.
2. Si vous devez utiliser un proxy HTTP non transparent dans votre environnement, configurez-le lors de l'installation du VDA. Reportez-vous à la section Configuration du proxy pour plus de détails.
3. Redémarrez la machine VDA une fois l'installation terminée.
4. Créez une stratégie Citrix ou modifiez une stratégie existante :
    - Définissez le paramètre **Protocole Rendezvous** sur **Autorisé**.
    - Si vous devez configurer un proxy HTTP ou SOCKS5 pour le trafic HDX, configurez le paramètre **Configuration du proxy Rendezvous**.
    - Assurez-vous que les filtres de stratégie Citrix sont correctement définis. La stratégie s'applique aux machines pour lesquelles Rendezvous doit être activé.
5. Assurez-vous que la stratégie Citrix a la bonne priorité afin de ne pas en remplacer une autre.

> **Remarque :**
>
> Si vous utilisez la version 2308 ou antérieure du VDA, la V1 est utilisée par défaut. Pour plus d'informations sur la configuration de la version à utiliser, consultez la section Fonctionnalités HDX

> gérées via le registre.

Validation de Rendezvous

Si vous répondez à toutes les exigences et que vous avez terminé la configuration, procédez comme suit pour vérifier si Rendezvous est utilisé :

1. Dans le bureau virtuel, ouvrez une invite de commande ou PowerShell.
2. Exécutez `ctxsession.exe -v`.
3. Les protocoles de transport utilisés indiquent le type de connexion :
    - TCP Rendezvous : TCP > SSL > CGP > ICA
    - EDT Rendezvous : UDP > DTLS > CGP > ICA
    - Pas Rendez-vous : TCP > CGP > ICA
4. La version de Rendezvous signalée indique la version en cours d'utilisation.

Autres considérations

Ordre de la suite de chiffrement Windows

Si l'ordre des suites de chiffrement a été modifié dans les machines VDA, assurez-vous d'inclure les suites de chiffrement prises en charge par les VDA :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Si l'ordre de la suite de chiffrement personnalisé ne contient pas ces suites de chiffrement, la connexion Rendezvous échoue.

Zscaler Private Access

Si vous utilisez Zscaler Private Access (ZPA), il est recommandé de configurer des paramètres de contournement pour Gateway Service afin d'éviter une latence accrue et son impact sur les performances. Pour ce faire, vous devez définir des segments d'application pour les adresses Gateway Service (spécifiées dans les conditions requises) et les définir de manière à toujours appliquer le contournement. Pour plus d'informations sur la configuration de segments d'application pour contourner ZPA, reportez-vous à la documentation Zscaler.

Problèmes connus

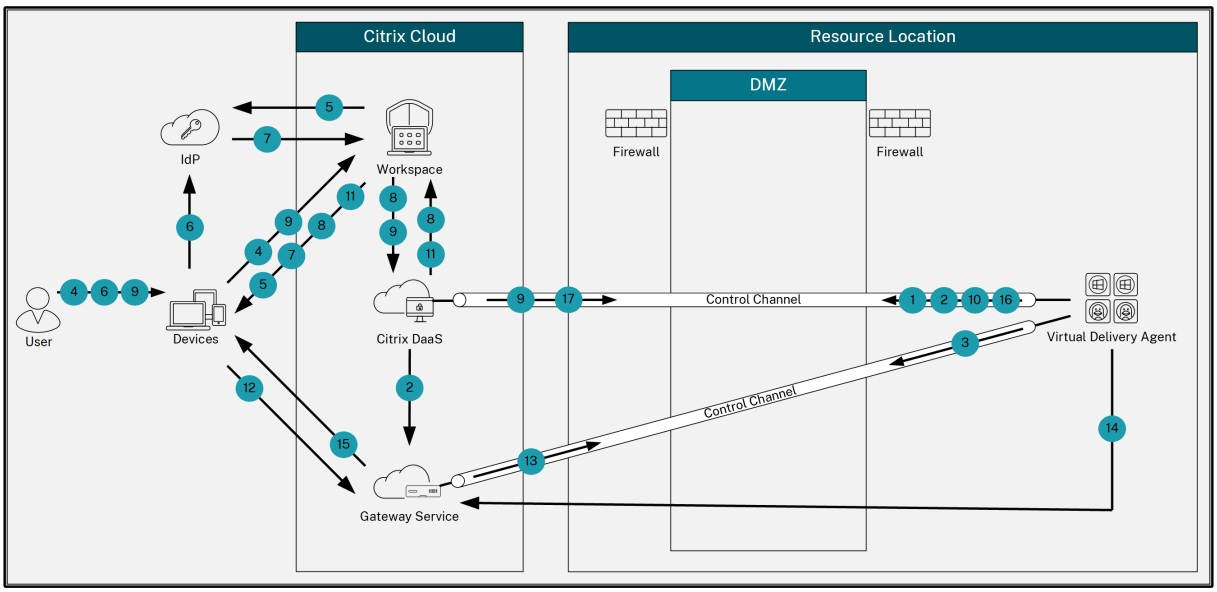
Le programme d'installation du VDA 2203 n'autorise pas la saisie d'une barre oblique (/) pour l'adresse du proxy

Pour contourner le problème, vous pouvez configurer le proxy dans le registre après l'installation du VDA :

```
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
Value type: String
Value name: ProxySettings
Value data: Proxy address or path to pac file. For example:
    Proxy address: http://squidk.test.local:3128
    Pac file: http://file.test.com/config/proxy.pac
```

Flux de trafic Rendez-vous

Le schéma suivant illustre la séquence des étapes relatives au flux de trafic Rendezvous.



1. Le VDA établit une connexion WebSocket avec Citrix Cloud et s'enregistre.
2. Le VDA s'enregistre auprès de Citrix Gateway Service et obtient un jeton dédié.
3. Le VDA établit une connexion de contrôle permanente avec Gateway Service.
4. L'utilisateur accède à Citrix Workspace.
5. Workspace évalue la configuration de l'authentification et redirige les utilisateurs vers le fournisseur d'identité approprié pour l'authentification.
6. L'utilisateur saisit ses informations d'identification.
7. Une fois les informations d'identification de l'utilisateur validées, l'utilisateur est redirigé vers Workspace.

8. Workspace compte les ressources liées à l'utilisateur et les affiche.
9. L'utilisateur sélectionne un bureau ou une application dans Workspace. Workspace envoie la demande à Citrix DaaS qui négocie la connexion et demande au VDA de préparer la session.
10. Le VDA répond à l'aide de la fonctionnalité Rendezvous et de son identité.
11. Citrix DaaS génère un ticket de lancement et l'envoie à la machine utilisateur via Workspace.
12. Le point de terminaison de l'utilisateur se connecte à Gateway Service et fournit le ticket de lancement pour authentifier et identifier la ressource à laquelle se connecter.
13. Gateway Service envoie les informations de connexion au VDA.
14. Le VDA établit une connexion directe pour la session avec Gateway Service.
15. Gateway Service établit la connexion entre le point de terminaison et le VDA.
16. Le VDA vérifie les licences pour la session.
17. Citrix DaaS envoie les stratégies applicables au VDA.

HDX Direct (Technical Preview)

June 12, 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
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 :

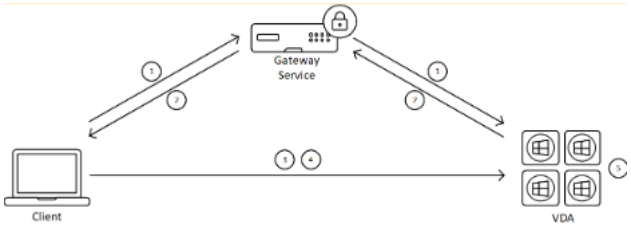
- HDX Direct pour les utilisateurs externes est uniquement disponible avec EDT (UDP) comme protocole de transport. Le **transport adaptatif** doit donc être activé.
- Si vous utilisez **HDX Insight**, notez que l'utilisation de **HDX Direct** empêche la collecte de données HDX Insight, car la session 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.

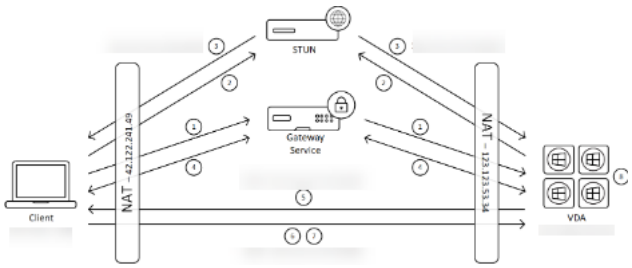


1. Le client établit une session HDX via Gateway Service.
2. Une fois la connexion établie, le VDA envoie au client le nom de domaine complet de la machine VDA, une liste de ses adresses IP et le certificat de la machine VDA via la connexion HDX.
3. Le client analyse les adresses IP pour voir s'il peut 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 12, 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 :

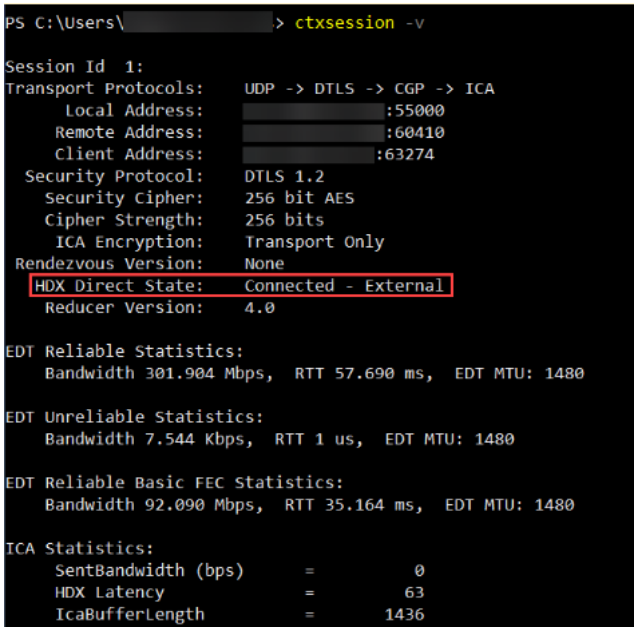
Machine cliente	Hôte de la session	Il devrait fonctionner ?
Cartographie indépendante des terminaux	Cartographie indépendante des terminaux	Oui
Cartographie indépendante des terminaux	Cartographie dépendante des terminaux	Oui
Cartographie dépendante des terminaux	Cartographie indépendante des terminaux	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

January 25, 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 au sein de la session et exécutez `ctxsession.exe -v`. Si la connexion **HDX Direct** est établie, le **statut HDX Direct** est `Connected`.



Pour savoir si la connexion HDX Direct a été établie ou a échoué, vous pouvez également consulter les journaux d'événements de l'hôte de session. Consultez la section **Journaux d'événements** pour plus de détails.

> 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.

HDX Direct ne parvient pas à établir une connexion directe

Si HDX Direct ne parvient pas à établir une connexion directe, passez en revue les étapes suivantes :

1. Vérifiez que la version du VDA et celle 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 pour activer HDX Direct et qu'aucune autre stratégie n'est définie avec une priorité plus élevée qui désactive 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. Vérifiez que le service Citrix CLxMTP est en cours d'exécution sur l'hôte de la session.
5. Vérifiez que le service Citrix Certificate Manager est en cours d'exécution sur l'hôte de la session. Si ce n'est pas le cas, 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 CA racine 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'organisation 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'organisation est Citrix Systems, Inc.

8. Si les certificats sont manquants, 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 CA racine auto-signé et le certificat de serveur auto-signé.
c) Démarrez le service Citrix Certificate Manager sur l'hôte de la session. Une fois démarré, le service crée les certificats.

10. Pour les utilisateurs internes :

a) Vérifiez que le pare-feu de l'hôte de session ne bloque pas le trafic entrant sur le port UDP 443 ou TCP 443, respectivement pour HDX sur EDT et HDX sur TCP.
b) Vérifiez que le pare-feu réseau ne bloque pas le trafic sur le port 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 fonctionne comme prévu. 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, vérifiez qu'il ne bloque pas le trafic sortant sur le port UDP 3478.
   ii. Vérifiez que les pare-feux du réseau ne bloquent pas le trafic sortant sur le port UDP 3478.
   iii. Vérifiez que les pare-feux ne bloquent pas la réponse du serveur STUN.
c) Vérifiez que les règles de pare-feu appropriées sont configurées pour autoriser tout le trafic nécessaire. 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 "Plage de ports HDX Direct", vérifiez que les 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 interne <username>.
Journaux des applications et des services > Citrix-HostCore-HDX Direct/Operational	2	HDX Direct	Information	Connexion HDX Direct établie pour un utilisateur externe <username>.
Journaux des applications et des services > Citrix-HostCore-HDX Direct/Operational	3	HDX Direct	Information	La connexion HDX Direct pour l'utilisateur <username>a échoué.

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 CA racine 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 de **SSLEenabled** sur `0`.
7. Supprimez le contenu de la valeur de **SSLThumbprint**.
8. Démarrez le **service Citrix Certificate Manager**.

Secure HDX (Technical Preview)

June 12, 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

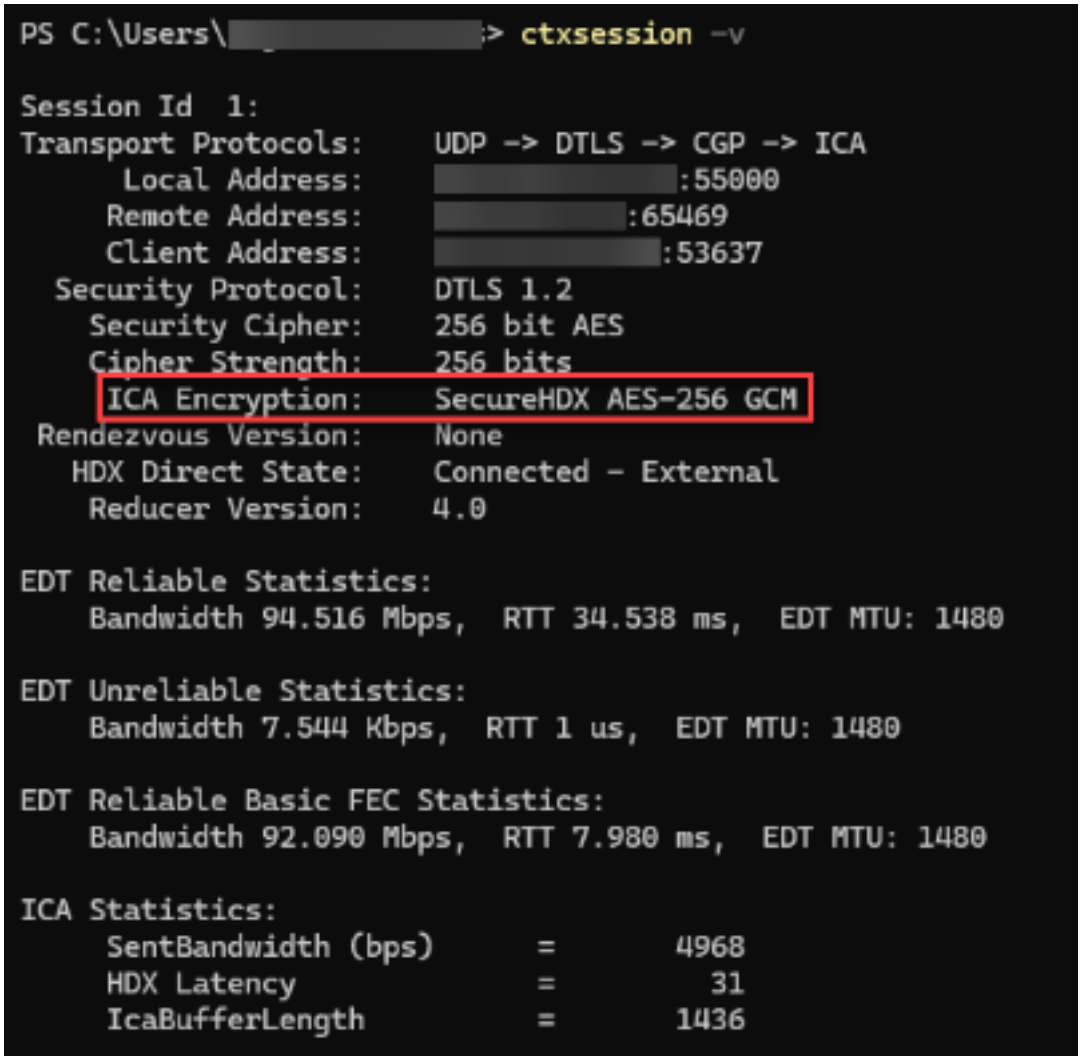
Les points suivants sont à prendre en compte lors de l'utilisation de Secure HDX :

- 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.
- 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.
- 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 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

May 17, 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

May 17, 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>
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>.

Nom du journal	ID	Source	Niveau	Description
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>

Nom du journal	ID	Source	Niveau	Description
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>.
Système	19	Rpm	Erreur	La variable d'environnement <varName> dans le chemin de stratégie VC est introuvable.

Canaux virtuels tiers connus

May 17, 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

November 2, 2023

HDX offre une expérience utilisateur haute définition sur n'importe quel périphérique, n'importe où. Les articles de la section Périphériques décrivent ces périphériques :

- Mappage des lecteurs clients
- Périphérique USB générique
- Appareils mobiles et à écran tactile
- Périphériques en série
- Claviers spécialisés
- Périphériques TWAIN
- Webcams
- Appareils WIA

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

Mappage des lecteurs clients (CDM)

November 2, 2023

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 est également 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 : référez-vous à la configuration système requise pour Linux VDA
- VDA
  - Windows : Citrix Virtual Apps and Desktops 1912 ou versions ultérieures
  - Linux : référez-vous à la documentation Linux VDA

Machine cliente

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
  - Linux : référez-vous à l'application Workspace pour connaître la configuration système requisepour Linux.

Stratégies associées

Reportez-vous à la section relative 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 la 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 utilisez l'Éditeur du Registre à vos propres risques. Veillez à faire une copie de sauvegarde de votre registre avant de le modifier.

Périphériques USB génériques

April 18, 2024

La technologie HDX offre une **prise en charge optimisée** pour la plupart des périphériques USB populaires, parmi lesquels :

- Moniteurs
- Souris
- Claviers
- Téléphones VoIP
- Casques
- Webcams
- Scanners

- Appareils photo
- Imprimantes
- Lecteurs
- Lecteurs de cartes à puce
- Tablettes graphiques
- Dispositifs de signature

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. Pour de plus amples informations sur la redirection USB générique, reportez-vous à Redirection USB générique.

Pour plus d'informations sur les périphériques USB et l'application Citrix Workspace pour Windows, voir Configuration de la redirection de périphérique USB composite et Configuration de la prise en charge USB.

Prise en charge des machines clientes mobiles et à écran tactile

February 21, 2024

Citrix Virtual Apps and Desktops permet aux utilisateurs d'accéder à leurs applications et bureaux publiés à partir de machines clientes mobiles et à écran tactile.

Exigences

Plan de contrôle Citrix

- Citrix Virtual Apps and Desktops 7.15 ou version ultérieure
- Citrix DaaS

Hôte de la session

- Système d'exploitation
  - Windows 10 1903 ou version ultérieure
  - Windows Server 2016 ou version ultérieure

- VDA
  - Windows : version 7.15 ou ultérieure

Machine cliente

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
- Application Citrix Workspace pour Windows version 1808 ou ultérieure

Mode tablette pour les machines 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 appareils à écran tactile mentionnées ci-dessus, les éléments suivants sont requis pour Windows Continuum :

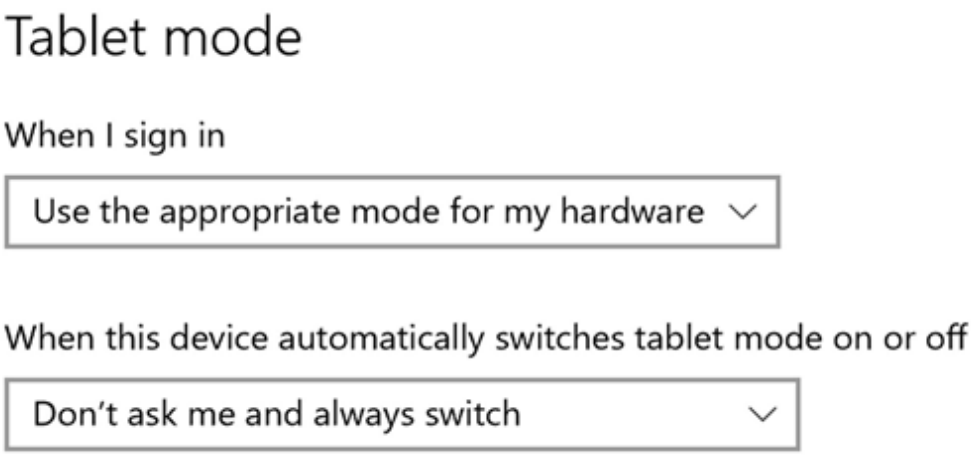
XenServer

- 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
- 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 Server 2016 ou version ultérieure
  - Windows 11
- VDA
  - Windows : version 1903 ou ultérieure

Machine cliente

- Système d'exploitation
  - Windows 10 1809 ou version ultérieure
- Application Citrix Workspace pour Windows version minimale 1902

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

April 27, 2022

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.

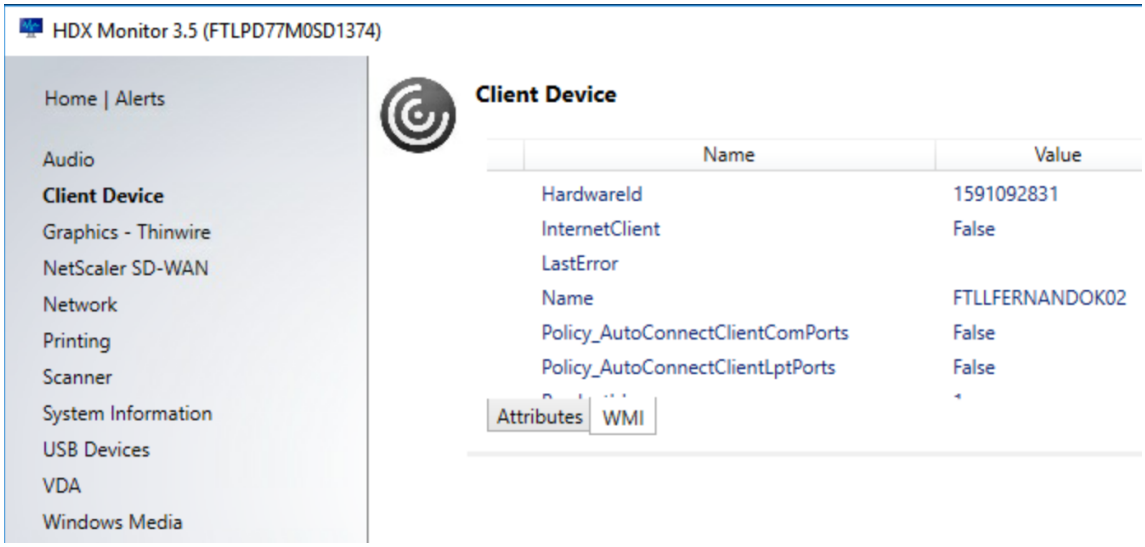
> **Important :**
>
> Si un périphérique peut se connecter au point de terminaison en utilisant directement USB, cela ne signifie pas qu'il peut être redirigé à l'aide de la redirection USB générique. Certains périphériques USB fonctionnent comme des ports COM virtuels, auxquels les applications peuvent 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 :

- Gérez les stratégies de console. 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

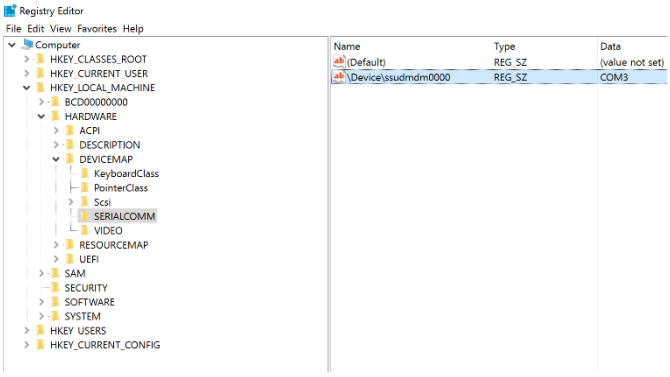
-------------------------------------------------------------------------------
             COM3      \\Client\COM3:            Citrix Client Network
```

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.

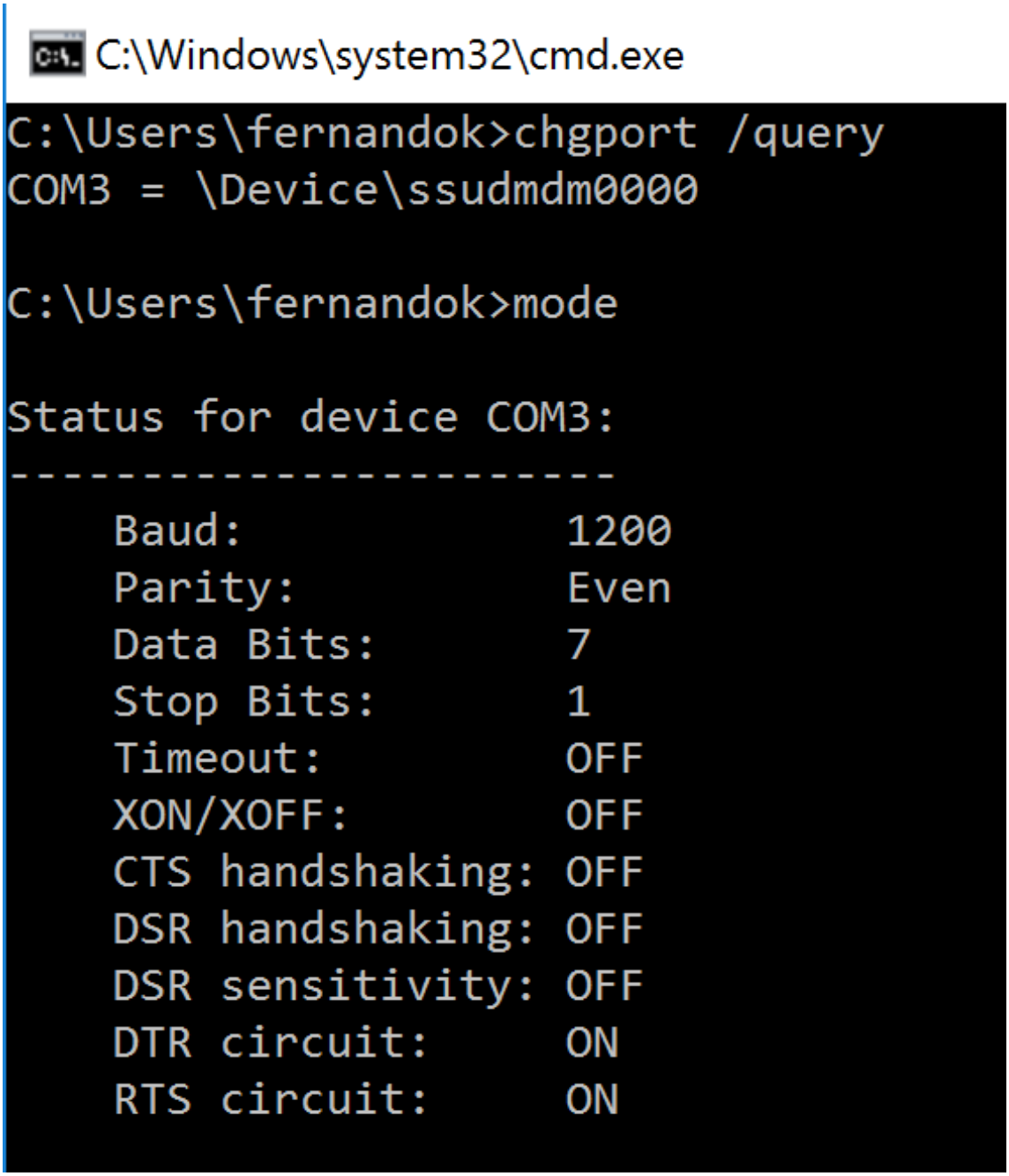
> **Important :**
>
> Le mappage des ports COM n'est pas compatible avec l'interface TAPI. Vous ne pouvez pas mapper les périphériques TAPI (Windows Telephony Application Programming Interface) aux ports COM du client. TAPI définit un moyen standard pour les applications de contrôler les fonctions téléphoniques 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.

Dépanner

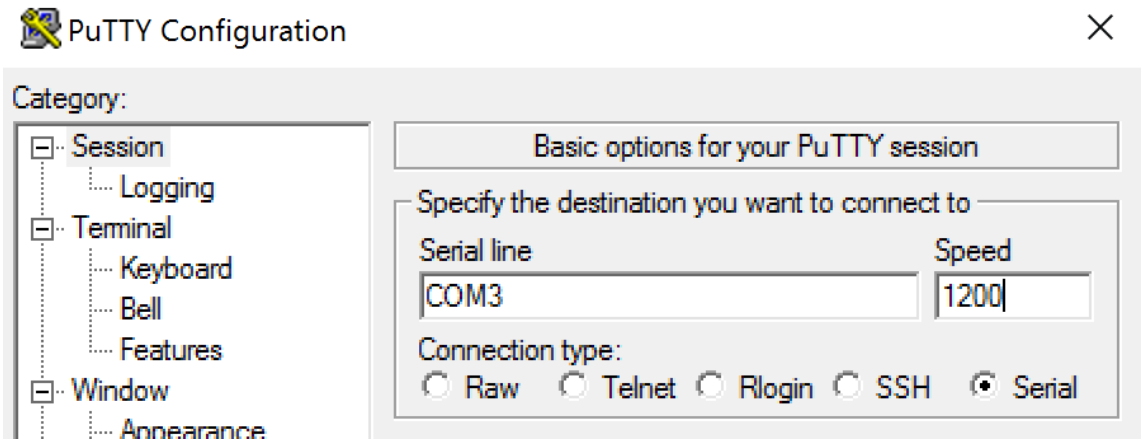
1. Assurez-vous que vous pouvez accéder au périphérique directement depuis le point de terminaison, sans passer par Citrix. Tant que le port n'est pas mappé au VDA, vous n'êtes pas connecté à une session Citrix. Suivez les instructions de dépannage fournies avec le périphérique et vérifiez d'abord qu'il 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 des ports COM à partir de l'éditeur de stratégie de groupe dans Active Directory au lieu de l'interface Gérer > Configuration complète du service. 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 de la console Gérer, 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

April 18, 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 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 Virtual Apps and Desktops prend en charge le clavier Starboard 4 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.

Ce clavier est compatible avec les boîtiers de commutation KVM et peut fonctionner dans deux modes :

- PC (un câble USB sans KVM)
- Mode KVM (Deux câbles USB avec un câble routé via KVM)

> **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 4 est un périphérique composite USB comprenant quatre 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 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 :

- 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.

Périphériques TWAIN

April 27, 2022

Exigences

- Le scanner doit être compatible TWAIN.
- Installez les pilotes TWAIN 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 pilote TWAIN local et non le service Windows Image Acquisition.
- 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

Pour plus d'informations sur les paramètres de stratégie, voir Paramètres de stratégie Périphériques TWAIN.

Webcams

August 23, 2022

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.

Périphériques WIA

April 27, 2022

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 d'autorisation d'applications 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.

Graphiques

April 27, 2022

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 DaaS (anciennement Citrix Virtual Apps and Desktops Service). 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 DaaS.

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 DaaS 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 VM 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 VM 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 basé sur du texte

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.

Informations connexes

- HDX 3D Pro
- Accélération GPU pour OS mono-session Windows
- Accélération GPU pour OS multi-session Windows
- Thinwire
- Filigrane de session basé sur du texte

HDX 3D Pro

January 25, 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.

HDX 3D Pro offre une accélération GPU des machines avec OS mono-session Windows et des machines avec OS multi-session Windows. Pour de plus amples informations, consultez les sections Accélération GPU pour OS mono-session Windows et Accélération GPU pour OS multi-session Windows.

HDX 3D Pro est compatible avec les technologies de virtualisation GPU Passthrough et GPU offertes par les hyperviseurs suivants, ainsi que les machines bare metal :

- XenServer
  - GPU Passthrough avec NVIDIA GRID, AMD et Intel GVT-d
  - Virtualisation GPU avec NVIDIA GRID, AMD et Intel GVT-d
  - Consultez la section Compatibilité matérielle dans la liste de compatibilité matérielle de l'hyperviseur.

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. Pour télécharger l'outil et en apprendre davantage sur celui-ci, consultez https://taas.citrix.com/hdx/download/.

Accélération GPU pour OS multi-session Windows

January 25, 2024

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.

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.

Pour les procédures qui impliquent la modification du registre, faites attention : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter de réinstaller 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, reportez-vous à 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.

Pour confirmer que l'accélération GPU se produit, utilisez un outil tiers tel que GPU-Z. GPU-Z est disponible sur http://www.techpowerup.com/gpuz/.

- 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.

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 2008 R2, DirectX et Direct3D ne requièrent aucun paramètre spécial pour utiliser un seul processeur graphique.
- Sur Windows Server 2012 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 2012 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

January 25, 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.

  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 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 **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 pour 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 + Maj + F5, définissez A=1, S=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.

- Prise en charge de multiples moniteurs haute résolution. Pour les machines avec OS monosession, HDX 3D Pro prend en charge les machines utilisateur avec jusqu'à quatre moniteurs. 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 per-

mettant 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**.

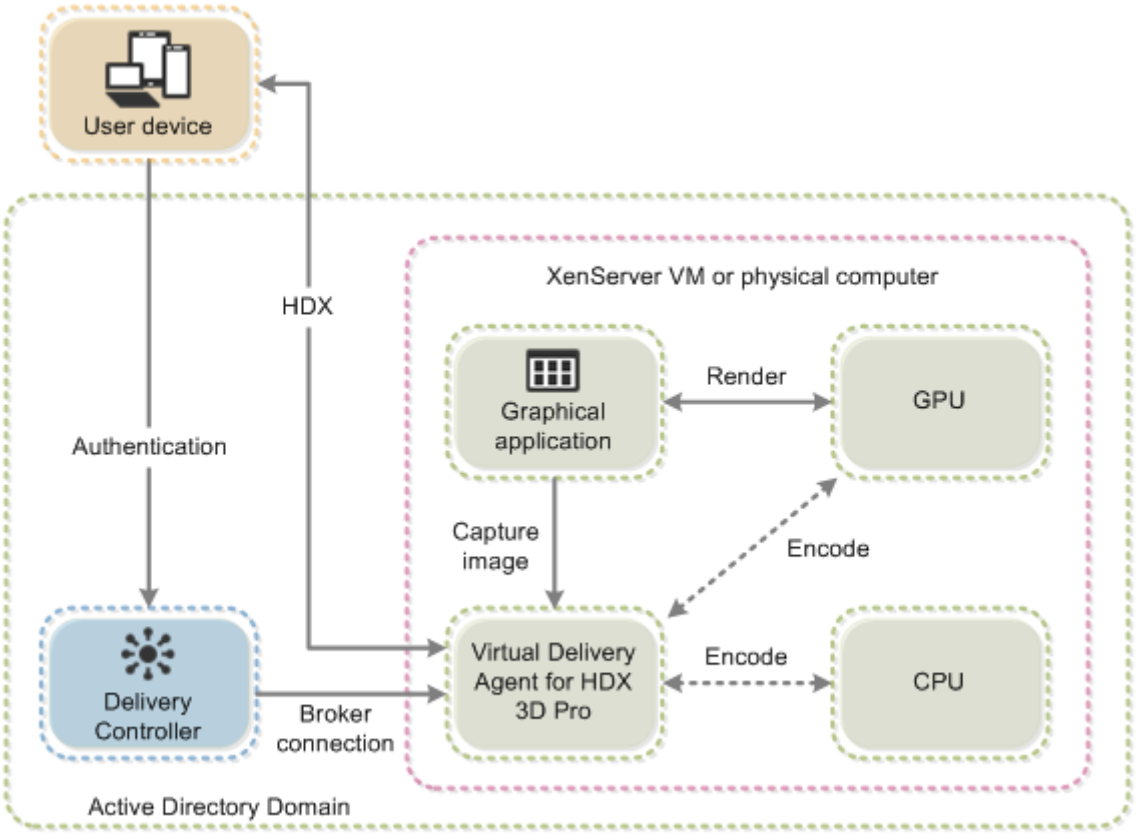
- Prise en charge de l'architecture NVIDIA vGPU. HDX 3D Pro prend en charge les cartes NVIDIA vGPU. Pour plus d'informations, consultez NVIDIA vGPU pour la technologie GPU Passthrough et le partage de GPU. NVIDIA vGPU permet à plusieurs machines virtuelles d'avoir un accès direct simultané à un GPU unique 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 de VMware vSphere/ESX à l'aide de NVIDIA vGPU et AMD MxGPU.
- Prise en charge de Microsoft Hyper-V à l'aide de la technologie DDA de Windows Server 2016.
- Prise en charge de Data Center Graphics avec les processeurs Intel Xeon de la famille E3. HDX 3D Pro prend en charge plusieurs moniteurs (maximum de trois), l'occultation de console, une résolution personnalisée et une fréquence d'images élevée avec la famille de processeurs Intel prise en charge. Pour plus d'informations, veuillez consulter http://www.citrix.com/intel et http://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Prise en charge d'AMD RapidFire sur les cartes pour serveur AMD FirePro S-series. HDX 3D Pro prend en charge plusieurs moniteurs (maximum de 6), l'occultation de la console, une résolution personnalisée et une haute fréquence d'images. Remarque : la prise en charge de HDX 3D Pro pour AMD MxGPU (virtualisation du GPU) fonctionne uniquement avec des vGPU VMware vSphere. XenServer et Hyper-V sont pris en charge avec GPU passthrough. Pour plus d'informations, consultez la section Solution de virtualisation AMD.
- Accès à un encodeur vidéo haute performance pour les GPU NVIDIA, GPU AMD et les processeurs graphiques Intel Iris Pro. Un paramètre de stratégie (activé par défaut) contrôle cette fonctionnalité. La fonctionnalité permet d'utiliser le 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.

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

Pour utiliser HDX 3D Pro avec plusieurs moniteurs, assurez-vous que l'ordinateur hôte est configuré avec au moins autant de moniteurs que sont connectés aux machines utilisateur. Les moniteurs connectés à l'ordinateur hôte peuvent être physiques ou virtuels.

Ne connectez pas de moniteur (qu'il soit physique ou virtuel) à un ordinateur hôte alors qu'un utilisateur est connecté au bureau ou à l'application virtuel(le) fournissant l'application graphique. Cela peut provoquer une instabilité au cours de la session d'un utilisateur.

Faites savoir à vos utilisateurs que les modifications apportées à la résolution du bureau (par eux ou une application) ne sont pas prises en charge lorsqu'une session d'application graphique est en cours d'exécution. Après fermeture de la session d'application, un utilisateur peut modifier la résolution de la fenêtre Desktop Viewer dans l'application Citrix Workspace : Préférences de Desktop Viewer.

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.

Thinwire

May 23, 2023

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 fournit une expérience utilisateur hautement 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 la capacité à monter en charge 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 recomman-

dons 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 ou H.265) 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 2012 R2, Windows Server 2016, Windows Server 2019 et Windows 10. Pour Windows Server 2008 R2, le mode graphique d'ancienne génération est recommandé. Utilisez les modèles de stratégie Citrix intégrés, Montée en charge du serveur élevée - anciens systèmes d'exploitation et Optimisé pour les connexions WAN –anciens systèmes d'exploitation, pour mettre à disposition les combinaisons de paramètres de stratégie recommandées par Citrix pour ces cas d'utilisation.

> **Remarque :**
>
> Nous ne prenons pas en charge le mode graphique d'ancienne génération dans cette version. Il est inclus pour la rétrocompatibilité lors de l'utilisation de XenApp 7.15 LTSR, XenDesktop 7.15 LTSR et des versions précédentes de VDA.

- Le paramètre de stratégie qui détermine le comportement de Thinwire, **Utiliser 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 négociée 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 :

- Thinwire plein écran H.264 ou H.265
- Thinwire avec H.264 ou H.265 sélectif

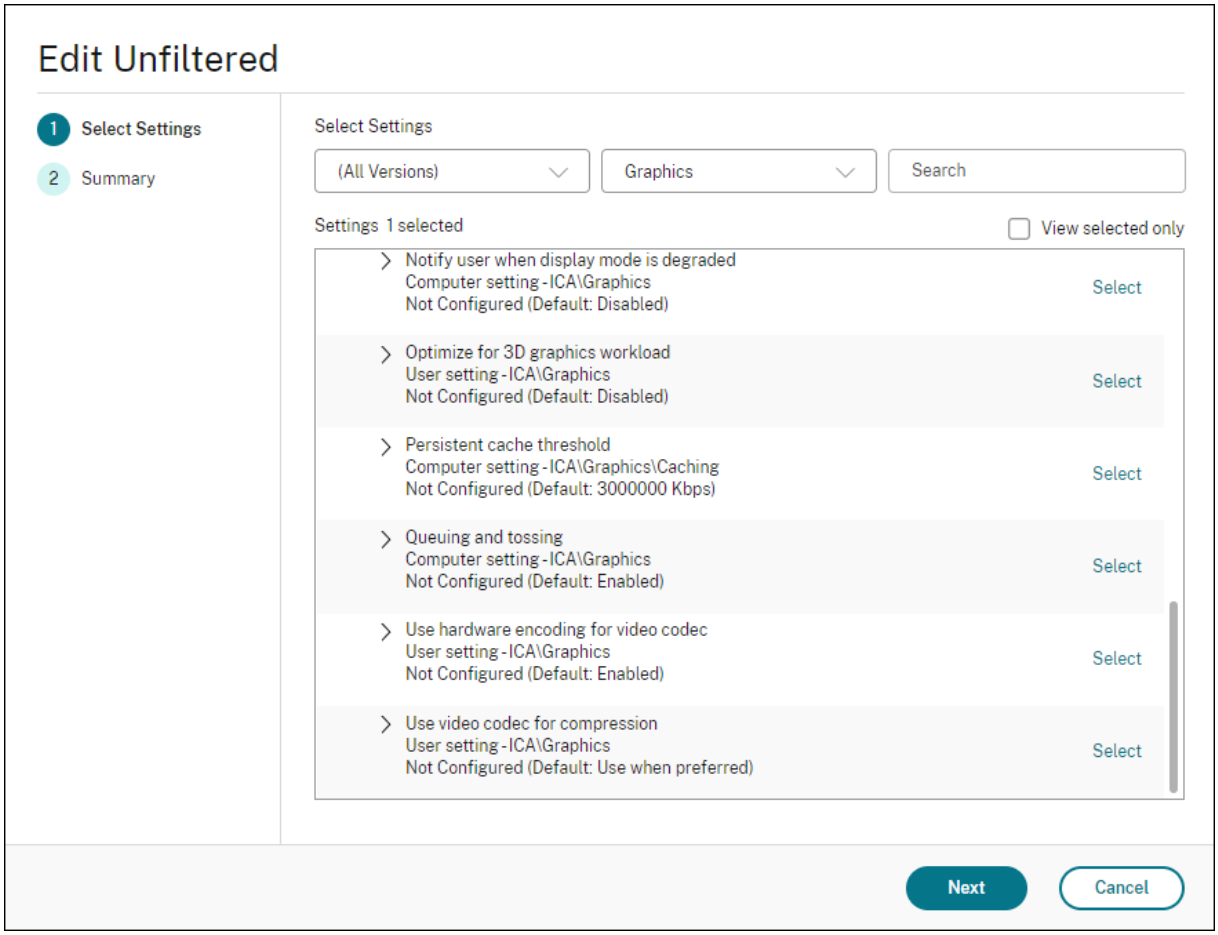
L'accès distant GDI utilise le pilote d'accès distant XPDM et non un codeur bitmap Thinwire.

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 ou H.265 uniquement dans la partie de l'écran sur laquelle l'image est en mouvement.
  - **Pour l'écran entier**. ce paramètre permet de mettre à disposition Thinwire avec H.264 ou H.265 plein écran pour optimiser l'expérience utilisateur et la bande passante, dans les cas dans lesquels 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. Dans de tels cas, envisagez d'utiliser plutôt H.264 Sans perte si possible.



Différents 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

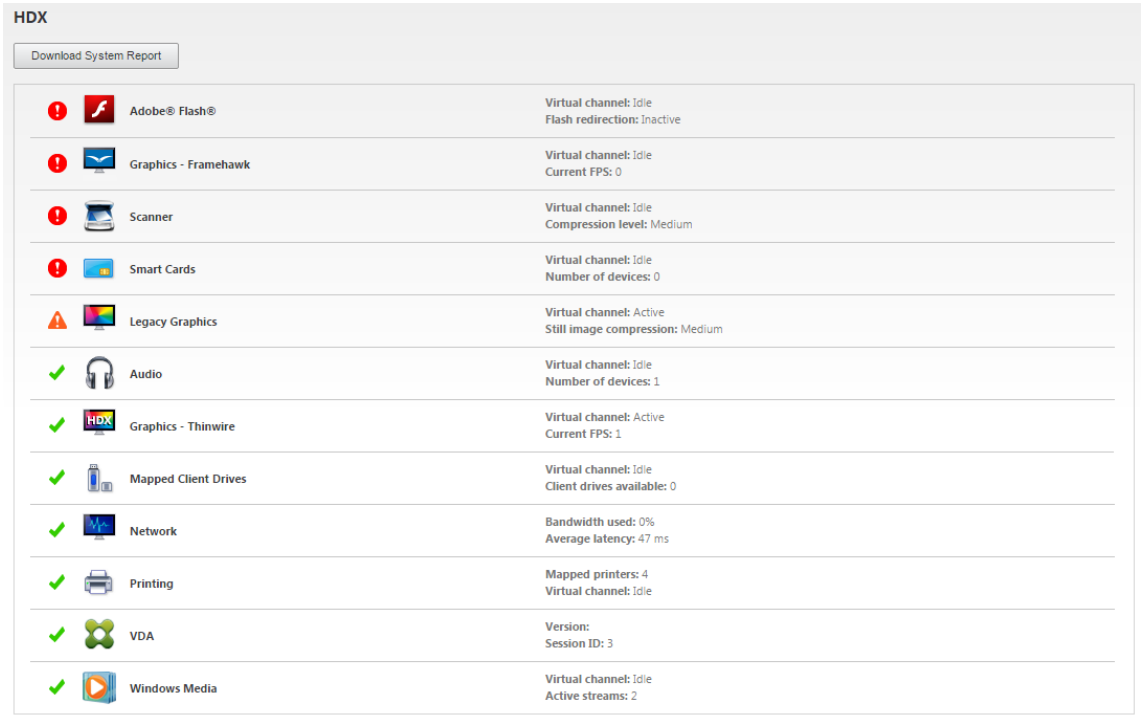
Pour obtenir les combinaisons de paramètres de stratégie recommandées par Citrix pour différents scénarios d'utilisation, utilisez les modèles de stratégie Citrix intégrés. Les modèles **Montée en charge du serveur élevée** et **Expérience utilisateur très haute définition** utilisent tous les deux Thinwire avec les combinaisons de paramètres de stratégie les mieux adaptées aux priorités de votre organisation et aux attentes de vos utilisateurs.

Contrôle de Thinwire

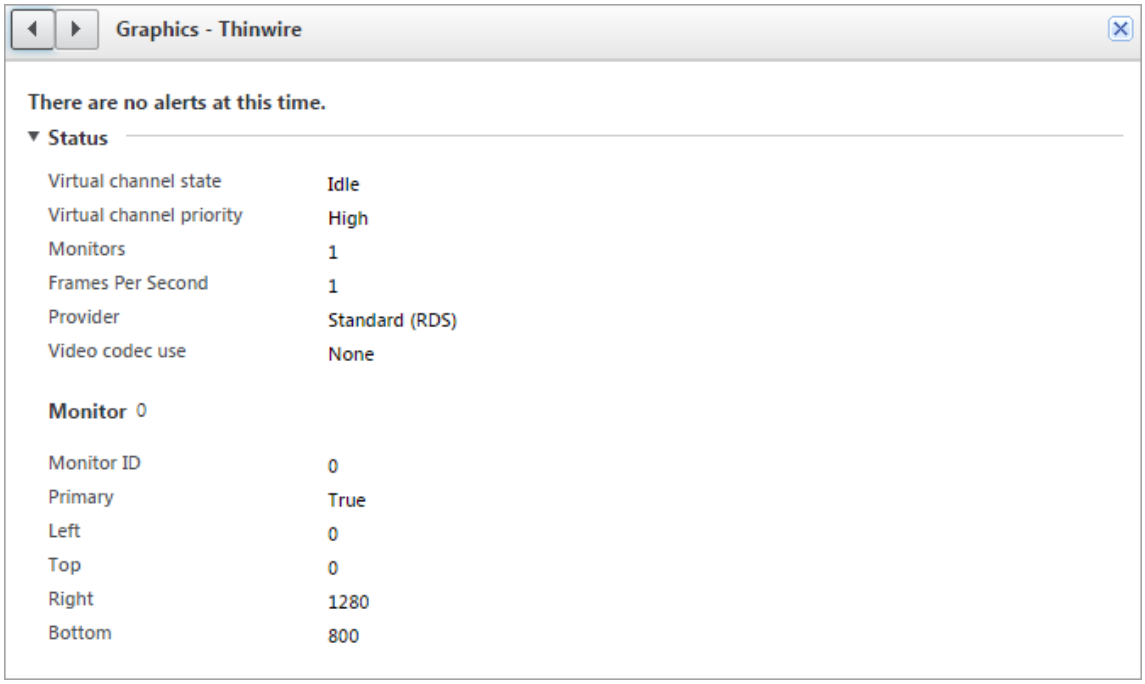
Vous pouvez contrôler l'utilisation et les performances de Thinwire depuis Citrix Director. La vue Détails du canal virtuel HDX contient des informations utiles pour la résolution des problèmes et le con-

trôle 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. Par exemple, la consommation de bande passante attendue lors de l'utilisation du codec MDRLE est d'environ 10 à 15 % inférieure à celle de XenApp et XenDesktop 7.15 LTSR pour les charges de travail de type Office.

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.

H.264 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**.

Sans perte si possible compresse l'écran à l'aide de H.264 (ou H.265) pendant l'activité de l'écran et règle la netteté au pixel près (sans perte) lorsque l'activité s'arrête. La qualité d'image H.264 (ou H.265) s'adapte aux ressources disponibles pour maintenir la meilleure fréquence d'images possible. L'étape de réglage de la netteté est effectuée progressivement, donnant une réponse immédiate si l'utilisateur commence une activité à l'écran peu de temps après le début du réglage. Par exemple, en sélectionnant un modèle et en le faisant pivoter.

L'option H.264 **Sans perte si possible** offre tous les avantages du plein écran H.264 ou H.265, y compris l'accélération matérielle, mais avec l'avantage supplémentaire d'un écran final garanti sans perte. 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, H.264 **Sans perte si possible** 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 :**
>
> En plus de la stratégie **Qualité visuelle**, définissez la stratégie **Utiliser le codec vidéo** sur **Utiliser au choix** (par défaut) ou **Pour les zones changeant constamment**. Vous pouvez revenir à la version non-H.264 Sans perte si possible en définissant la stratégie **Utiliser le codec vidéo** sur **Ne pas utiliser le codec vidéo**. Les images en mouvement sont alors encodées avec JPEG au lieu de H.264 (ou H.265).

Filigrane de session basé sur du texte

March 30, 2022

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.

Multimédia

April 1, 2022

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.

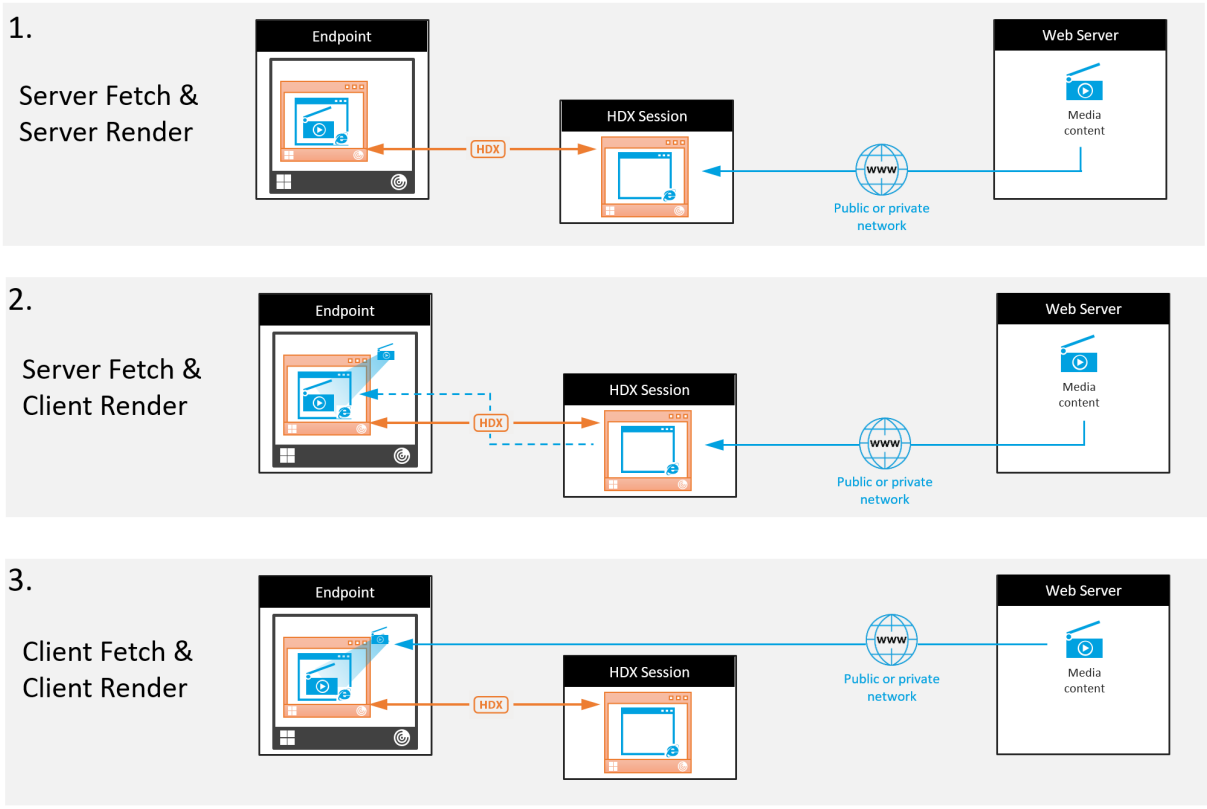
Avec la mise à disposition de multimédia restitué par le serveur, le contenu audio et vidéo est décodé et restitué sur le serveur Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) par l'application. Le contenu est ensuite compressé et distribué via le protocole ICA à l'application Citrix 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 du contenu du navigateur	Non
	Redirection de webcam HDX	Oui
	Redirection vidéo HTML5	Oui
	Redirection Windows Media	Oui

Fonctionnalités audio

September 26, 2022

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.

> **Important :**
>
> Nous vous recommandons de diffuser l'audio à l'aide du protocole UDP (User Datagram Protocol) plutôt que TCP. Seul le Virtual Delivery Agent (VDA) pour Windows prend en charge l'audio via UDP.
>
> 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.

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 :

- Haute qualité (par défaut)
  - 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.

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 plus d'informations, 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 et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) 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 Gérer du service 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.

Limitation

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 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 du contenu de navigateur

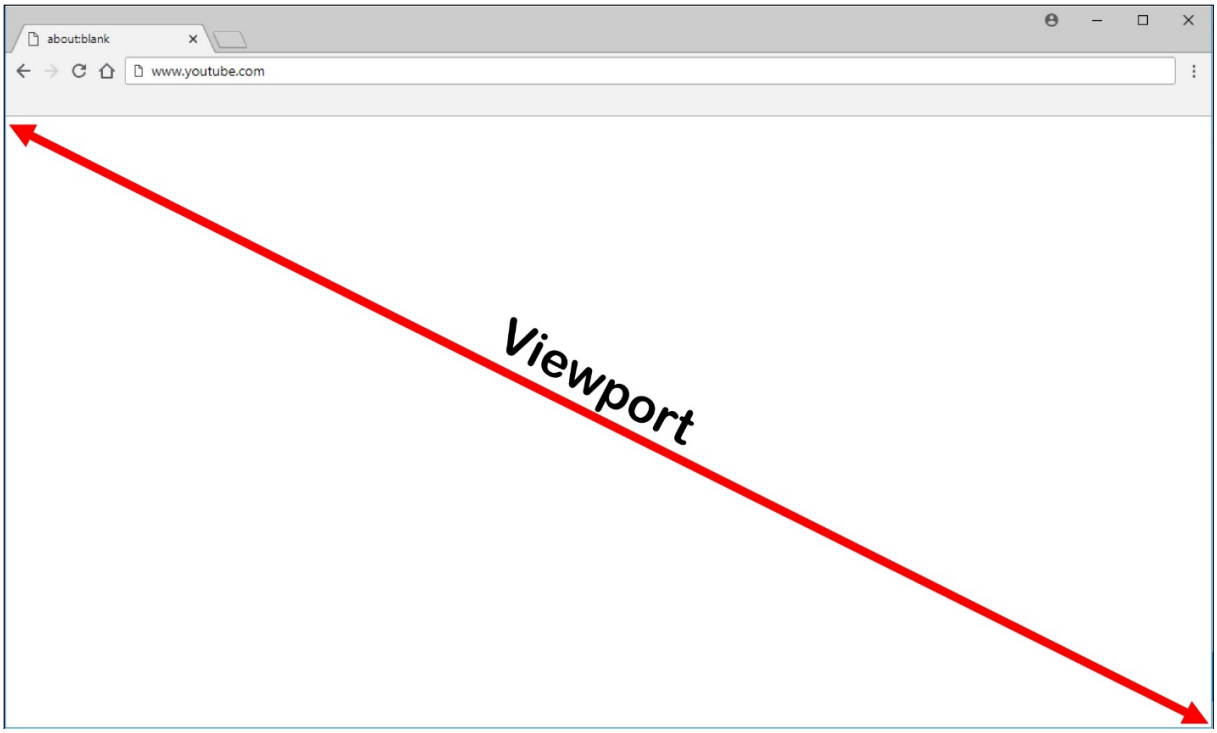
June 30, 2022

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 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 dans l'interface Gérer > Configuration complète qui spécifie la liste de contrôle d'accès contenant les URL de redirection à partir des listes d'autorisation ou de blocage. 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. L'extension de navigateur (BHO) pour Internet Explorer 11 est incluse dans le support d'installation et elle est installée automatiquement. 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.
2. Si une correspondance est trouvée dans la liste d'autorisation (par exemple `https://www.`

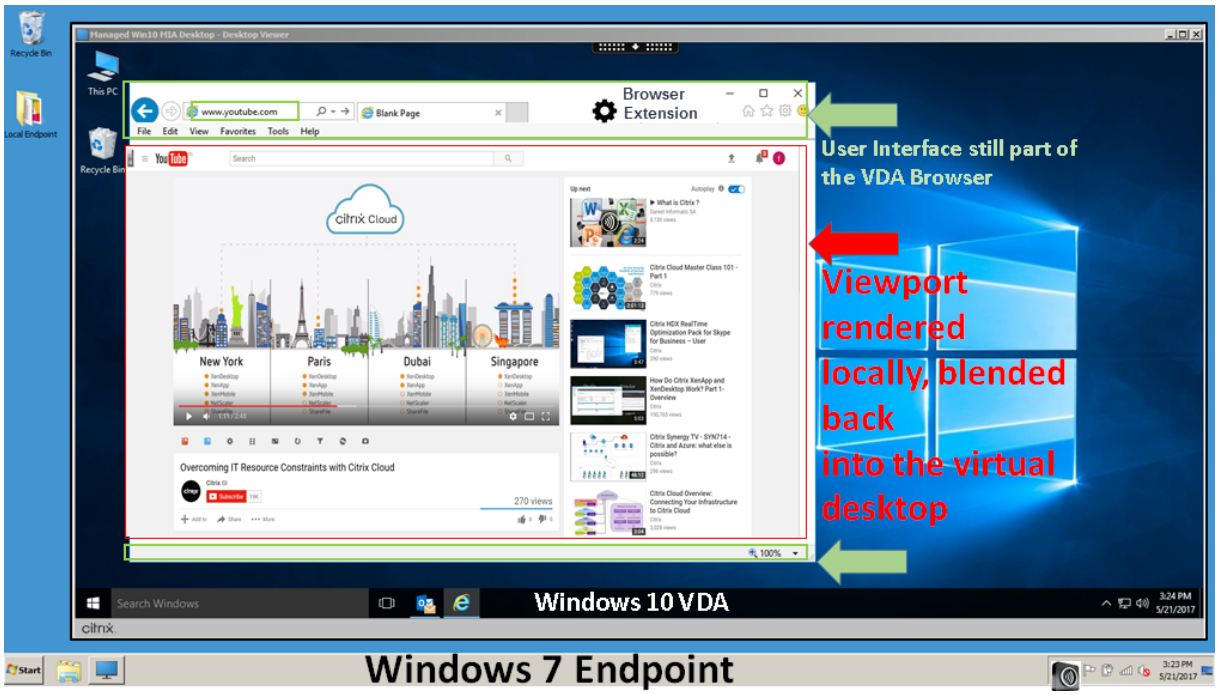
mycompany.com/) et qu'il n'y a pas de correspondance avec une URL dans la liste de blocage (par exemple `https://www.mycompany.com/engineering`), un canal virtuel (CTXCSB) indique à l'application Citrix Workspace qu'une redirection est requise et relaie l'URL. L'application Citrix Workspace instancie 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.

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 :

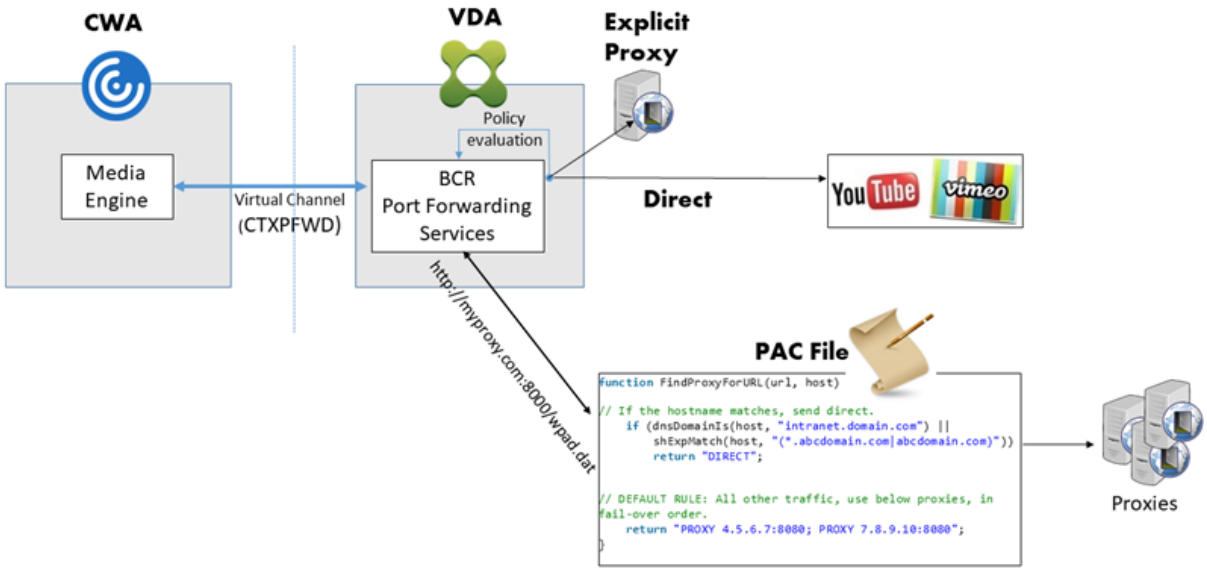
- **Récupération serveur et rendu serveur :** il n'y a pas de redirection car vous n'avez pas ajouté le site à la liste d'autorisation ou la redirection a échoué. Nous revenons au rendu de page Web sur le VDA et utilisons Thinwire pour utiliser à distance les graphiques. Utiliser les stratégies pour contrôler le comportement de secours. Consommation élevée de CPU, de RAM et de bande passante sur le VDA.
- **Récupération serveur et rendu 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.

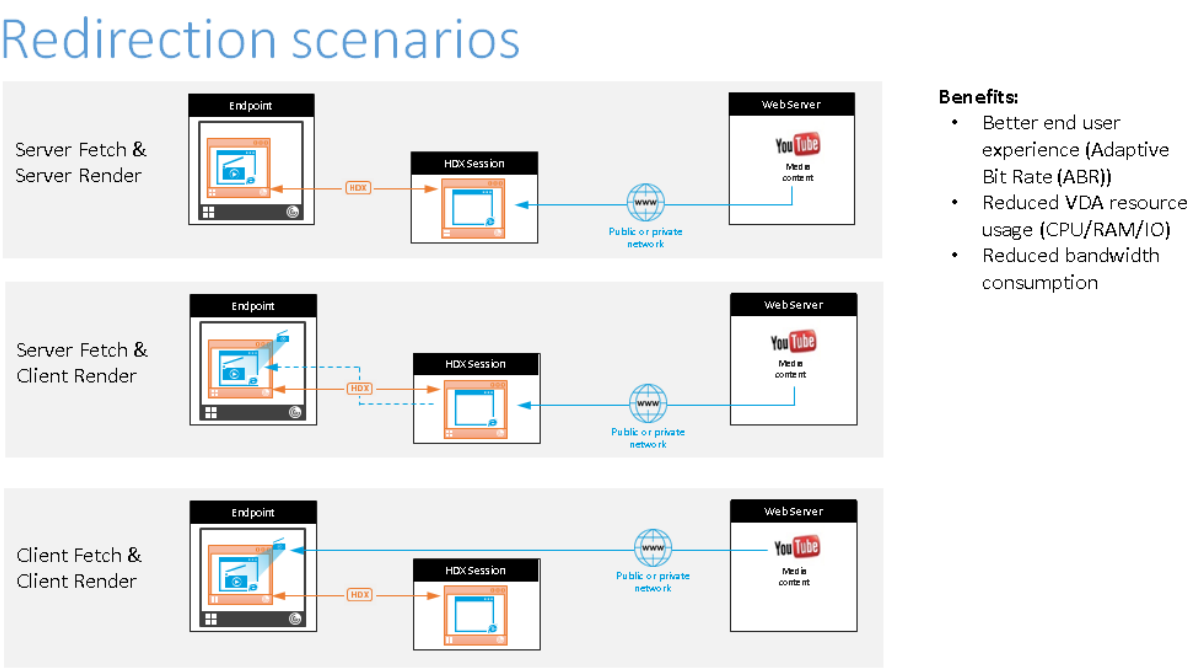
Il existe trois modes de fonctionnement pour ce scénario. Le terme proxy fait référence à un périphérique proxy auquel le VDA accède pour se connecter à Internet.

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 proxy 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 votre site XenApp et XenDesktop.



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 :

Points de terminaison Windows :

- Windows 10 ou 11
- Application Citrix Workspace 1809 pour Windows ou version ultérieure

> **Remarque :**
>
> La redirection de contenu du navigateur est prise en charge uniquement sur la version Current Release de l'application Citrix Workspace pour Windows, mais pas sur les versions LTSR, 1912 et 2203.1 de l'application Citrix Workspace.

Points de terminaison Linux :

- Application Citrix Workspace 1808 pour Linux ou version ultérieure
- Citrix Receiver pour Linux 13.9 ou version ultérieure
- Les terminaux clients légers doivent inclure WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808 et XenApp et XenDesktop 7.15 CU5, 7.18, 7.17, 7.16 :

- Système d'exploitation VDA : Windows 10 (version minimale 1607), Windows Server 2012 R2, Windows Server 2016
- Navigateur sur le VDA :
  - Google Chrome v66 ou version ultérieure (Chrome requiert l'application Citrix Workspace 1809 pour Windows sur le noeud final d'utilisateur, VDA Citrix Virtual Apps and Desktops 7 1808 et l'extension de redirection du contenu du navigateur)
  - Internet Explorer 11 et configurez ces options :
    * Désélectionnez **Mode protégé amélioré** sous **Options Internet** > **Avancé > Sécurité**.
    * Cochez **Activer les extensions tierce partie du navigateur** sous **Options Internet > Avancé > Navigation**.

Résolution des problèmes

Pour obtenir des informations de dépannage, veuillez consulter l'article https://support.citrix.com/article/CTX230052 du centre de connaissances.

Extension Chrome de redirection du contenu du navigateur

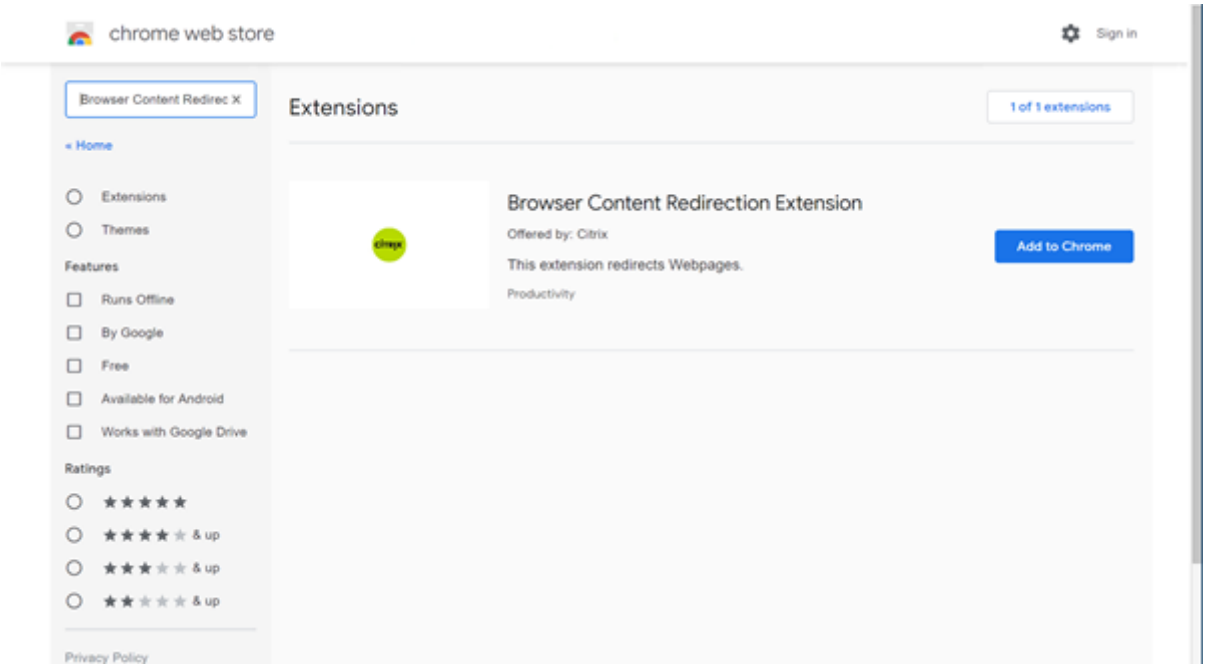
Pour utiliser la redirection du contenu du navigateur avec Chrome, ajoutez l'extension correspondante à partir du Chrome Web Store. Cliquez sur **Ajouter à Chrome** dans l'environnement Citrix Virtual Apps and Desktops.

L'extension **n'est pas** requise sur la machine cliente de l'utilisateur - uniquement dans le VDA.

Configuration système requise

- Chrome v66 ou version ultérieure
- Extension de redirection du contenu du navigateur
- Citrix Virtual Apps and Desktops 7 1808 ou version ultérieure
- Application Citrix Workspace 1809 pour Windows ou version ultérieure

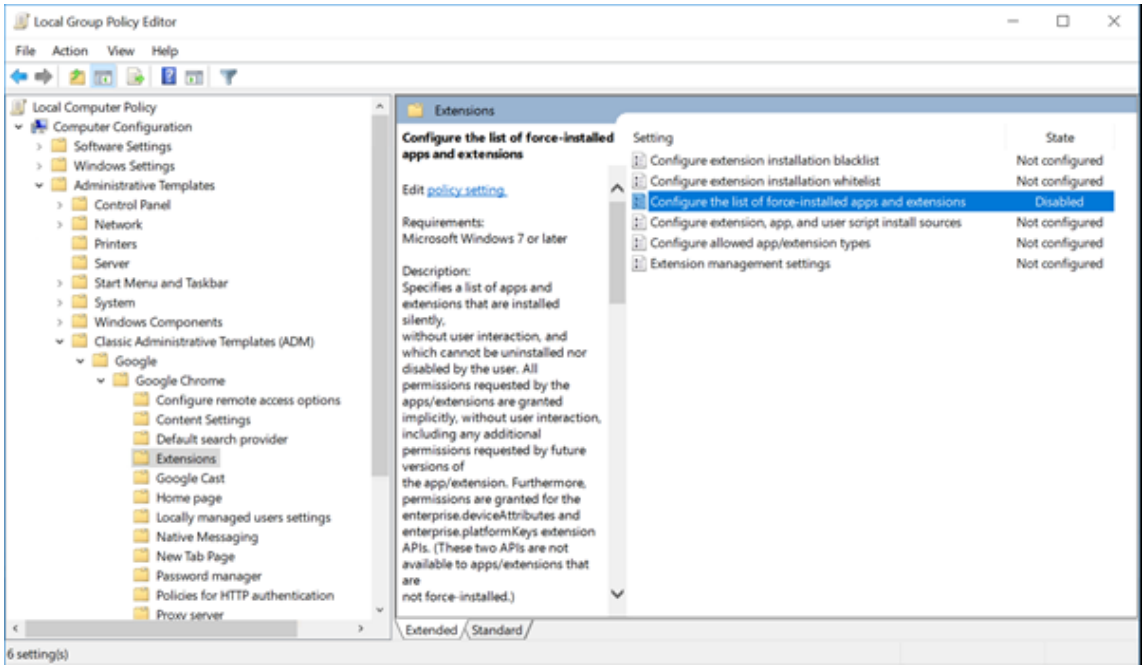
> **Remarque :**
>
> La redirection de contenu du navigateur est prise en charge uniquement sur la version Current Release de l'application Citrix Workspace pour Windows, mais pas sur les versions LTSR, 1912 et 2203.1 de l'application Citrix Workspace.



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.

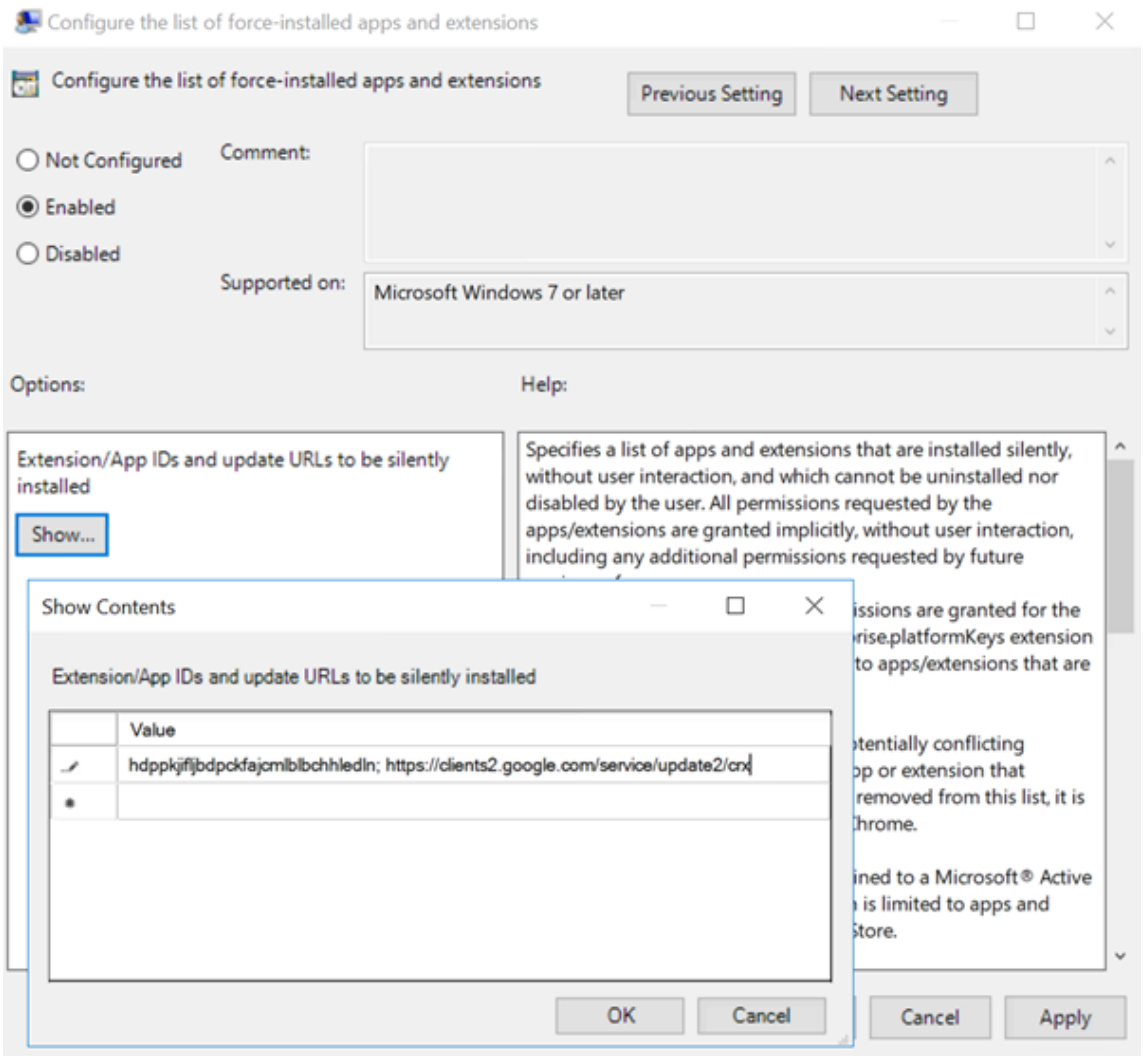
Déployer l'extension à l'aide d'une stratégie de groupe

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 tapez 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.

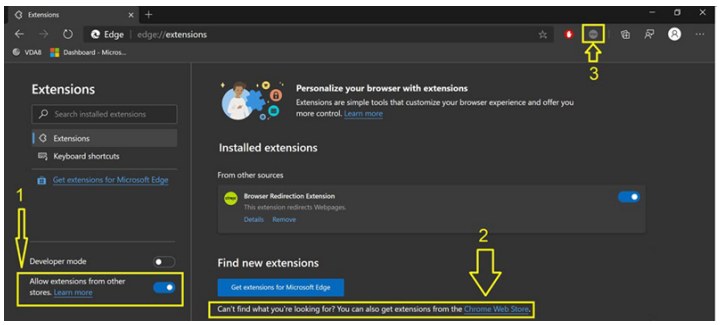
   Toutes les mises à jour de l'extension sont automatiquement installées sur les ordinateurs des utilisateurs via l'URL de mise à jour que vous avez spécifiée dans le paramètre.

   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** dans le menu et activez **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.

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 appareils 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.

Conférences vidéo et compression vidéo de webcam HDX

March 30, 2022

> **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 de webcam HDX

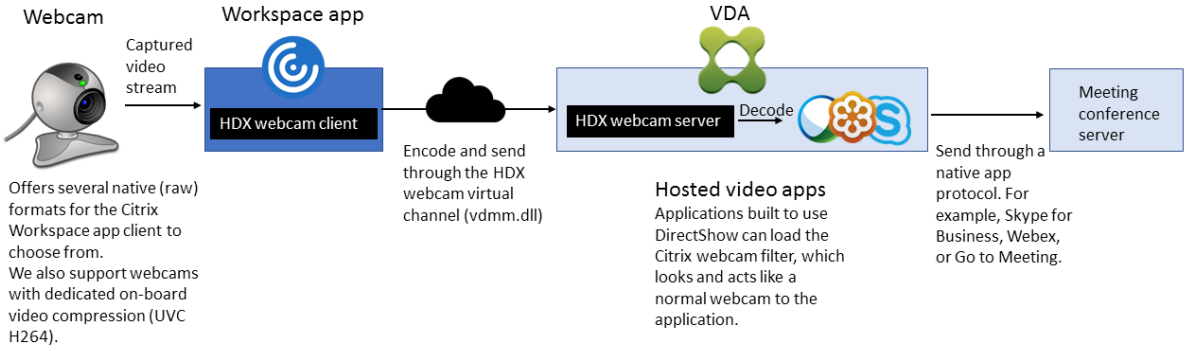
La compression vidéo de webcam HDX est également appelée mode webcam **optimisé**. Ce type de compression vidéo de webcam envoie la vidéo H.264 directement à l'application de visioconférence exécutée dans la session virtuelle. Pour optimiser les ressources VDA, la compression de webcam HDX n'effectue pas de codage, de transcodage ni de décodage de la vidéo webcam. Par défaut, cette fonction est activée.

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

- Conférences multimédia
- Redirection Windows Media

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.
Application Citrix Workspace pour Linux	L'application Citrix Workspace pour Linux prend en charge uniquement les applications 32 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 les résolutions de webcam jusqu'à 1920x1080.

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 de type de média échoue, HDX revient à la résolution par défaut de 352 x 288 CIF. 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 12, 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 appareils 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.com 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 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 Server 2016 RTM 14393 (1607) ; Windows Server 2012 R2
Chrome 51	Windows 10 x86 (1607 RS1) et x64 (1607 RS1) ; 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/XenDesktop Engineering; CN = Citrix XenApp/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/XenDesktop Engineering; CN = Citrix XenApp/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

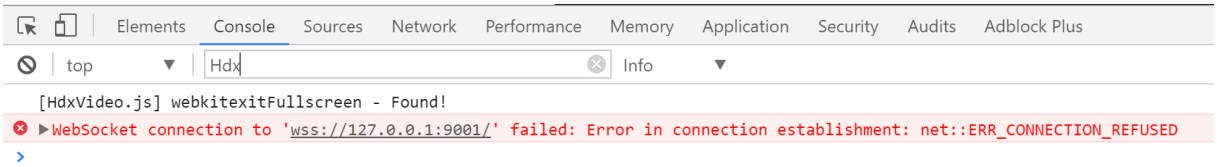
Dans cette version, cette fonctionnalité est disponible pour les pages Web contrôlées uniquement. Elle requiert l'ajout de JavaScript HdxVideo.js (fournie sur le support d'installation de Citrix Virtual Apps and Desktops) aux pages web sur lesquelles le contenu multimédia HTML5 est disponible. Par exemple, 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 12, 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).
>
> Si vous utilisez 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 blanche par défaut.
>
> Les applications publiées sont désormais prises en charge par la nouvelle version de Microsoft Teams.
>
> Si vous utilisez Citrix Virtual Apps and Desktops 2311 ou une version antérieure, un nouveau paramètre de configuration de registre est requis dans le VDA pour permettre à la nouvelle ver-

> sion de Microsoft Teams d'accéder au canal virtuel Citrix. Pour activer l'optimisation de Microsoft Teams 2.1, configurez la clé de registre suivante dans le VDA :
>
> **Emplacement** : `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
>
> **Clé** (REG_Multi_SZ) : `ProcessWhitelist`
>
> **Valeur** : `msedgewebview2.exe`
>
> Pour plus d'informations, consultez la documentation de Microsoft.

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).

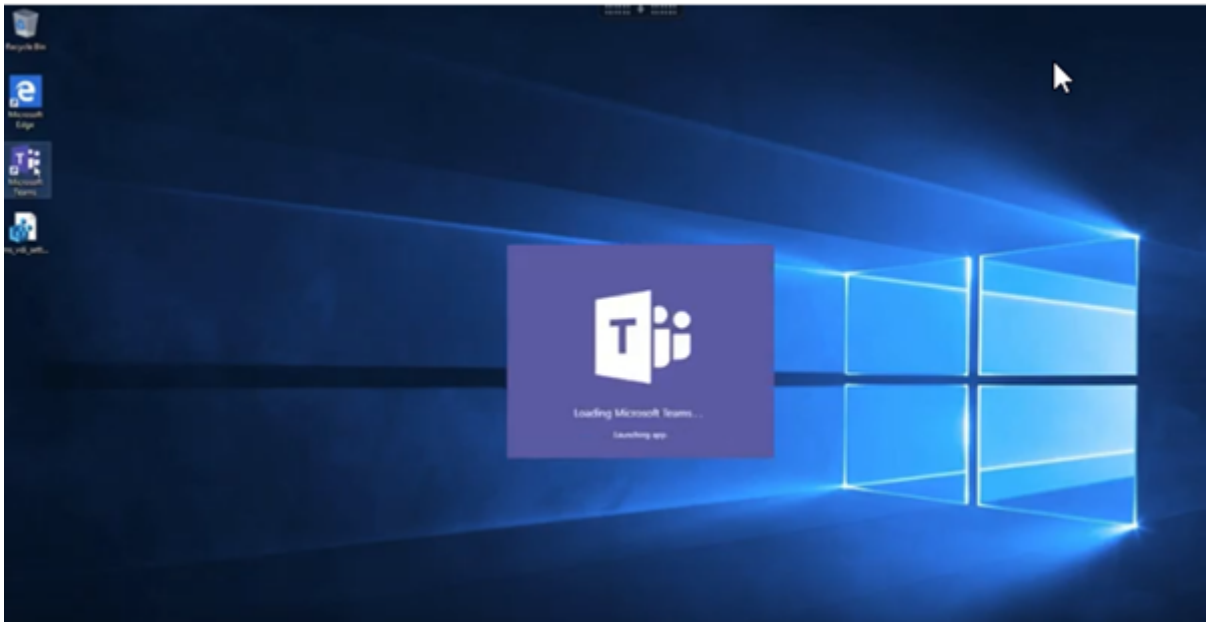
Notre optimisation pour Microsoft Teams inclut des services et une API HDX côté VDA afin de créer une interface avec l'application hébergée Microsoft Teams pour recevoir des commandes. Ces composants ouvrent un canal virtuel de contrôle (CTXMTOP) vers Media Engine côté application Citrix Workspace. Le 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 démo 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 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'environnements VDI permanents dédiés 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 :**
>
> Nous vous recommandons 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

Nous vous recommandons d'installer Microsoft Teams version 1.4.00.22472 ou supérieure, 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 du PC distant (HDX ou local). Cela est dû au fait que Microsoft Teams peut uniquement évaluer le mode VDI au moment du lancement de l'application,

> 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 nouvelle 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` (~600–700 Mo) 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 :

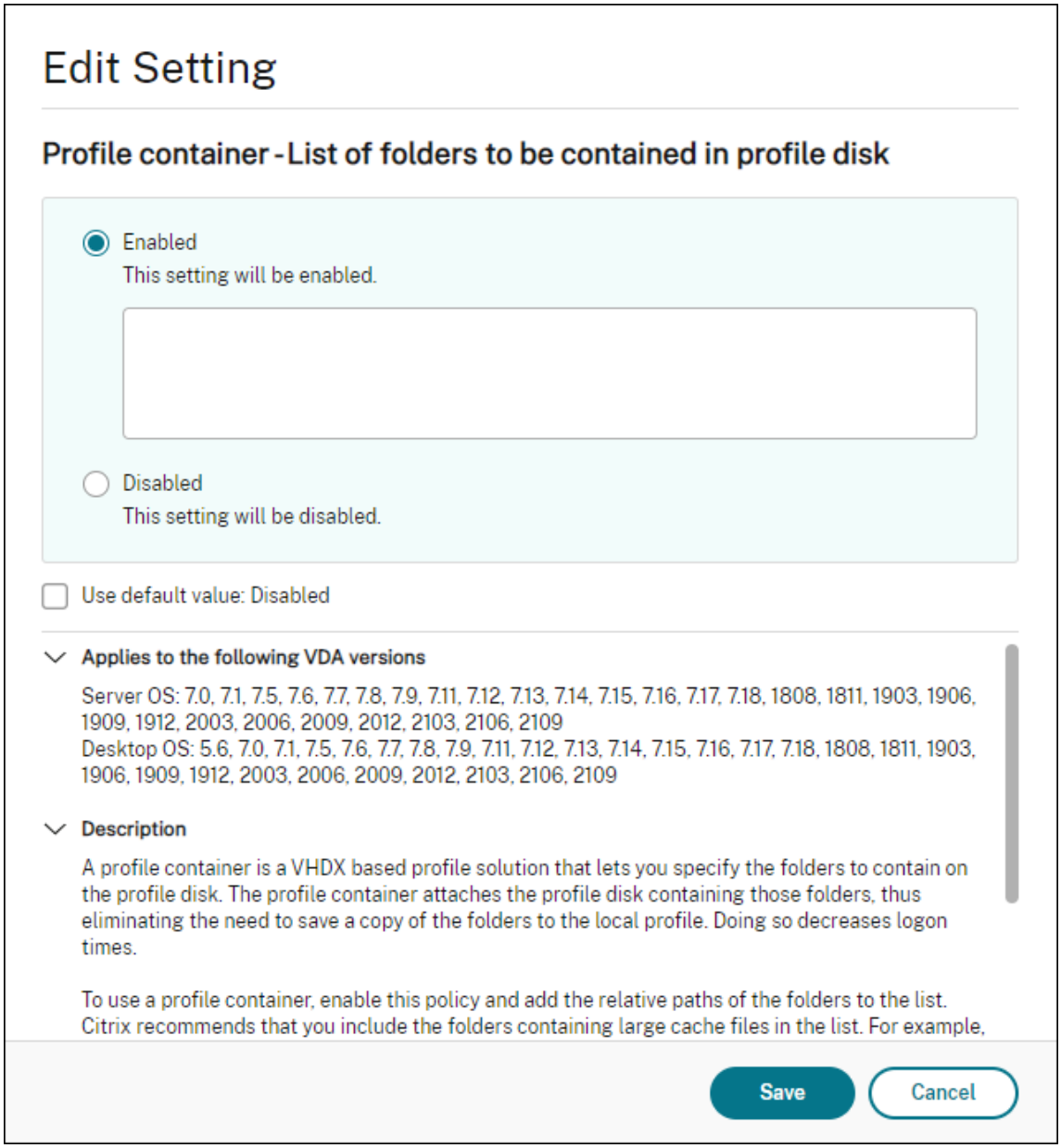
- C:\Users\<username>\AppData\Local\Microsoft\IdentityCache
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

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 de 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

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
- Distribution Linux x64

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 Chrome OS exécutée sur la dernière version de Chrome OS

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. Notez que 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 Chrome OS
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 Chrome OS
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 2112 ou version supérieure, les sous-titres instantanés ne fonctionneront 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.

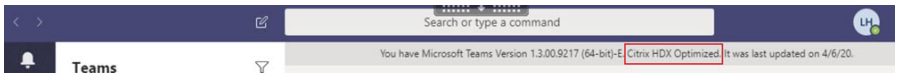
> **Remarque :**
>
> Toutes les fonctionnalités répertoriées dans l'**application Citrix Workspace pour Windows 1912 CU6 (ou version ultérieure)** s'appliquent à l'application Citrix Workspace pour Windows 2203.1 LTSR CU1.

Activer l'optimisation pour Microsoft Teams

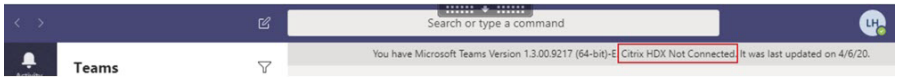
Pour activer l'optimisation pour Microsoft Teams, utilisez la stratégie de la console Gérer décrite dans Stratégie de redirection Microsoft Teams. Cette stratégie est **activée** par défaut. Outre l'activation de cette stratégie, HDX vérifie que la version de l'application Citrix Workspace est au moins 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.

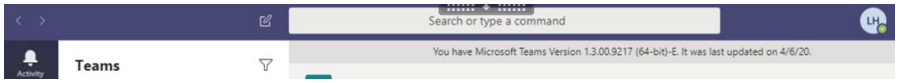
Si vous cliquez sur **About > Version**, la légende **Citrix HDX Optimized** affiche :



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. Pour obtenir des instructions détaillées concernant la planification du réseau, consultez les principes de connectivité réseau Microsoft 365.

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 varie en fonction 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
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 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 appareils 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 l'établissement de médias de conférence téléphonique 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, 52.120.0.0/14	**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.

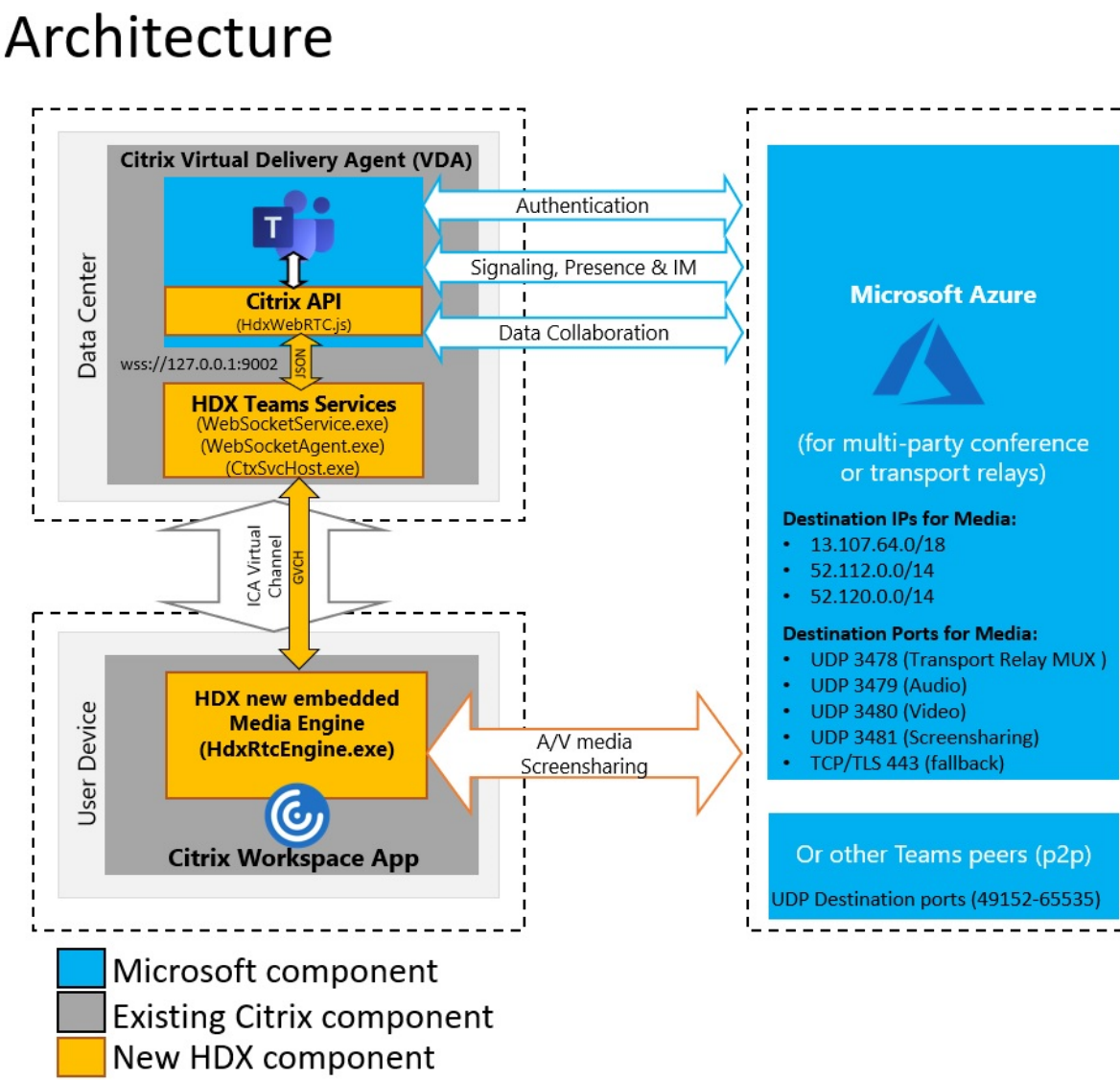
Le moteur multimédia WebRTC de l'application Workspace contacte le relais de transport Microsoft Teams le plus proche dans le cloud Microsoft 365. Le moteur multimédia utilise une adresse IP anycast et le port 3478—3481 UDP (différents ports UDP par charge de travail, bien qu'un multiplexage soit possible) 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 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 connectez 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 Chrome OS 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 Chrome OS 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

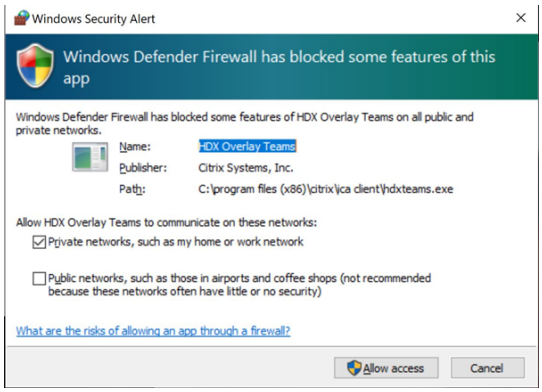
Pour plus d'informations sur les appels d'urgence dynamiques, consultez la documentation Microsoft.

Les informations d'emplacement que l'application Citrix Workspace transmet à Microsoft Teams sont les suivantes :

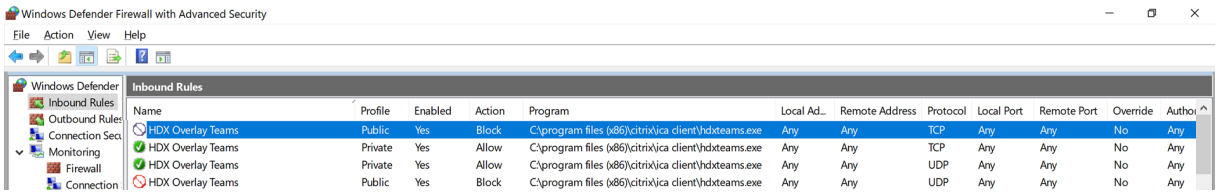
- ID de châssis/ID de port utilisant le protocole LLDP (Link Layer Discovery Protocol) pour les connexions Ethernet/Switch. Ethernet/Switch (LLDP) est pris en charge sur :
  - Versions Windows 8.1 et 10
  - macOS (exige un logiciel d'activation LLDP) Pour télécharger le logiciel d'activation LLDP, accédez 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.
  - 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 fin (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.

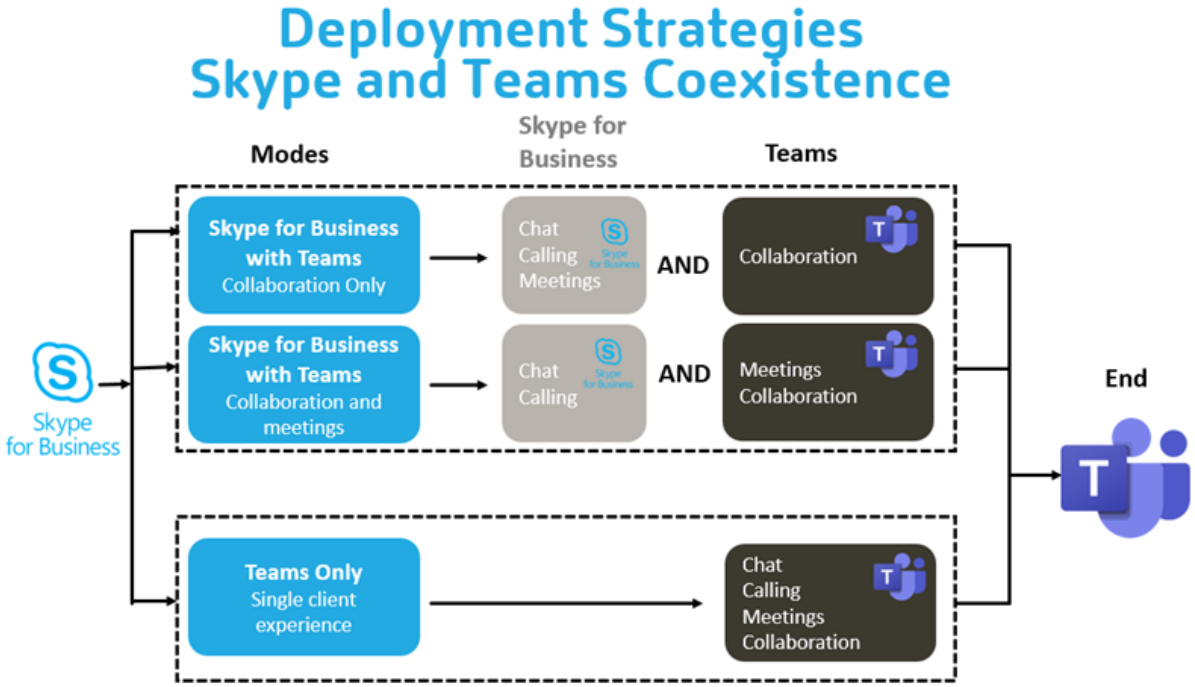


Coexistence Microsoft Teams/Skype Entreprise

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

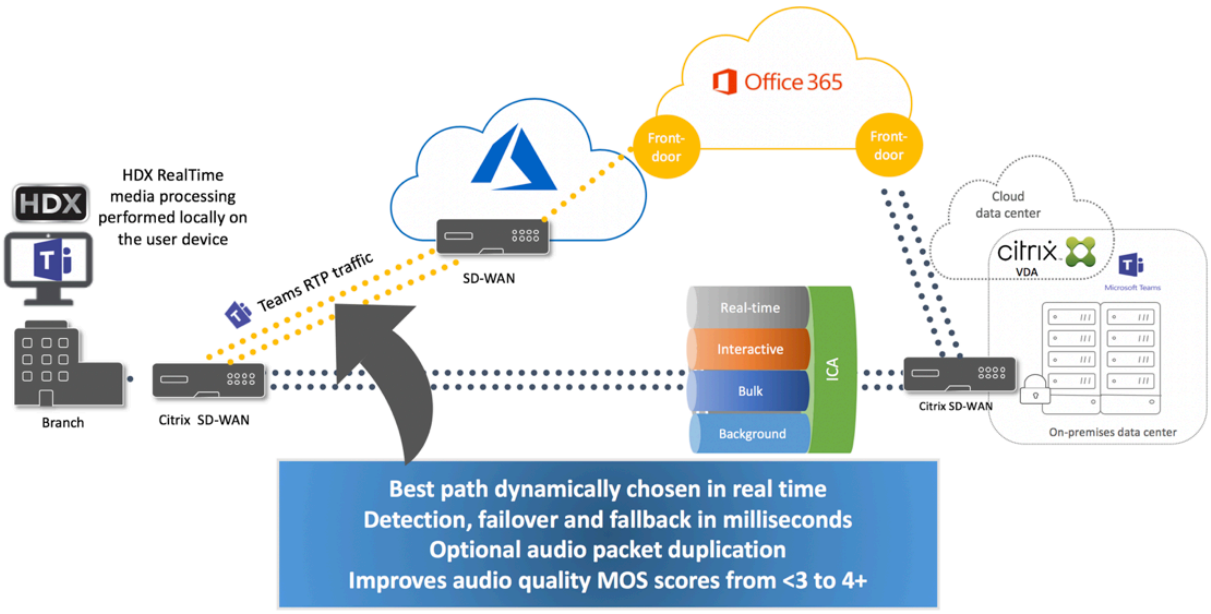
Une qualité audio et vidéo optimale nécessite une connexion réseau au cloud Microsoft 365 avec une faible latence, une faible gigue et une faible perte de paquets. Le rétroacheminement du trafic RTP audio-vidéo Microsoft Teams à partir des utilisateurs de l'application Citrix Workspace situés dans des 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 et VDA 2112.

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 2212
- 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 définie sur 1 rend l'arrière-plan flou. Cette valeur peut être définie soit par l'utilisateur final, soit par l'administrateur.

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"

 }

<!--NeedCopy-->
```

Sur HTML5 Pour HTML5, uniquement le flou d'arrière-plan est pris en charge. Le remplacement d'image personnalisé n'est pas pris en charge.

Pour le flou d'arrière-plan, procédez comme suit :

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

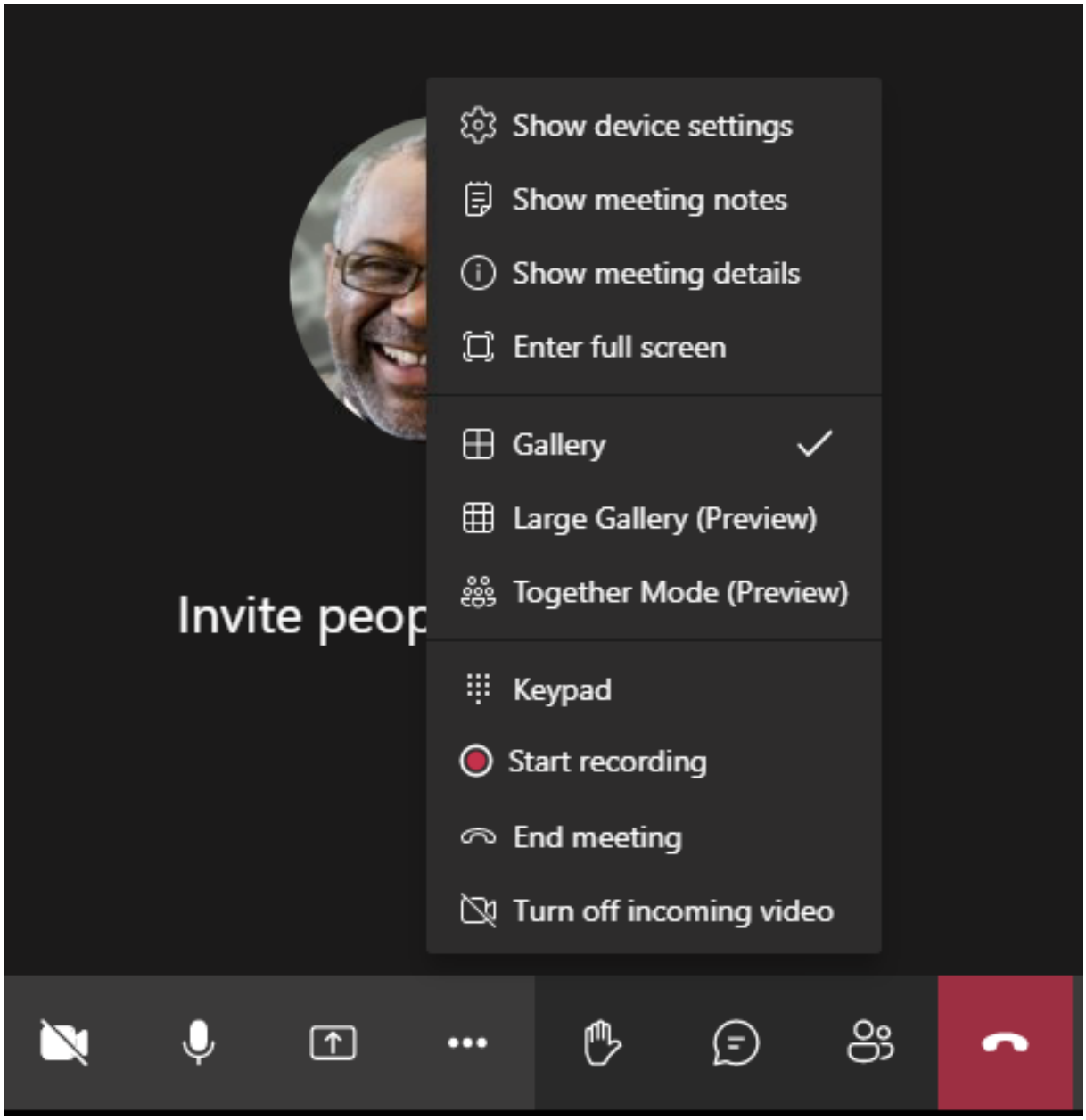
Microsoft Teams prend en charge les dispositions **Galerie**, **Grande galerie** et **Mode Ensemble**.

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 des vidéos, 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 la vidéo 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 (CWA pour Windows 2102, CWA pour Linux 2106, CWA pour MAC 2106 ou supérieur) :

- 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.

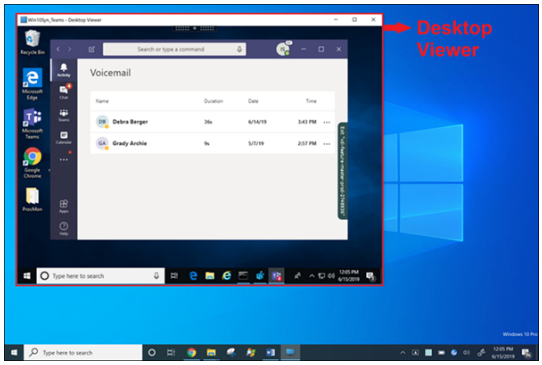
Moniteurs multiples

Lorsque Desktop Viewer (CDViewer.exe) est en mode plein écran et s'étend sur plusieurs moniteurs, l'application Citrix Workspace 2106 ou ultérieure (Windows/Linux/Mac) permet au sélecteur d'écran de sélectionner le moniteur à partager.

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 l'autre participant 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 (de 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.



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.

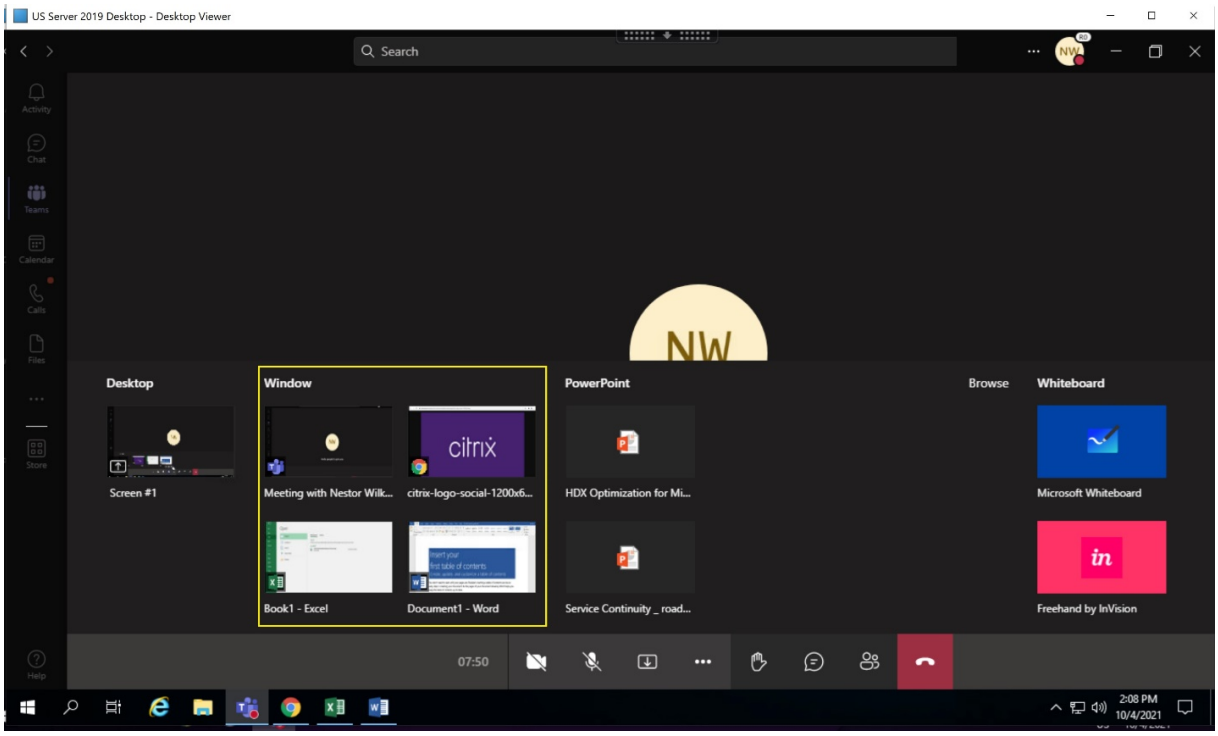
À partir de l'application Citrix Workspace pour Windows 2109, Mac 2203, Linux 2209 et VDA 2109, Microsoft Teams prend en charge le partage d'écran d'applications spécifiques exécutées dans la session virtuelle. Pour partager une application spécifique, procédez comme suit :

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 :**
>
> - 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.
> - 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 aux homologues ou au serveur 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.

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.

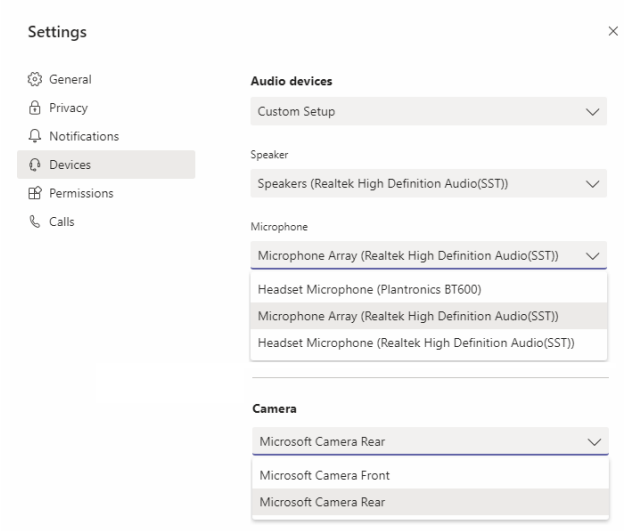
Pour prendre le contrôle lorsqu'un écran est partagé, cliquez sur le bouton **Demander le contrôle** dans l'interface utilisateur Microsoft Teams. Le participant à la réunion qui partage l'écran peut accepter ou refuser votre demande.

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 :**
>
> - La fonction Donner ou demander le contrôle n'est pas disponible 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.

- Caméras certifiées Microsoft Teams, bien que les périphériques certifiés Skype Entreprise soient compatibles avec Microsoft Teams.
- 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

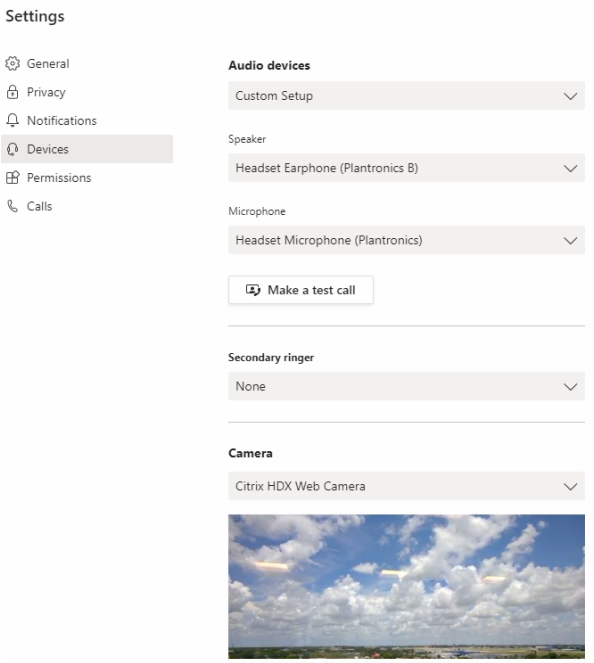
Si Microsoft Teams ne parvient pas à se charger en mode VDI optimisé ("Citrix HDX non connecté" dans Teams/À propos de/Version), le VDA revient aux technologies HDX héritées. Les technologies HDX héritées peuvent être la redirection de webcam et la redirection de l'audio et du microphone client. Si vous 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 de l'appel 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.
- La fonctionnalité complémentaire de protection des applications pour l'application Citrix Workspace empêche le partage d'écran sortant et bloque le partage d'écran et la vidéo entrants.
- 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 **Oui**, 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. Dépendance de Microsoft Teams : contactez Microsoft pour connaître la date de disponibilité de la résolution 1080p.
- 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 fonctionnalité multi-fenêtres sont disponibles dans l'article Tech Community : New Meeting and Calling Experience in Microsoft Teams.

Vous devez 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 terminaux pour prendre en charge le mode multi-fenêtres, vous ne pourrez établir que des appels audio. Vous ne pourrez pas utiliser les fonctionnalités optimisées de vidéo et de partage d'écran.

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	Version LTSR compatible	Version recommandée
Microsoft Teams	1.5.00.11865	Non applicable	Dernière version
VDA	1912 CU6 LTSR, 2203 LTSR, 2112 CR	1912 CU7+, 2203 CU2+	2308 CR+
Application Citrix Workspace pour Windows	2205 CR	2203 CU2+	2309 CR+
Application Citrix Workspace pour Mac	2209 CR	Non applicable	2308 CR+
Application Citrix Workspace pour Linux	2209 CR	Non applicable	2308 CR+
Application Citrix Workspace pour ChromeOS ou HTML5	2303 CR	Non applicable	2309 CR+

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

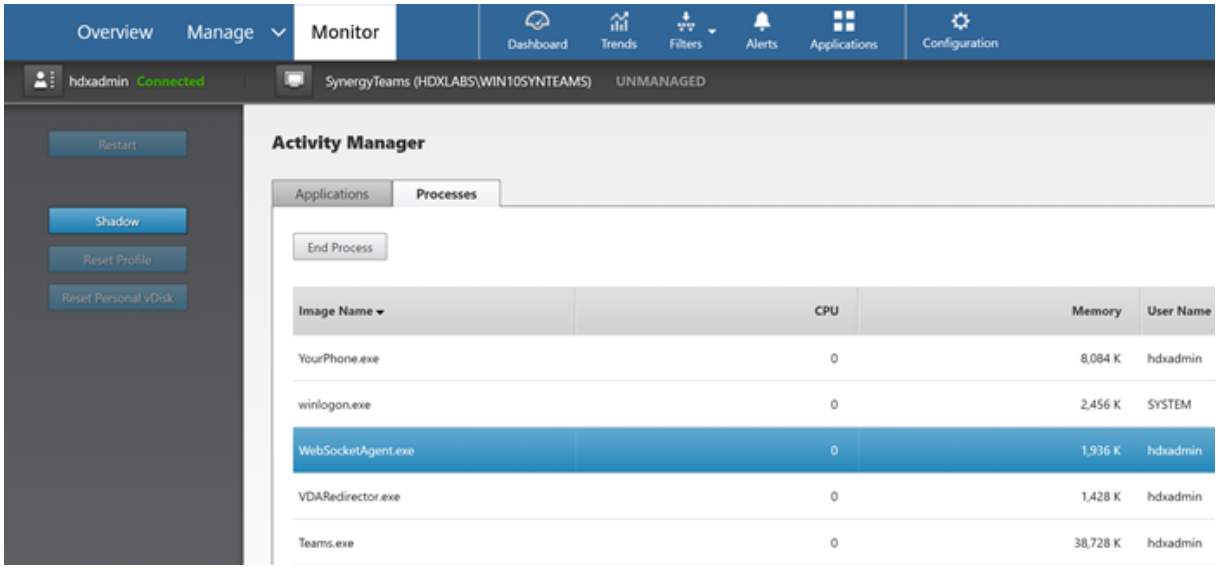
Surveiller, dépanner et prendre en charge Microsoft Teams

April 18, 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.



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`.

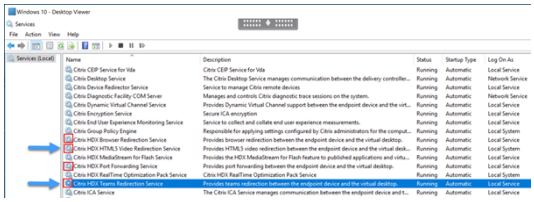
Pour plus d'informations, consultez la section *Surveillance* dans l'article CTX253754 du centre de connaissances.

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.

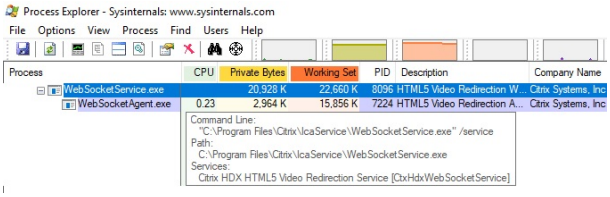


- **Citrix HDX Teams Redirection Service** établit le canal virtuel utilisé dans Microsoft Teams. Le service repose sur CtxSvcHost.exe.
- **Citrix HDX HTML5 Video Redirection Service** s'exécute en tant que WebSocketService.exe en écoute sur 127.0.0.1:9002 TCP. WebSocketService.exe exécute deux fonctions 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	Chemin d'accès au fichier exécutable dans le système d'exploitation Windows Server	Ouvrir une session en tant que	Description
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. 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 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 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 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 :

```
1  RPCStubs Info: -> device id = \?\display#int3470#4&1835d135&0&uid13424
       #{
2   65e8773d-8f56-11d0-a3b9-00a0c9223196 }
3   {
4   bf89b5a5-61f7-4127-a279-e187013d7caf }
5    label = Microsoft Camera Front groupId =
6
7  webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
8  webrtcapi.RTCPeerConnection Info: setLocalDescription.
9  >>> begin:sdp
10 [...]
11
12 webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
       HaveLocalOffer
13
14 webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
       Gathering
15
16 [...]
17 >>> begin:sdp
18 candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
       generation 0 ufrag oVk6 network-id 1
19 <<< 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-->
```

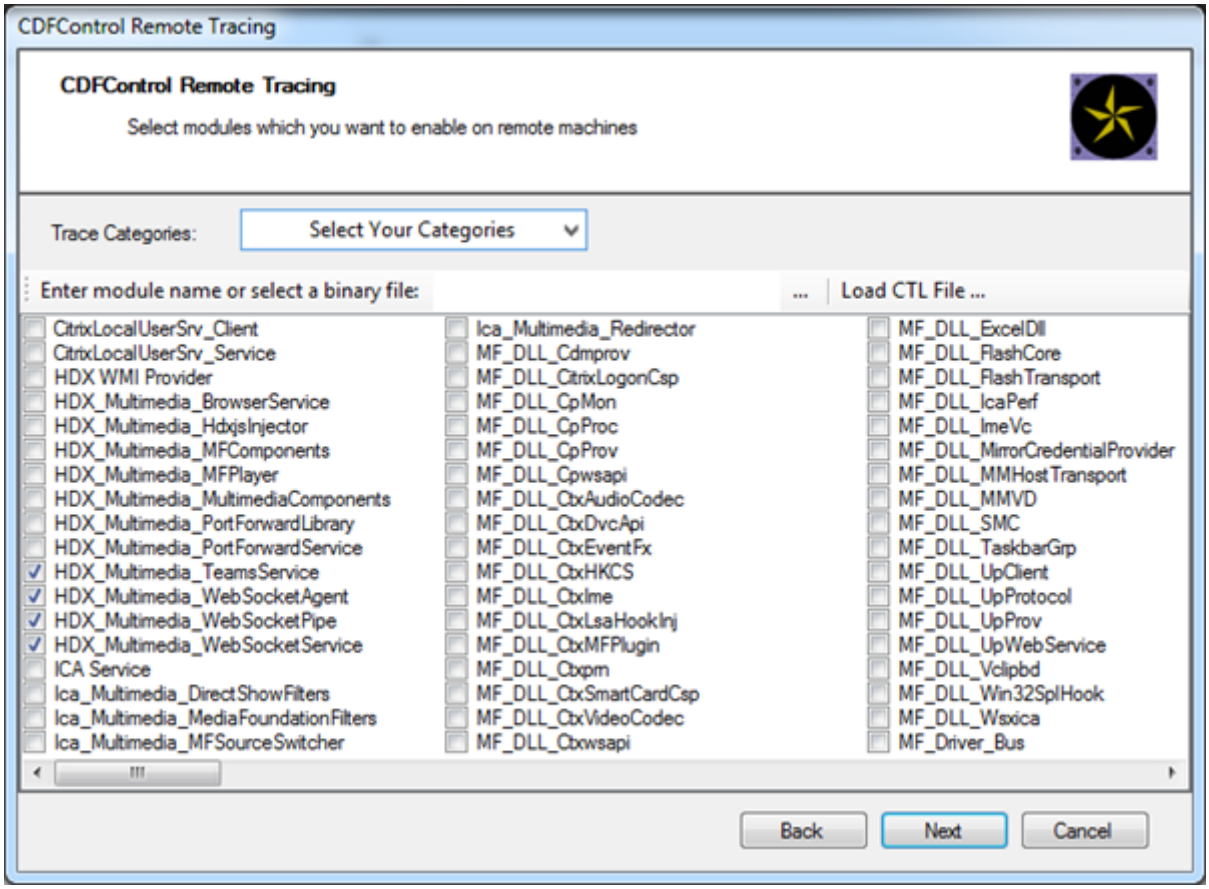
S'il y a plusieurs candidats ICE, l'ordre de préférence est :

1. hôte
2. réflexion homologue
3. réflexion serveur
4. relais de transport

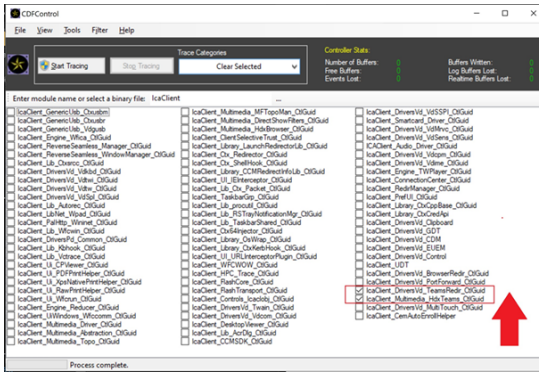
Si vous rencontrez un problème et que vous pouvez le reproduire, nous vous recommandons de cliquer sur **Aide > Signaler un problème** dans Teams. Les journaux sont partagés entre Citrix et Microsoft pour résoudre les problèmes techniques si vous avez ouvert un dossier avec Microsoft.
La capture de traces 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

April 27, 2022

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

April 27, 2022

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

March 30, 2022

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 dés-

activez 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 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.

Configuration de redirection bidirectionnelle du contenu

February 13, 2024

La redirection bidirectionnelle du contenu permet de rediriger les URL du client vers le serveur ou du serveur vers le client, selon les configurations. Ce paramètre de stratégie remplace les trois paramètres suivants, qui ne sont plus pris en charge :

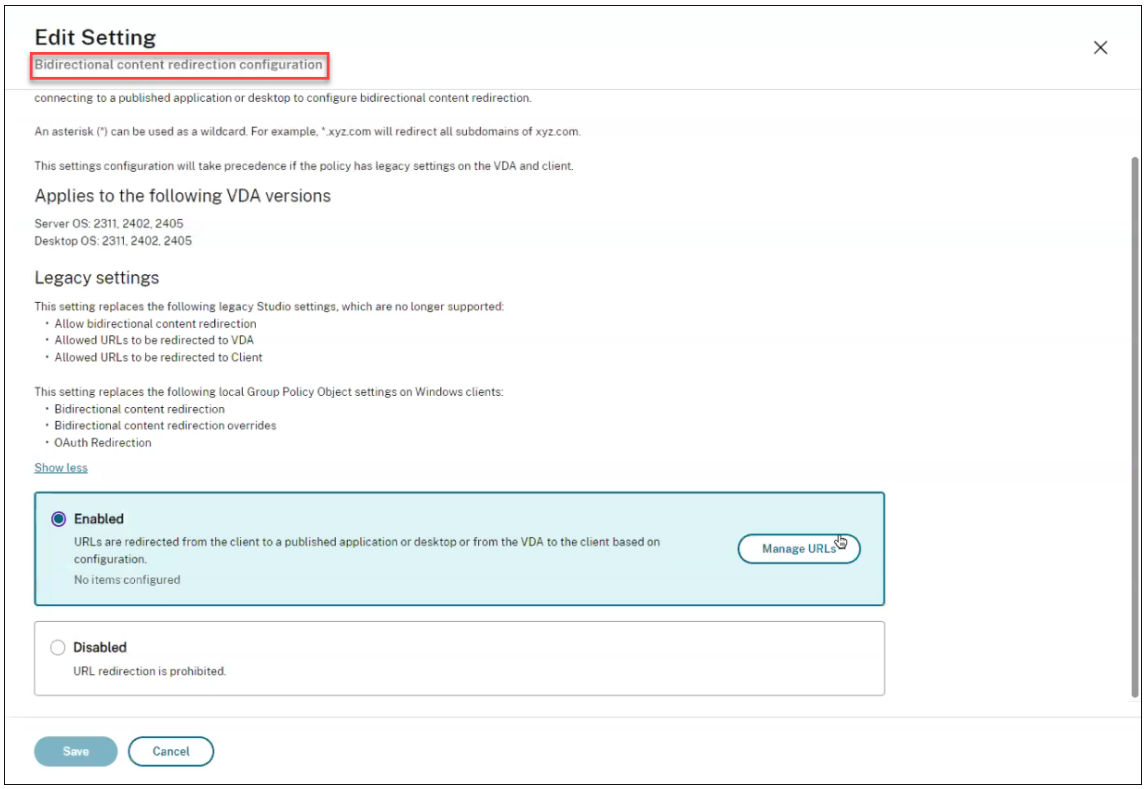
- Autoriser la redirection bidirectionnelle du contenu
- URL autorisées à être redirigées sur le VDA
- URL autorisées à être redirigées sur le client

Il remplace également les trois paramètres d'objets de stratégie de groupe locaux suivants sur les clients Windows :

- Redirection bidirectionnelle du contenu
- Remplacements de la redirection bidirectionnelle du contenu
- Redirection OAuth

Si ce paramètre est configuré, il a priorité sur les anciens paramètres dans Studio et sur le client. Pour configurer la stratégie de redirection bidirectionnelle du contenu, procédez comme suit :

1. Sur la page de configuration de Citrix DaaS, cliquez sur l'onglet **Gérer**.
2. Cliquez sur l'onglet **Stratégies**.
3. Cliquez sur **Créer une stratégie**. La lame **Créer une stratégie** s'ouvre.
4. Recherchez `Bidirectional content redirection configuration` dans le champ **Rechercher**, cochez la case et cliquez sur **Modifier**.
5. Dans la lame **Modifier les paramètres**, définissez cette stratégie sur **Activé** et cliquez sur**Gérer les URL**.



6. Dans la lame **Gérer les URL**, pour la **redirection du VDA vers le client**, spécifiez les éléments suivants :

    - **URL** (obligatoire) : ajoutez l'URL qui doit déclencher la redirection depuis le VDA pour l'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'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 précisé, l'URL de fin devrait être au format : `scheme://<something>`. Si aucun schéma n'est spécifié (vide), 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 également indiquer le **schéma**.

7. Dans la lame **Gérer les URL**, pour la **redirection du client vers le VDA**, spécifiez les éléments suivants :

    - **Type** : choisissez **Bureau** ou **Application**.
    - **Nom** :donnez un nom au type.
    - **URL** : indiquez l'URL que vous souhaitez rediriger vers la source. Vous pouvez ajouter plusieurs URL et supprimer celles qui ne sont pas obligatoires

8. Cliquez sur **Enregistrer**. La lame **Modifier les paramètres** affiche le nombre d'éléments configurés.
9. Cliquez sur **Enregistrer**. La lame **Créer une stratégie** indique la **valeur actuelle** configurée. Cliquez sur **Suivant**.
10. À l'étape **Attribuer la stratégie à**, cliquez sur **Suivant**.
11. À l'étape **Résumé**, cochez la case **Activer la stratégie** et saisissez un nom dans le champ **Nom de la stratégie**.
12. Cliquez sur **Terminer**. La nouvelle stratégie est répertoriée.

13. Sélectionnez la nouvelle stratégie créée pour passer en revue les paramètres configurés.

Pour les paramètres existants, consultez les sections Redirection de l'hôte vers le client et Redirection bidirectionnelle du contenu.

Redirection de l'hôte vers le client

February 13, 2024

> **Remarque :**
>
> Cet article décrit les anciens paramètres de redirection de l'hôte vers le client. Pour les derniers paramètres, consultez la section Configuration de la redirection bidirectionnelle du contenu. Les nouveaux paramètres de stratégie auront priorité sur les anciens paramètres. Citrix recommande d'utiliser uniquement les nouveaux paramètres de stratégie et de supprimer tous les paramètres existants pour éviter tout comportement inattendu.

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 de l'hôte vers le 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" />

</DefaultAssociations>
<!--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 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 des 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 complets 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.

Redirection bidirectionnelle du contenu

April 18, 2024

> **Remarque :**
>
> Cet article décrit les anciens paramètres de redirection bidirectionnelle de contenu. Pour connaître les derniers paramètres de stratégie, consultez la section Configuration de la redirection bidirectionnelle de contenu. Les nouveaux paramètres de stratégie auront priorité sur les anciens paramètres. Citrix recommande d'utiliser uniquement les nouveaux paramètres de stratégie et de supprimer tous les paramètres existants pour éviter tout comportement inattendu.

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

La redirection bidirectionnelle du contenu doit être activée à l'aide de la stratégie Citrix sur le VDA et le client pour que la redirection fonctionne. 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 la configuration du client, reportez-vous à la section Redirection bidirectionnelle du contenu dans la documentation de l'application Citrix Workspace pour Windows.

Les extensions de navigateur doivent être enregistrées à l'aide des commandes affichées. Exécutez les commandes selon vos besoins sur le VDA et le client en fonction du navigateur utilisé.

Pour enregistrer les extensions de navigateur sur le VDA, ouvrez une invite de commande. Ensuite, exécutez `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` avec l'option de navigateur requise, comme indiqué dans les exemples illustrés :

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

Pour enregistrer l'extension sur tous les navigateurs disponibles, exécutez :

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

Pour annuler l'enregistrement d'une extension de navigateur, utilisez l'option `/unreg<browser>` comme dans l'exemple illustré :

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

Pour enregistrer les extensions de navigateur sur le client, ouvrez une invite de commande et exécutez `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` avec les mêmes options que dans les exemples illustrés.

> **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.

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.

Dans Citrix Studio, définissez l'URL générique dans **URL autorisées à être redirigées sur le client**. L'astérisque (*) est le caractère générique.

> **REMARQUE :**
>
> - Ne définissez pas **URL autorisées à être redirigées sur le VDA** dans la stratégie client. Assurez-vous que les sites définissent **URL autorisées à être redirigées sur le VDA** afin d'éviter les boucles de redirection infinies.
> - Les domaines de premier niveau ne sont pas gérés. Par exemple, `https://www.citrix.*` et `http://www.citrix.co*` ne sont pas redirigés.

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 Citrix Studio, définissez le protocole personnalisé dans **URL autorisées à être redirigées sur le client**.

> **REMARQUE :**
>
> - 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. L'utilisation du même type de navigateur sur le VDA et le client n'est PAS requise.
- 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.
- Seules les URL du protocole HTTP/HTTPS sont prises en charge. Les raccourcis d'URL ne sont pas pris en charge.

- La redirection client vers VDA nécessite que le client Windows soit installé 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.

Local App Access et redirection d'adresse URL

June 15, 2022

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.

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. Dans **Gérer > Configuration complète**, sélectionnez **Stratégies** dans le volet gauche.
2. Sélectionnez **Créer une stratégie** dans la barre d'actions.
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. Pour plus d'informations, consultez Mise en route et recherchez *Modèle d'administration d'objet de stratégie de groupe*.
> - 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`/`CitrixBse.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 Citrix DaaS, utilisez le kit SDK PowerShell à distance Citrix Virtual Apps and Desktops. Pour plus d'informations, consultez Kit de développement logiciel distant SDK Citrix Virtual Apps and Desktops Remote PowerShell.

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. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet 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. Vous pouvez également cliquer sur **Ajouter l'application Local App Access** dans le volet Actions. Pour afficher l'option Ajouter l'application Local App Access dans le volet 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 sera 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

April 18, 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.
> - Lors de la négociation de session à l'aide du logiciel Citrix vers une machine virtuelle Azure, Citrix fournit la meilleure assistance possible pour la redirection USB vers la machine

> virtuelle Azure. Nous aidons à la résolution d'un problème logiciel Citrix, mais nous ne proposons pas d'assistance pour la machine virtuelle Azure sous-jacente.
> - Les périphériques CD/DVD dotés de capacités de gravure de disques peuvent être redirigés, mais les capacités de gravure de ces appareils ne peuvent pas être utilisées. Cela est dû aux limites de tampon d'une session.

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 :

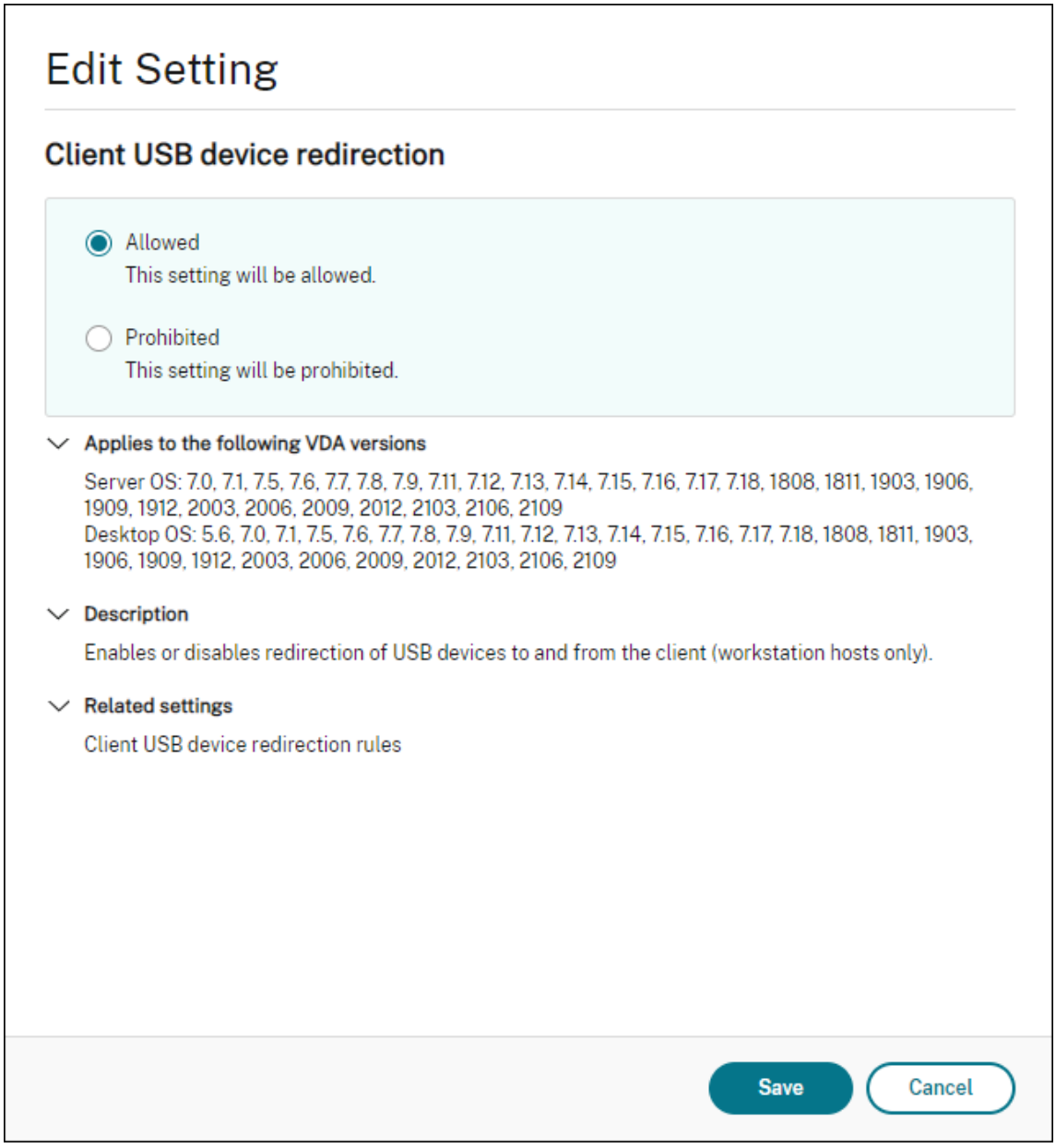
- Si deux organisations ou services distincts sont responsables de l'application Citrix Workspace et du VDA, elles peuvent appliquer le contrôle séparément. Cette configuration s'applique lorsqu'un utilisateur d'une organisation accède à une application située dans une autre organisation.
- Les paramètres 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**.

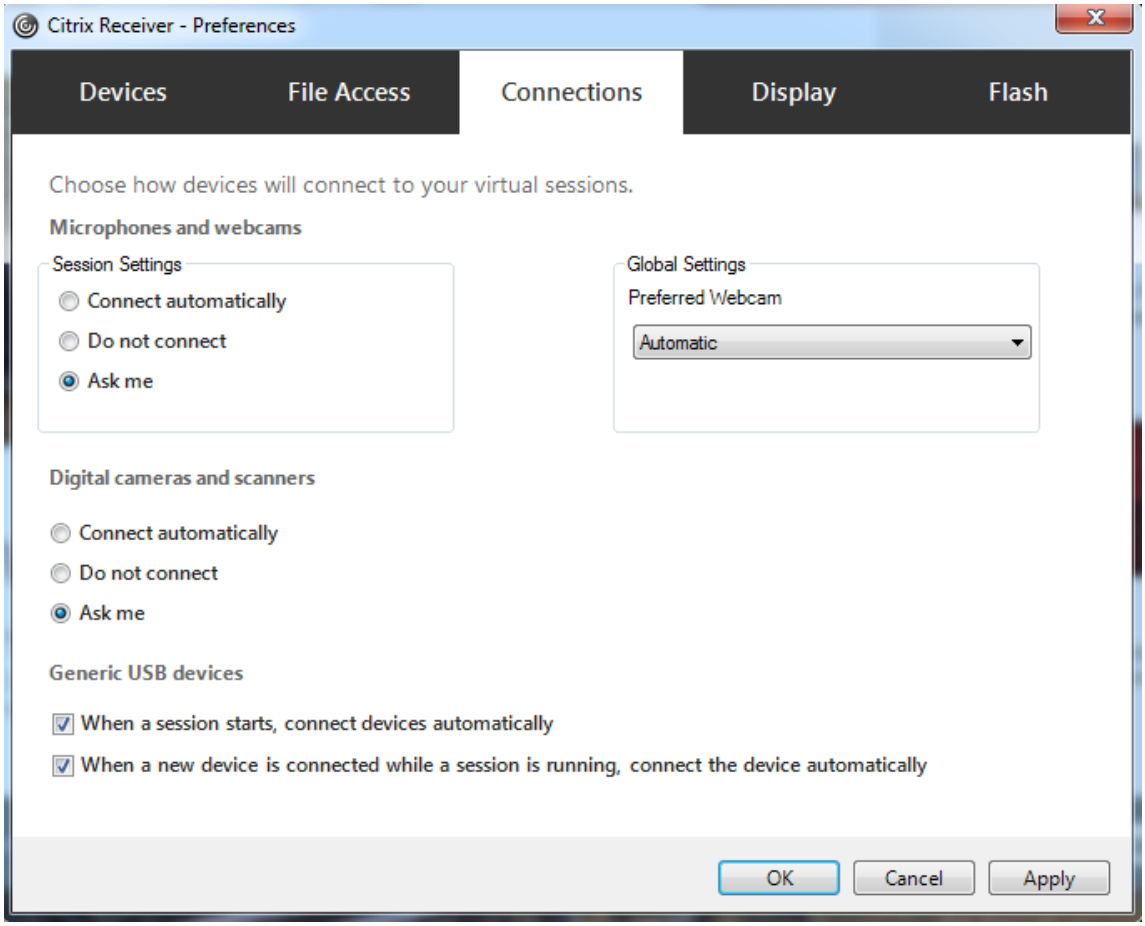


2. (Facultatif). Pour mettre à jour la liste des périphériques USB disponibles pour la redirection, ajoutez le paramètre Règles de redirection de périphérique USB client à une stratégie et spéci-

fiez les règles de stratégie USB.

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.

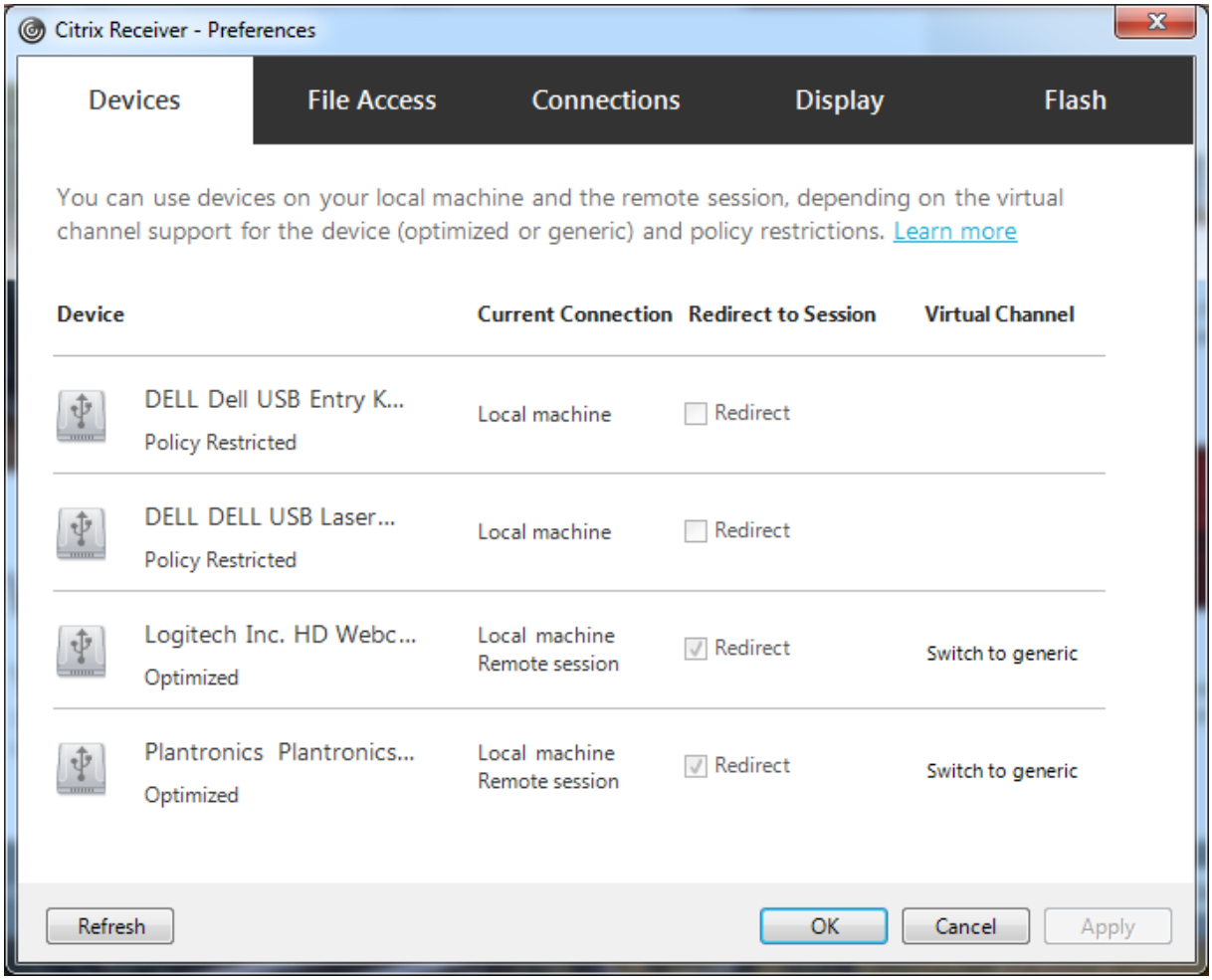
pour les clients légers, consultez le fabricant pour obtenir des détails sur la prise en charge USB et sur la configuration requise.

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 pour l'application Citrix Workspace et le VDA qui remplaceront les règles de stratégie USB par défaut.

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 :
  - Pour x64 : dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - Pour x86 : dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

Sur 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 HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. 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 HKLM\SOFTWARE\Policies\Citrix\PortICA\Gene
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 :**
>
> 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

Gérer

April 27, 2022

Citrix gère les déploiements du service Citrix Virtual Apps and Desktops en installant et en gérant les fonctionnalités et composants principaux dans Citrix Cloud.

Vous vous chargez des machines (VDA) dans les emplacements de ressources qui mettent à disposition des applications et des postes de travail. Vous gérez également les connexions à ces emplacements de ressources, ainsi qu'aux applications, postes de travail et utilisateurs.

- **Autoscale :** solution cohérente et hautes performances pour gérer de manière proactive vos machines.
- **Applications :** permet de gérer les applications dans les groupes de mise à disposition.
- **Adresses IP virtuelles et bouclage virtuel :** la fonctionnalité d'adresse IP virtuelle Microsoft fournit une application publiée avec une adresse IP unique attribuée dynamiquement à chaque session. Avec le bouclage virtuel Citrix, vous pouvez également configurer des applications qui dépendent des communications avec localhost (127.0.0.1 par défaut) pour utiliser une adresse de bouclage virtuel unique dans la plage localhost (127.*).
- **Enregistrement de VDA :** avant qu'un VDA ne puisse mettre à disposition des applications et des postes de travail, il doit s'enregistrer (établir la communication) auprès d'un Cloud Connector. Vous pouvez spécifier les adresses de Cloud Connector à l'aide de plusieurs méthodes, qui sont décrites dans cet article. Les VDA doivent disposer d'informations récentes lorsque vous ajoutez des Cloud Connector.
- **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.
- **Utilisation de la recherche :** pour afficher des informations sur les machines, sessions, catalogues de machines, applications ou groupes de mise à disposition dans l'interface de gestion Configuration complète, utilisez la fonctionnalité de recherche flexible.
- **Prise en charge 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.
- **Profile Management :** Citrix Profile Management peut être installé lorsque vous installez un VDA. Si vous utilisez cette solution de gestion des profils utilisateur, consultez la documentation l'accompagnant.

- **Citrix Insight Services :** Citrix Insight Services (CIS) est une plate-forme Citrix depuis laquelle vous pouvez générer des informations d'instrumentation, de télémétrie et d'autres données stratégiques. Des informations analytiques et de diagnostic sont collectées lorsque vous installez un VDA.
- **Cache d'hôte local :** la fonctionnalité de cache d'hôte local permet de poursuivre les opérations de négociation de connexion lorsqu'un Cloud Connector dans un emplacement de ressources ne peut pas communiquer avec Citrix Cloud. L'échelle, la taille et d'autres considérations de configuration sont également fournies.
- **Administration déléguée :** l'administration déléguée de Citrix Cloud vous permet de configurer les autorisations d'accès requises par tous vos administrateurs conformément à leur rôle dans votre organisation.
- **Journalisation de la configuration :** la journalisation de la configuration suit les modifications de configuration et les activités administratives.
- **Journaux d'événements :** les services dans Citrix Virtual Apps and Desktops consignent les événements qui se produisent. Les journaux d'événements peuvent être utilisés pour les opérations de surveillance et de dépannage.
- **Licences :** vous pouvez afficher les informations d'utilisation des licences Citrix pour ce service à partir de la console Citrix Cloud.
- **Équilibrer la charge des machines :** vous pouvez contrôler comment équilibrer la charge des machines.

Accès adaptatif

June 30, 2022

Dans les situations en constante évolution d'aujourd'hui, la sécurité des applications est vitale pour toutes les entreprises. Prendre des décisions de sécurité basées sur le contexte avant d'autoriser l'accès aux applications réduit les risques associés tout en permettant l'accès aux utilisateurs.

La fonction d'accès adaptatif offre une approche d'accès zéro confiance complète qui fournit un accès sécurisé aux applications. L'accès adaptatif permet aux administrateurs de fournir un accès granulaire aux applications auxquelles les utilisateurs peuvent accéder en fonction du contexte. Le terme « contexte » fait référence à :

- Utilisateurs et groupes (utilisateurs et groupes d'utilisateurs)
- Appareils (ordinateurs de bureau ou appareils mobiles)
- Localisation (géolocalisation ou emplacement réseau)

- Posture de l'appareil (vérification de la posture de l'appareil)
- Risque (indice de risque utilisateur)

Posture de l'appareil

February 21, 2024

Le service Posture de l'appareil Citrix est une solution basée sur le cloud qui aide les administrateurs à faire respecter certaines exigences auxquelles les appareils finaux doivent satisfaire pour accéder aux ressources Citrix DaaS (Citrix Virtual Apps
and Desktops) ou Citrix Secure Private Access (applications SaaS et Web ou applications TCP et UDP). Pour mettre en œuvre un accès basé sur le zéro confiance, il est essentiel d'établir la confiance de l'appareil en vérifiant sa posture. Le service Posture de l'appareil applique les principes de confiance zéro sur votre réseau en vérifiant la conformité des appareils finaux (gestion, BYOD et posture de sécurité) avant d'autoriser un utilisateur final à se connecter.

Pour plus de détails, consultez la section Posture de l'appareil.

Service d'authentification adaptative

March 30, 2024

Les clients Citrix Cloud peuvent utiliser Citrix Workspace pour fournir une authentification adaptative à Citrix DaaS. Authentification adaptative est un service Citrix Cloud qui permet une authentification avancée pour les clients et les utilisateurs qui se connectent à Citrix Workspace. Le service Authentification adaptative est un ADC géré par Citrix et hébergé sur Citrix Cloud qui fournit toutes les fonctionnalités d'authentification avancées, telles que les suivantes :

- Authentification multifacteur utilisant différentes méthodes d'authentification telles que AD, RADIUS, certificat, plusieurs IdP tiers utilisant SAML 2.0, OAuth, OIDC, Google Captcha.
- Vérification de l'identité des utilisateurs et des niveaux d'autorisation en fonction de facteurs tels que l'emplacement, l'état de l'appareil et le groupe d'utilisateurs.
- Accès contextuel ou intelligent à DaaS (virtualisé) et aux SPA (ressources non virtualisées telles que des applications Web et SaaS).
- Personnalisation de la page

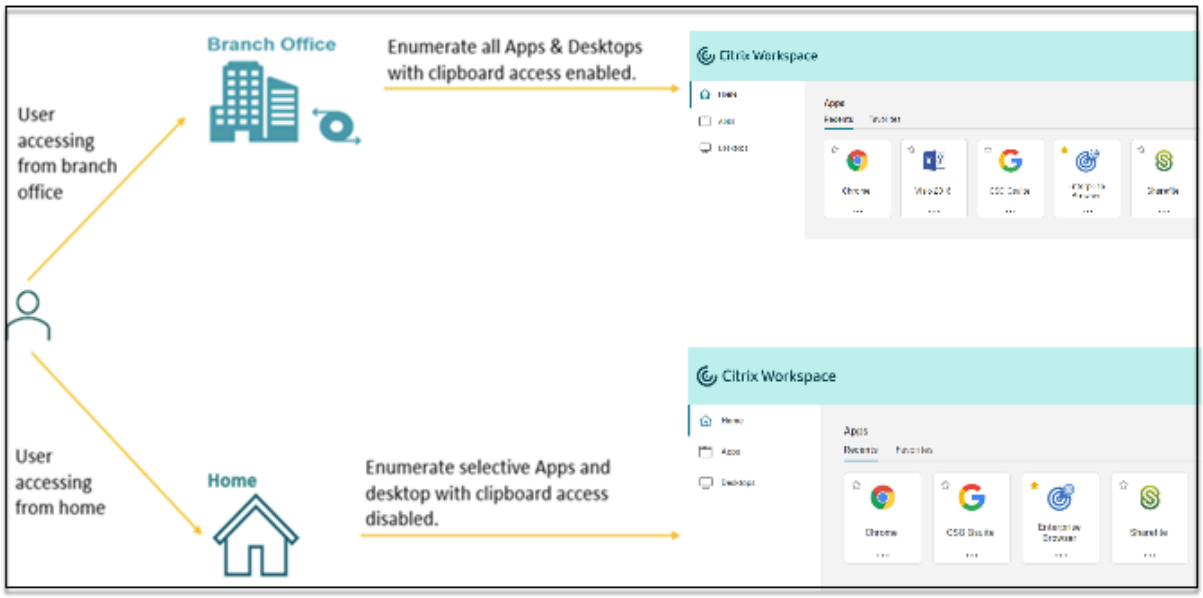
Pour plus de détails sur l'authentification adaptative, voir Service d'authentification adaptative.

Accès adaptatif basé sur l'emplacement réseau des utilisateurs

June 12, 2024

La fonctionnalité d'accès adaptatif de Citrix Workspace utilise une infrastructure de stratégie avancée pour permettre l'accès à Citrix DaaS en fonction de l'emplacement réseau des utilisateurs. L'emplacement est défini à l'aide de la plage d'adresses IP ou des adresses de sous-réseau.

Les administrateurs peuvent définir des stratégies pour énumérer ou non les applications et les bureaux virtuels en fonction de l'emplacement réseau des utilisateurs. Les administrateurs peuvent également contrôler les actions des utilisateurs en activant ou désactivant l'accès au presse-papiers, les imprimantes, le mappage des lecteurs clients, etc., en fonction de l'emplacement réseau des utilisateurs. Par exemple, les administrateurs peuvent définir des stratégies de sorte que les utilisateurs accédant aux ressources depuis leur domicile ont un accès limité aux applications et les utilisateurs accédant aux ressources depuis les succursales disposent d'un accès complet.



Un administrateur peut mettre en œuvre les stratégies suivantes pour l'accès aux applications :

- Énumérer certaines applications sensibles uniquement à partir du site de l'entreprise ou de ses succursales.
- Ne pas énumérer les applications sensibles si les employés accèdent à l'espace de travail à partir d'un réseau externe.
- Désactiver l'accès à une imprimante depuis les succursales.
- Désactiver l'accès au presse-papiers et à une imprimante lorsque les utilisateurs se trouvent en dehors du réseau d'entreprise.

Droits

La fonctionnalité Accès adaptatif est disponible pour les clients possédant les licences suivantes.

- DaaS Premium/Premium Plus
- Secure Private Access Advanced

Logiciels requis

- Assurez-vous que la fonctionnalité **Accès adaptatif** est activée (**Citrix Workspace > Accès > Accès adaptatif**). Pour plus de détails, voir Activer la fonctionnalité Accès adaptatif.

  Lorsque l'accès adaptatif est activé, les stratégies d'accès DaaS sont mises à jour pour utiliser l'option **Connexions transitant par Citrix Gateway**.

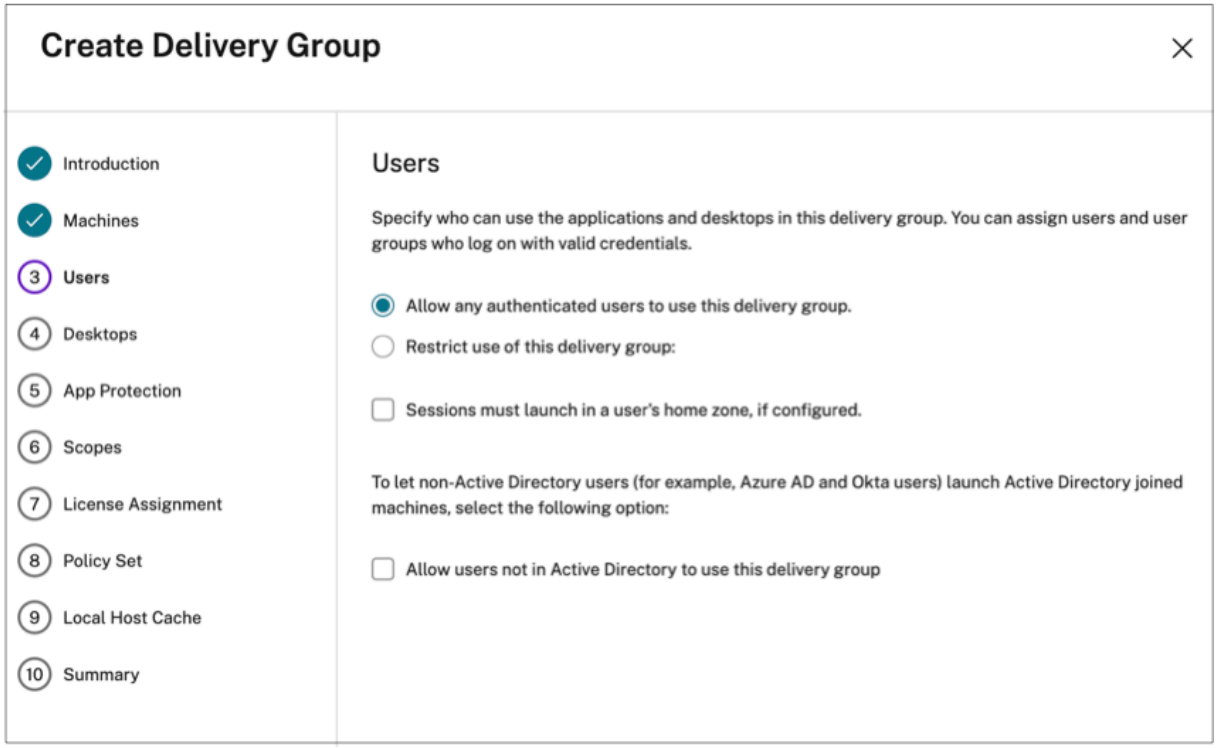
  > **Remarque :**
  >
  > NetScaler Gateway est nécessaire pour ajouter des balises d'accès intelligentes dans les stratégies d'accès DaaS. Toutefois, étant donné que DaaS utilise des balises provenant des services Posture de l'appareil, Accès adaptatif et Authentification adaptative, il n'est pas nécessaire de configurer NetScaler Gateway.

- Comprendre les balises d'emplacement. Pour plus de détails, consultez la section Balises d'emplacement réseau.

Points à noter

Les points suivants ne s'appliquent que si vous souhaitez restreindre l'énumération des applications en fonction de l'emplacement. Si vous prévoyez d'utiliser l'accès adaptatif pour restreindre les contrôles utilisateur tels que la désactivation de l'accès au presse-papiers, la redirection de l'imprimante, le mappage des lecteurs clients, en fonction de l'emplacement réseau, vous pouvez ignorer ces consignes.

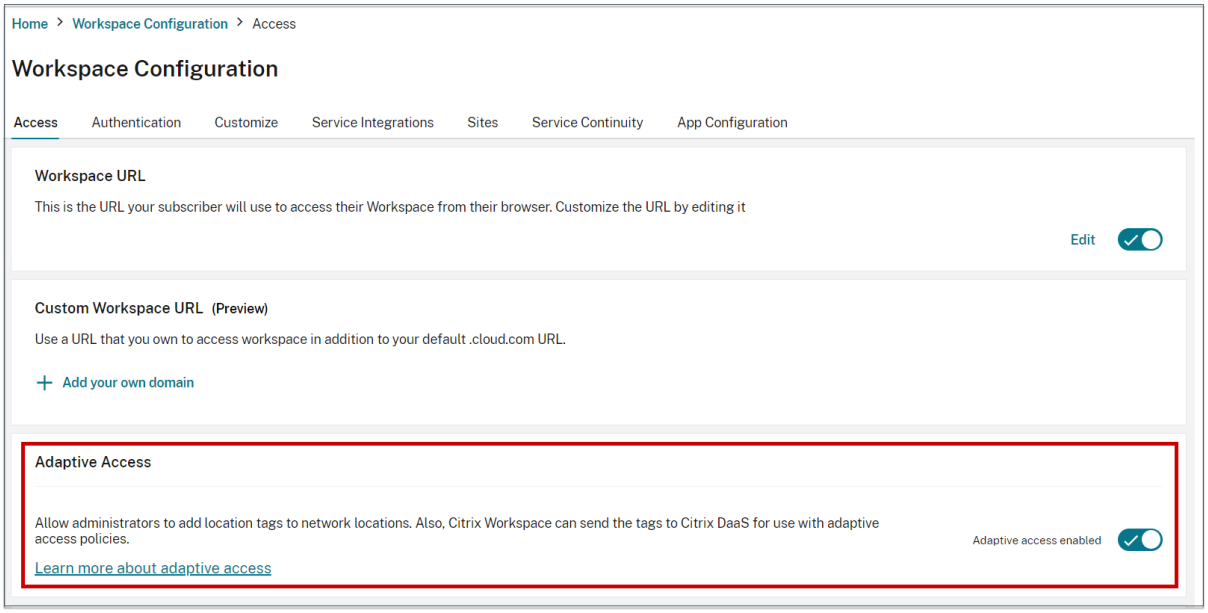
- Si vous prévoyez d'énumérer de manière sélective DaaS en fonction de l'emplacement réseau, la gestion des utilisateurs doit être effectuée à l'aide de stratégies Citrix Studio au lieu de Workspace pour ces groupes de mise à disposition. Lors de la création d'un groupe de mise à disposition, dans **Paramètres utilisateur**, choisissez **Restreindre l'utilisation de ce groupe de mise à disposition aux utilisateurs** ou **Autoriser les utilisateurs authentifiés à utiliser ce groupe de mise à disposition**. Cela vous permet de configurer l'accès adaptatif dans l'onglet **Stratégie d'accès** sous **Groupe de mise à disposition**.

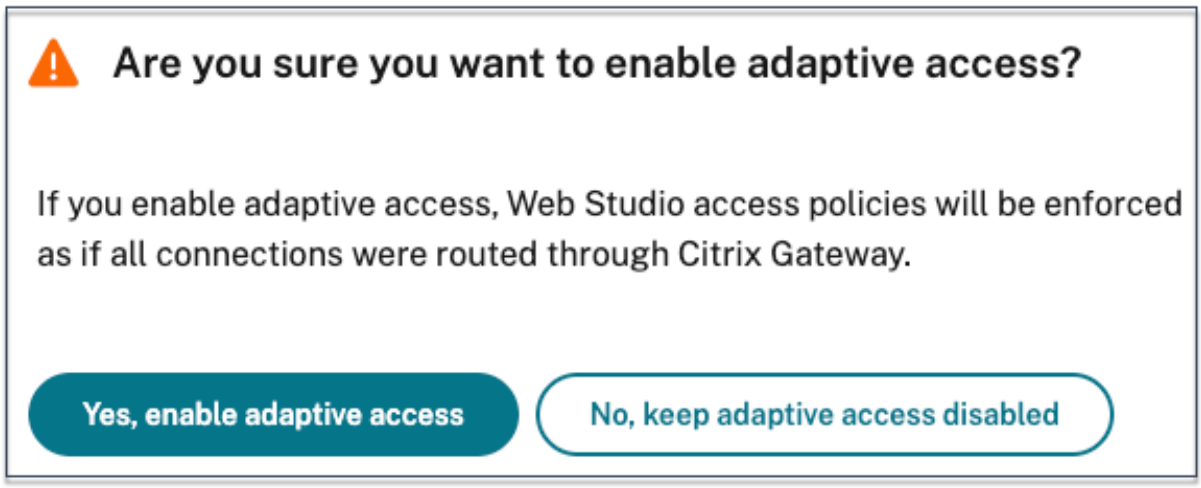


- Modifications apportées à Direct Workload Connection lorsque l'accès adaptatif est activé.
  - Le champ **Balises d'emplacement** est visible dans **Citrix Cloud > Emplacements réseau > Ajouter un emplacement réseau > Balises d'emplacement**.
  - Les stratégies Direct Workload Connection existantes fonctionnent comme prévu.
  - De nouvelles stratégies doivent être créées dans le service Emplacements réseau (sans définir de balises) ainsi que dans le groupe de mise à disposition. De plus, le type de connectivité réseau doit être **Interne**.
  - Pour les nouvelles stratégies Direct Workload Connection avec des balises, les balises doivent être définies dans le service Emplacement réseau et les mêmes balises doivent également être définies dans le groupe de mise à disposition ou la stratégie d'accès dans DaaS Studio. De plus, le type de connectivité réseau doit être **Interne**. Les balises d'emplacement ne sont pas pertinentes pour Direct Workload Connection.
- Il est recommandé de tester votre déploiement Citrix DaaS comme suit.
  - Identifiez un groupe de mise à disposition test ou créez un groupe de mise à disposition pour implémenter cette fonctionnalité.
  - Créez une stratégie ou identifiez une stratégie pouvant être utilisée avec un groupe de mise à disposition test.

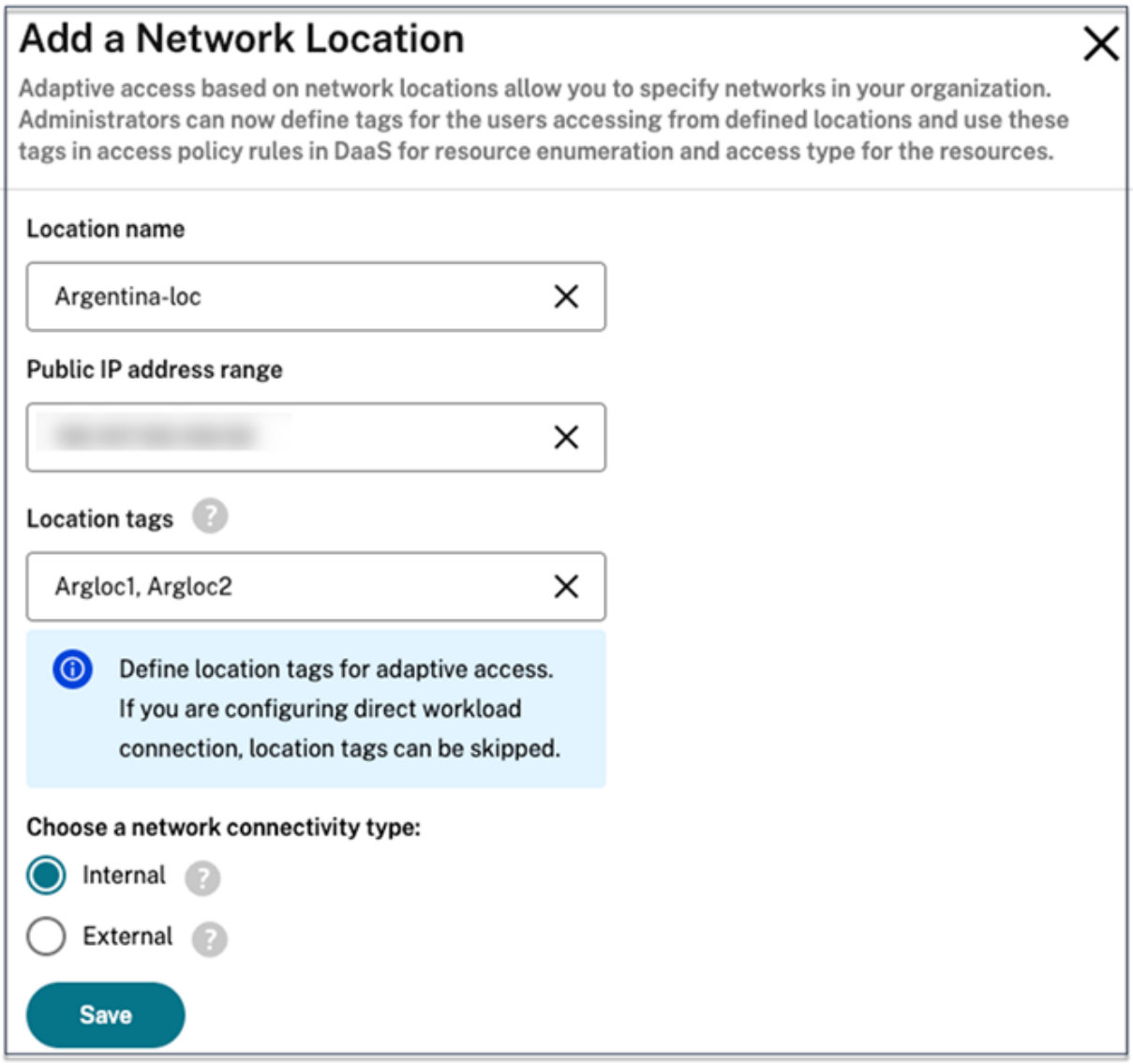
Activer la fonctionnalité Accès adaptatif

1. Connectez-vous à Citrix Cloud.
2. Sélectionnez **Configuration de l'espace de travail** dans le menu hamburger.
3. Le bouton à bascule **Accès adaptatif** est désactivé par défaut. Activez le bouton **Accès adaptatif**.
4. Cliquez sur **Oui, activer l'accès adaptatif** dans le message de confirmation.

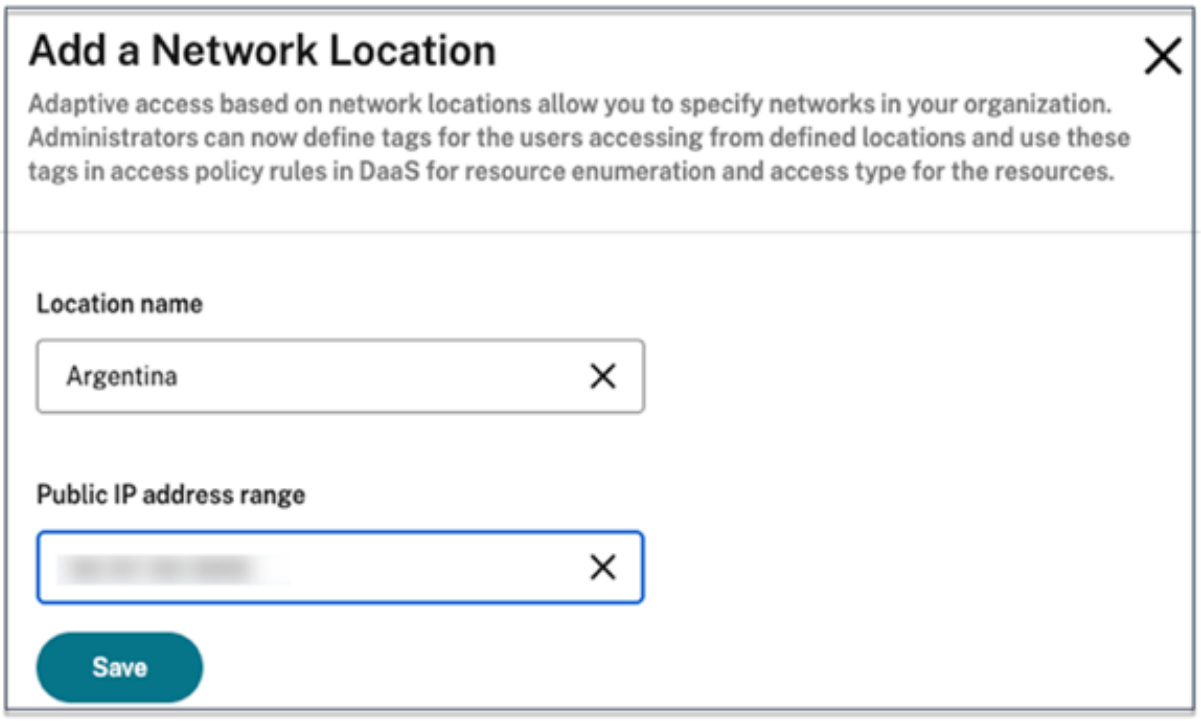




Lorsque l'accès adaptatif est activé, vous pouvez définir les balises d'emplacement pour l'accès adaptatif (**Citrix Cloud > Emplacements réseau > Ajouter un emplacement réseau > Balises d'emplacement**).

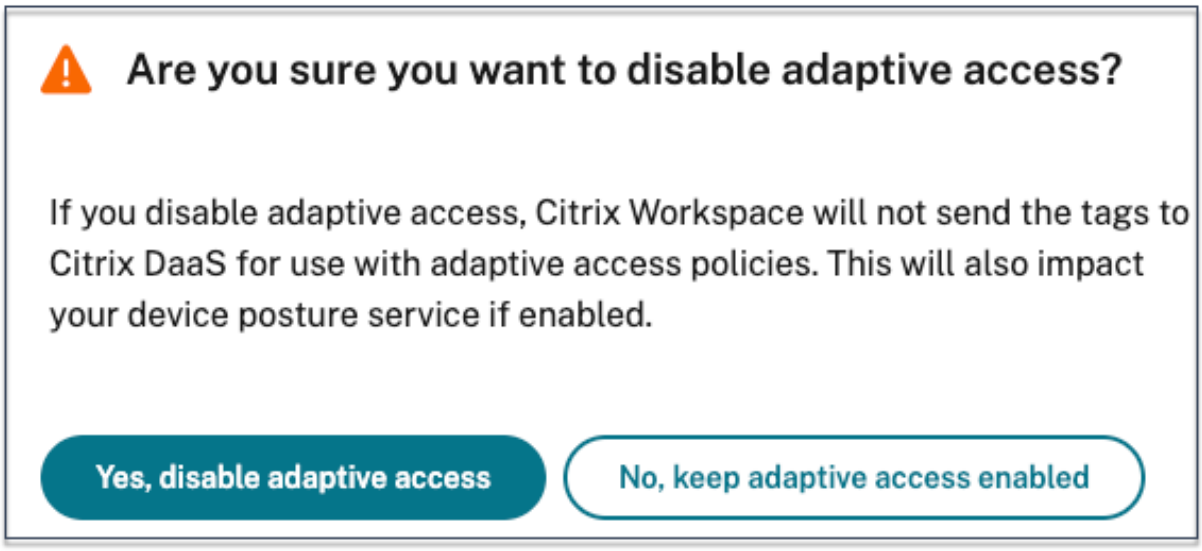


Lorsque l'accès adaptatif est désactivé, vous ne pouvez pas ajouter d'emplacement réseau. Les balises d'emplacement ne sont pas applicables dans ce cas.



Important :

Lorsque vous essayez de désactiver la fonctionnalité Accès adaptatif, le message suivant apparaît. Notez que Workspace n'envoie pas les balises à DaaS pour l'accès adaptatif lorsque la fonctionnalité est désactivée.



Configurer l'accès adaptatif

La configuration de l'accès adaptatif en fonction des emplacements réseau implique les étapes principales suivantes.

1. Définir les stratégies d'emplacement réseau
2. Définir les balises dans DaaS Studio

Pour les exemples de configuration, deux types d'utilisateurs (utilisateurs **BranchOffice** et utilisateurs **WorkFromHome**) sont sélectionnés pour obtenir le cas d'utilisation suivant.

- Les utilisateurs BranchOffice doivent pouvoir accéder aux applications avec tous les accès.
- Les utilisateurs WorkFromHome ne doivent pas avoir accès au presse-papiers.

Dans cet exemple de configuration, **Home** et **Office** sont utilisés comme balises dans les exemples.

Configurer les stratégies d'emplacement réseau

1. Connectez-vous à Citrix Cloud.
2. Sélectionnez **Emplacements réseau** dans le menu hamburger.
   Assurez-vous que le bouton Accès adaptatif est activé. Sinon, l'interface utilisateur de Direct Workload Connection s'affiche.
3. Cliquez sur **Ajouter un emplacement réseau**.

   - **Nom de l'emplacement :** entrez un nom approprié pour la stratégie.

     Exemple : BranchOffice ou WorkFromHome

   - **Plage d'adresses IP publiques :** définissez la plage d'adresses IP publiques de votre réseau.

     Exemple : 172.9.2.1-172.9.2.30

   - **Balises d'emplacement :** définissez des balises pour votre emplacement. Il peut s'agir d'un nom faisant référence à votre emplacement. Ces balises sont utilisées pour configurer les stratégies d'accès adaptatif dans Citrix Studio. Pour plus de détails, consultez la section **Définir des balises dans Citrix Studio**.

     Exemple : *BranchOffice* ou *WorkFromHome*

   - **Type de connectivité :** définissez le type de lancement de l'application.

   Interne : contournez la passerelle pour le lancement de l'application.
   Externe : utilisez le service Citrix Gateway ou une passerelle traditionnelle pour lancer l'application.

4. Cliquez sur **Enregistrer**.

Vous pouvez désormais utiliser ces balises dans DaaS Studio pour activer l'accès adaptatif.

> **Remarque :**
>
> lors de la définition des balises d'emplacement, assurez-vous de ne saisir que le nom de balise préféré sans le préfixe « LOCATION_TAG », par exemple « BranchOffice ». Toutefois, lorsque vous définissez des balises dans Citrix Studio, vous devez préfixer le nom de la balise par « LOCATION_TAG ». Par exemple, « LOCATION_TAG_BRANCHOFFICE ».

Définir des balises dans Citrix Studio à l'aide de l'interface graphique

Dans cet exemple, des balises sont définies dans les groupes de mise à disposition afin de restreindre l'énumération des applications pour les utilisateurs. Deux groupes de mise à disposition sont créés.

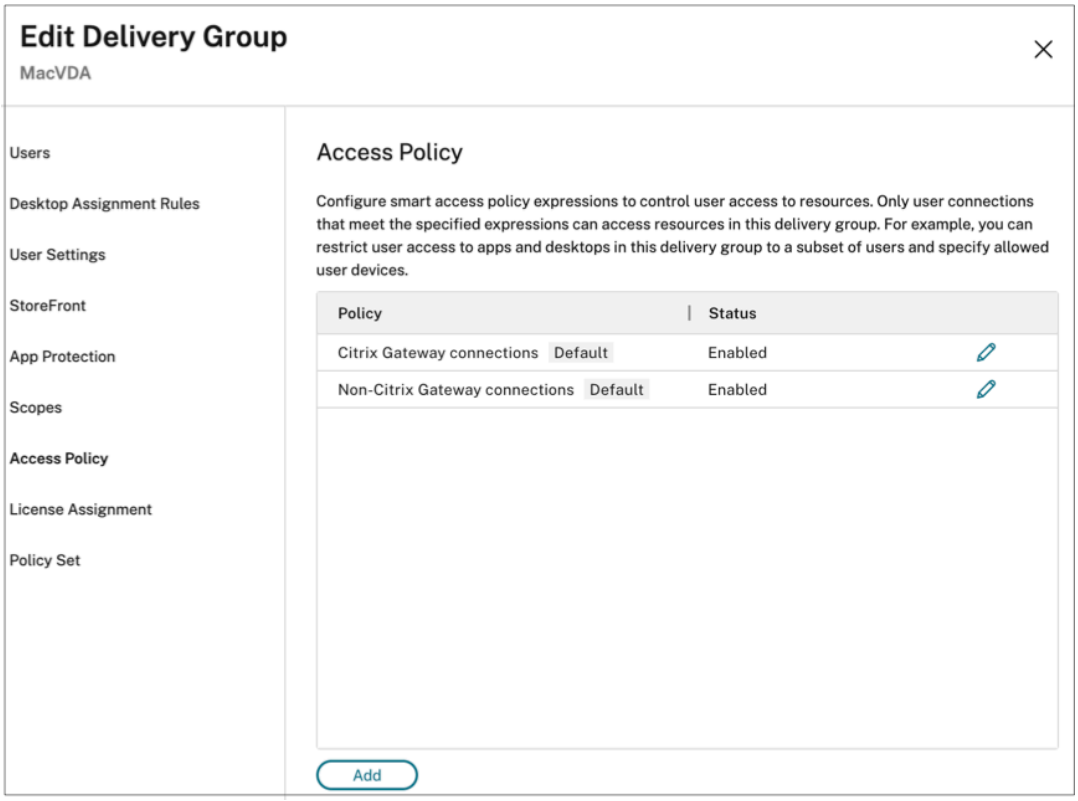
- Groupe de mise à disposition Accès adaptatif —Pour les utilisateurs de l'emplacement **BranchOffice**. Ces utilisateurs doivent voir toutes les applications de ce groupe de mise à disposition.
- Groupe de mise à disposition WFH —Pour les utilisateurs de l'emplacement **WorkFromHome**. Ces utilisateurs doivent voir les applications de ce groupe de mise à disposition.

1. Connectez-vous à Citrix Cloud.
2. Dans la vignette **Citrix DaaS**, cliquez sur **Gérer**.
3. Créez un groupe de mise à disposition. Pour de plus amples informations, consultez la section Créer des groupes de mise à disposition.
4. Sélectionnez le groupe de mise à disposition que vous avez créé et cliquez sur **Modifier le groupe de mise à disposition**.
5. Cliquez sur **Stratégie d'accès**.
6. Pour les clients qui utilisent l'accès adaptatif dans la plate-forme Citrix Workspace, procédez comme suit pour restreindre l'accès d'un groupe de mise à disposition aux réseaux internes uniquement :

    a) Cliquez avec le bouton droit sur le groupe de mise à disposition et sélectionnez **Modifier**.

    b) Sélectionnez la stratégie d'accès dans le panneau de gauche.

    c) Cliquez sur l'icône "Modifier"pour modifier la stratégie de connexion par défaut de Citrix Gateway.



d) Sur la page **Modifier la stratégie**, sélectionnez **Connexions répondant aux critères suivants**, sélectionnez **N'importe quelle connexion**, puis ajoutez les critères.

Pour les utilisateurs de WorkFromHome, entrez les valeurs suivantes dans le Delivery Controller correspondant.

Batterie : espace de travail

Filtre : LOCATION_TAG_WORKFROMHOME

Pour les utilisateurs de BranchOffice, entrez les valeurs suivantes dans le Delivery Controller correspondant.

Filtre : espace de travail

Valeur : LOCATION_TAG_BRANCHOFFICE

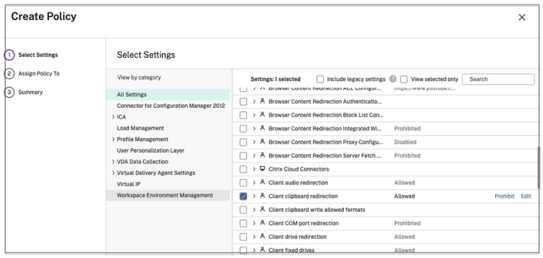
Vous pouvez désormais utiliser ces balises pour restreindre l'accès aux applications.

> **Remarque :**
>
> Assurez-vous de saisir dans le champ **Valeur** le nom de balise d'emplacement correct, tel que vous l'avez défini lors de la création des stratégies d'emplacement réseau préfixées par « LOCATION_TAG ». Par exemple, si vous avez défini la balise d'emplacement « BranchOffice », vous devez saisir « LOCATION_TAG_BRANCHOFFICE » dans le champ **Valeur**. Pour plus de détails sur la configuration des balises d'emplacement, reportez-vous à la section Configurer les stratégies d'emplacement réseau.

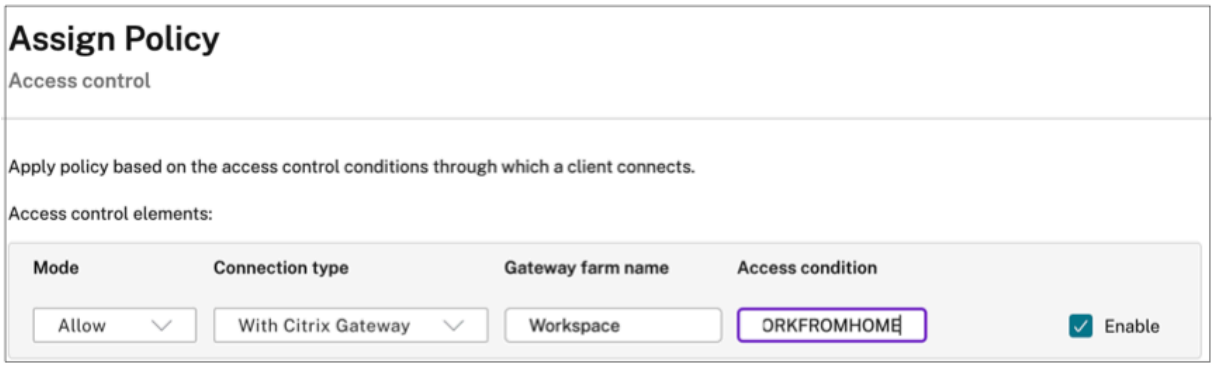
Restreindre l'accès aux applications

Dans cet exemple, la redirection du presse-papiers du client est désactivée pour les utilisateurs de l'emplacement WorkFromHome.

1. Connectez-vous à Citrix DaaS.
2. Accédez à **Stratégies** et cliquez sur **Créer une stratégie**.
3. Sélectionnez **Redirection du Presse-papiers client**, puis cliquez sur **Interdire**.
4. Cliquez sur **Suivant**.



1. Sur la page **Attribuer la stratégie à**, sélectionnez **Contrôle d'accès**.
2. Définissez les valeurs suivantes pour la stratégie :
   - Mode : **Autoriser**
   - Type de connexion : **Avec Citrix Gateway**
   - Nom de la batterie Gateway : **Workspace**
   - Condition d'accès : **LOCATION_TAG_WORKFROMHOME** (tout en majuscules)



1. Cliquez sur **Suivant**.
2. Entrez le nom de la stratégie et ajoutez une description de la stratégie.
3. Cliquez sur **Terminer**.

Les utilisateurs de l'emplacement **WorkFromHome** ne peuvent pas accéder aux ressources qu'ils ont lancées dans le presse-papiers.

Configurer les stratégies d'enregistrement de session en fonction des balises

L'enregistrement de session permet aux organisations d'enregistrer l'activité des utilisateurs à l'écran lors de sessions virtuelles. Vous pouvez spécifier des balises, telles que des balises d'emplacement réseau, lors de la création d'une stratégie d'enregistrement de session personnalisée, d'une stratégie de détection d'événements ou d'une stratégie de réponse aux événements. Pour consulter un exemple, reportez-vous à Créer une stratégie d'enregistrement personnalisée.

Balises d'emplacement réseau

Le service Emplacements réseau fournit les balises suivantes.

- **Balises par défaut :** ces balises sont définies sur le service Emplacements réseau. Les balises par défaut suivantes sont disponibles.
  - **Location_internal :** balise envoyée par défaut lorsque le type de connectivité réseau est défini sur **INTERNAL**.
  - **Location_external :** balise envoyée par défaut lorsque le type de connectivité réseau est défini sur **EXTERNAL**.
  - **Location_undefined :** balise envoyée pour une adresse IP qui n'est pas définie dans la stratégie mais qui passe par le service Emplacements réseau. Les lancements pour ces utilisateurs sont identiques à ceux définis dans le groupe de ressources.
- **Balises personnalisées :** les administrateurs peuvent définir des noms de balises personnalisés dans les stratégies. Exemple : bureau, domicile, succursale

Exemples :

Balises par défaut : LOCATION_INTERNAL, LOCATION_EXTERNAL, LOCATION_UNDEFINED

Balises personnalisées : LOCATION_TAG_OFFICE, LOCATION_TAG_HOME

> **Remarque :**
>
> Lorsque vous définissez des balises pour le service Emplacement réseau, assurez-vous de respecter ces règles :
>
> - Les balises par défaut commencent toujours par le préfixe « LOCATION_<tag name> ». Par exemple, LOCATION_INTERNAL.
> - Les balises personnalisées commencent toujours par le préfixe « LOCATION_TAG<tag name> ». Par exemple, LOCATION_TAG_OFFICE.

Problèmes connus

Si vous désactivez la fonctionnalité Accès adaptatif une fois qu'elle a été activée et que les règles ont été définies (balises et type de connectivité), les emplacements ne sont pas supprimés de la page Emplacements réseau, bien que les balises d'emplacement et les colonnes du type de connectivité soient masquées. Mais ces emplacements sont désactivés dans le back-end. Il s'agit d'un problème esthétique.

Packages d'applications

June 12, 2024

Plusieurs technologies de packaging permettent de fournir des applications aux utilisateurs, telles qu'App-V, MSIX, l'attachement d'application MSIX et FlexApp. Cet article explique comment déployer et fournir ces applications packagées dans votre environnement Citrix DaaS :

- 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 distribuer des applications FlexApp

Déployer et fournir des applications App-V

Cette section contient les informations suivantes :

- Vue d'ensemble. Décrit les méthodes de gestion utilisées par Citrix DaaS 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 par Citrix DaaS pour fournir et 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.

Citrix DaaS fournit et gère les packages App-V à l'aide des méthodes suivantes :

- **Administration double**. Les packages d'applications sont configurés et gérés sur les serveurs App-V. Les serveurs Citrix DaaS et App-V fonctionnent ensemble pour fournir et gérer les packages.

  Cette méthode exige que Citrix DaaS 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 DaaS 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 Citrix Cloud 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 DaaS 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 Citrix Cloud. 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 des packages d'applications dans Citrix Cloud.
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 DaaS 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 Citrix DaaS fournit et gère les packages MSIX et les packages créés via l'attachement d'application MSIX.
- Procédures. Fournit des procédures pour le déploiement et la mise à disposition de ces packages.

Vue d'ensemble

Citrix DaaS 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 des packages d'applications dans Citrix Cloud.
3. Ajouter des applications à des groupes de mise à disposition.

Déployer et distribuer des applications FlexApp

Cette section contient les informations suivantes :

- Vue d'ensemble. Décrit la manière dont Citrix DaaS fournit et gère les packages FlexApp.
- Procédures. Fournit des procédures pour le déploiement et la mise à disposition de ces packages.

Vue d'ensemble

Citrix DaaS fournit des applications FlexApp aux utilisateurs via le composant Citrix Personalization et l'agent de distribution FlexApp installés sur les machines VDA. Ces deux composants gèrent tous les aspects des cycles de vie des packages sur la machine hôte.

Procédures

Pour prendre en charge la mise à disposition d'applications FlexApp, vous devez installer les composants suivants sur les machines VDA :

- Le composant Citrix Personalization sur les machines VDA. Consultez Installer le composant Citrix Personalization sur les machines VDA pour obtenir plus d'informations.
- L'agent FlexApp sur les VDA. Consultez l'article Installer l'agent FlexApp pour plus de détails.

Pour mettre à disposition de vos utilisateurs des applications packagées FlexApp , procédez comme suit :

1. Stocker les packages d'applications sur des partages réseau.
2. Charger des packages d'applications dans Citrix Cloud.
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, aux formats crées via l'attachement d'application MSIX et FlexApp. 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.
    - Pour **les applications FlexApp**: 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 des packages d'applications dans Citrix Cloud

Après avoir stocké les packages d'applications sur un emplacement réseau selon vos besoins, chargez-les sur Citrix Cloud afin de les distribuer. Si nécessaire, utilisez l'une des méthodes suivantes :

- Chargement en bloc
- Chargement un par un

Préparations

Citrix DaaS 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
  - Pour découvrir les packages FlexApp : version 2311 ou 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

Rôles requis

Par défaut, si vous avez le rôle Administrateur Cloud ou Administrateur complet, vous pouvez charger des packages d'applications sur Citrix Cloud. Vous pouvez également créer des rôles personnalisés pour effectuer les actions de chargement. Le tableau suivant répertorie les autorisations requises par les actions des packages d'applications.

Action	Autorisation requise
Ajouter un package (chargement un par un)	Créer des sessions de détection d'applications
Ajouter la source (chargement en bloc)	Créer des profils de détection d'applications
Rechercher des mises à jour de packages	Créer des sessions de détection d'applications
Supprimer la source	Supprimer les profils de détection d'applications

Charger des packages d'applications en bloc

Chargez des packages dans un emplacement réseau sur Citrix Cloud. 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 **Gérer > Configuration complète**, sélectionnez **Packages d'applications** dans le volet gauche.
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, l'attachement d'application MSIX et FlexApp.
  - 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 DaaS charge les packages sur Citrix Cloud à l'aide d'un VDA dans le 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 Citrix Cloud, 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 Citrix Cloud. 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 télécharger un package sur Citrix Cloud, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Packages d'applications** dans le volet gauche.
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.

> **Remarque :**
>
> - Vous pouvez fournir des applications packagées à des VDA monosession et à des VDA multisession via des groupes de mise à disposition.
> - Par défaut, les utilisateurs ont accès à toutes les applications packagées attribuées aux groupes de mise à disposition associés à leurs VDA *monosession* (ou appelés VDA de*bureau*). Pour limiter la visibilité d'une application packagée sur des VDA de *bureau* à des utilisateurs ou à des groupes spécifiques, accédez au nœud **Applications**, sélectionnez l'application, puis **Modifier les propriétés de l'application > Limiter la visibilité** pour apporter les modifications souhaitées.

Pour ajouter une ou plusieurs applications d'un package à plusieurs groupes de mise à disposition, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Packages d'applications** dans le volet gauche.
2. Dans l'onglet **Packages**, sélectionnez un package selon vos besoins.
3. Dans la barre d'actions, cliquez sur **Attribuer des applications à des groupes de mise à disposition**. La page Attribuer des applications à des groupes de mise à disposition apparaît.
4. Sélectionnez une ou plusieurs applications dans le package selon vos besoins, puis cliquez sur **Suivant**.
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.
> - Si vous avez sélectionné un package *FlexApp*, seuls les groupes de mise à disposition dont le niveau fonctionnel est 2206 ou supérieur sont affichés dans la liste.

6. Cliquez sur **Terminer**.

Pour ajouter des applications de différents packages à plusieurs groupes de mise à disposition, procédez comme suit :

1. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet gauche.
2. Dans l'onglet **Applications**, sélectionnez **Ajouter des applications**.
3. Sur la page **Groupes**, sélectionnez un ou plusieurs groupes de mise à disposition selon vos besoins.
4. Sur la page **Applications**, sélectionnez un ou plusieurs packages d'applications comme suit :
    a) Cliquez sur **Ajouter**, puis sélectionnez **Packages d'applications**.
    b) Sélectionnez le type de source de package requis (par exemple, App-V Single Admin). Tous les packages de ce type s'affichent.
    c) Sélectionnez un ou plusieurs packages selon vos besoins.
    d) Cliquez sur **OK**, puis sur **Suivant**.
    e) Pour ajouter d'autres applications d'un type de package différent, répétez les étapes de a à d.
5. 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'isolement 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 DaaS 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 Citrix Cloud 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.

Autoscale

March 7, 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 intègre la technologie Smart Scale obsolète dans la solution de gestion de l'alimentation de la console **Gérer**.

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)
- Provisioning dynamique des machines
- 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 DaaS. Cela inclut une variété de plateformes d'infrastructure, notamment XenServer (anciennement Citrix Hypervisor), Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware

vSphere, etc. Pour obtenir la liste complète des plates-formes prises en charge, consultez la section Configuration système requise pour Citrix DaaS.

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, disponible sous l'onglet **Surveiller**.

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

November 2, 2023

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.

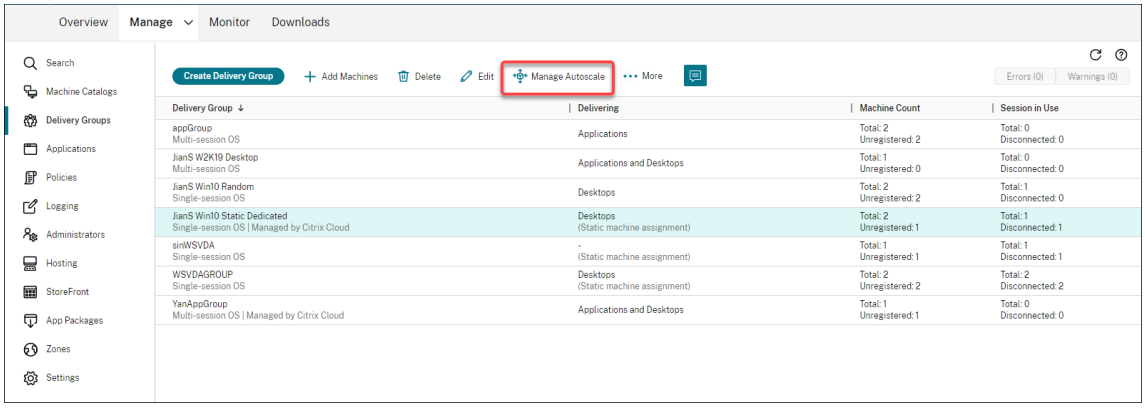
- Le chiffre « 0 » indique une machine déchargée. Une machine dont la valeur d'indice de charge est 0 est à une charge de base.
- Le chiffre « 10 000 » indique une machine entièrement chargée qui ne peut plus exécuter de sessions.

Activer Autoscale pour un groupe de mise à disposition

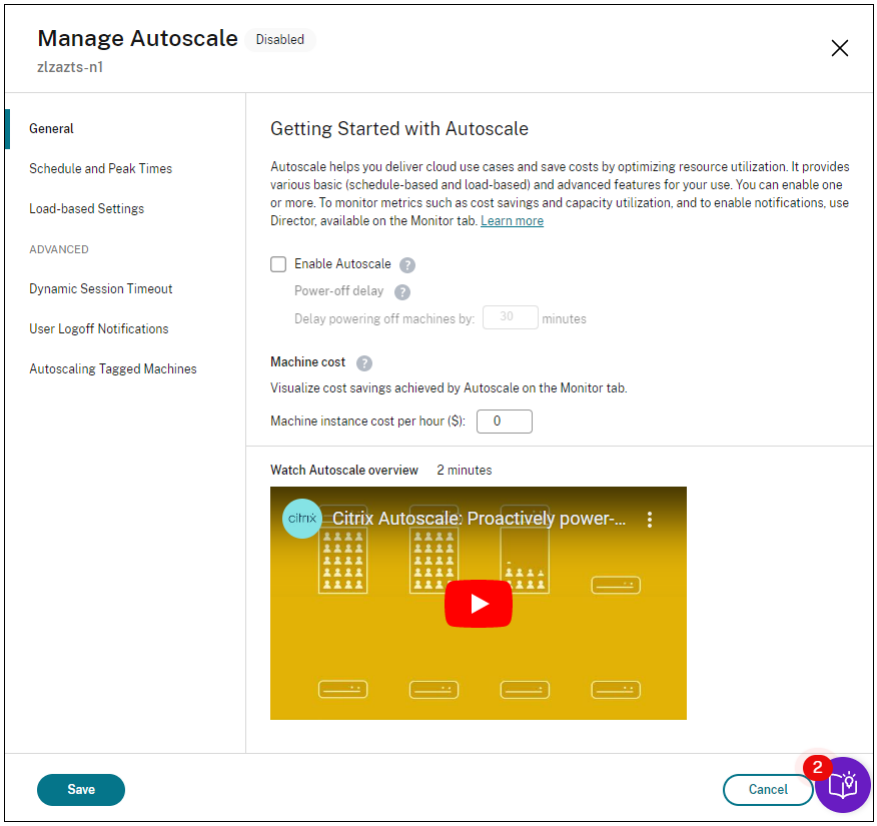
Par défaut, Autoscale est désactivé lorsque vous créez un groupe de mise à disposition. Pour activer et configurer Autoscale pour un groupe de mise à disposition à l'aide de l'interface Configuration complète, procédez comme suit :

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. Dans **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet 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.

Vous pouvez provisionner dynamiquement des machines pour le groupe à l'aide d'un script PowerShell. Pour plus d'informations, voir Provisioning dynamique des machines.

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 sous l'onglet **Surveiller**.

- 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**.

Pour surmonter ce goulot d'étranglement, vous pouvez utiliser un script PowerShell pour créer des machines et les supprimer dynamiquement. Pour plus d'informations, consultez Provisionner dynamiquement les machines.

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

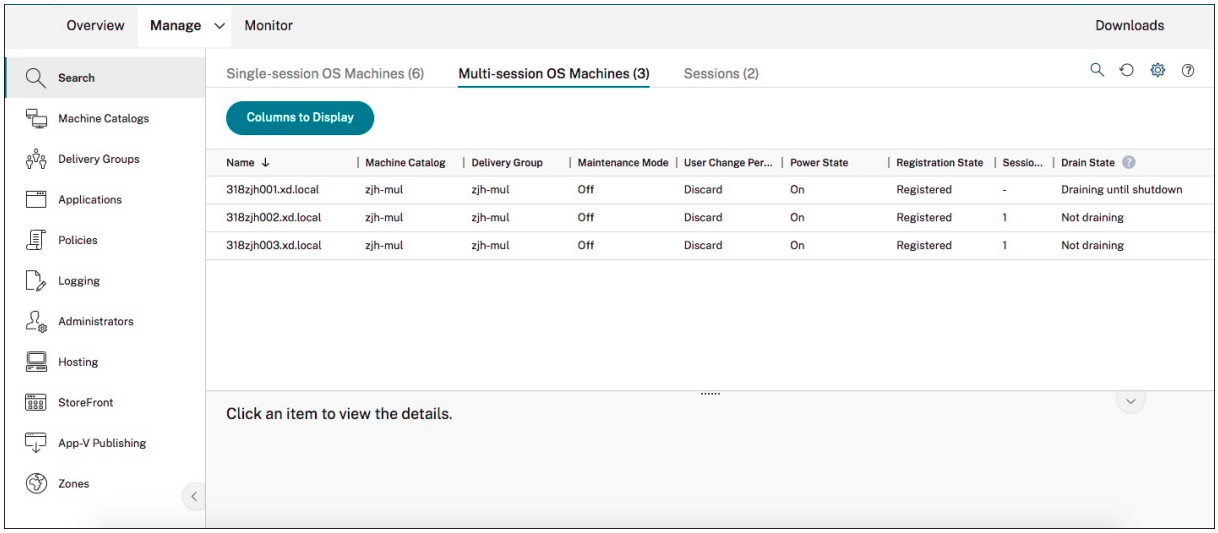
> **Remarque :**
>
> Cette fonctionnalité s'applique uniquement aux machines multi-session.

Dans **Gérer > Configuration complète**, vous pouvez afficher les machines qui sont en état de drainage, vous permettant 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

November 2, 2023

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.

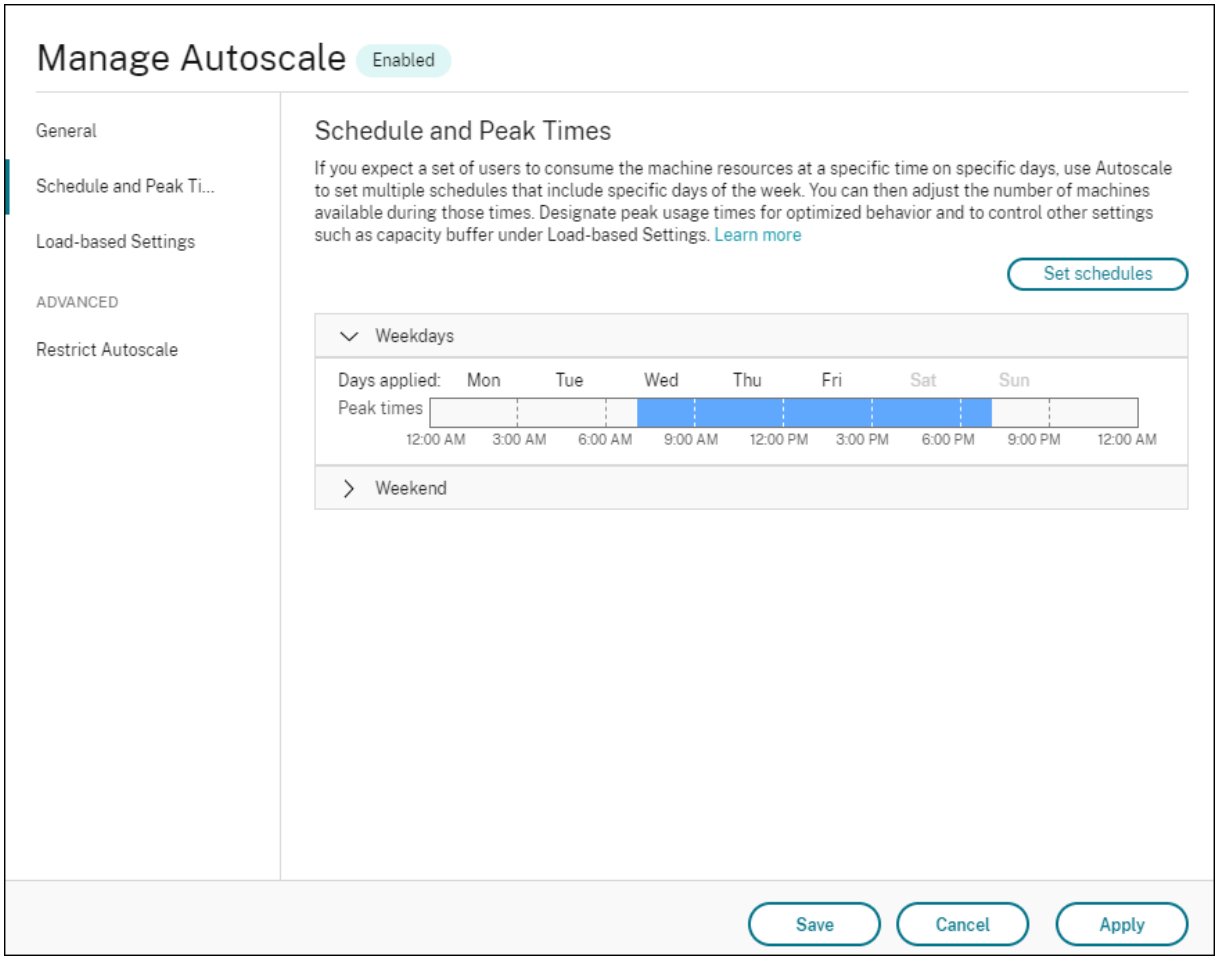
Autoscale a deux calendriers par défaut : les *jours de la semaine* (du lundi au vendredi) et le *week-end* (le samedi et le dimanche). Par défaut, le programme **Jours ouvrés** maintient une machine sous tension de 7h00 à 18h30 pendant les heures de pointe et aucune pendant les heures creuses. Le tampon 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.

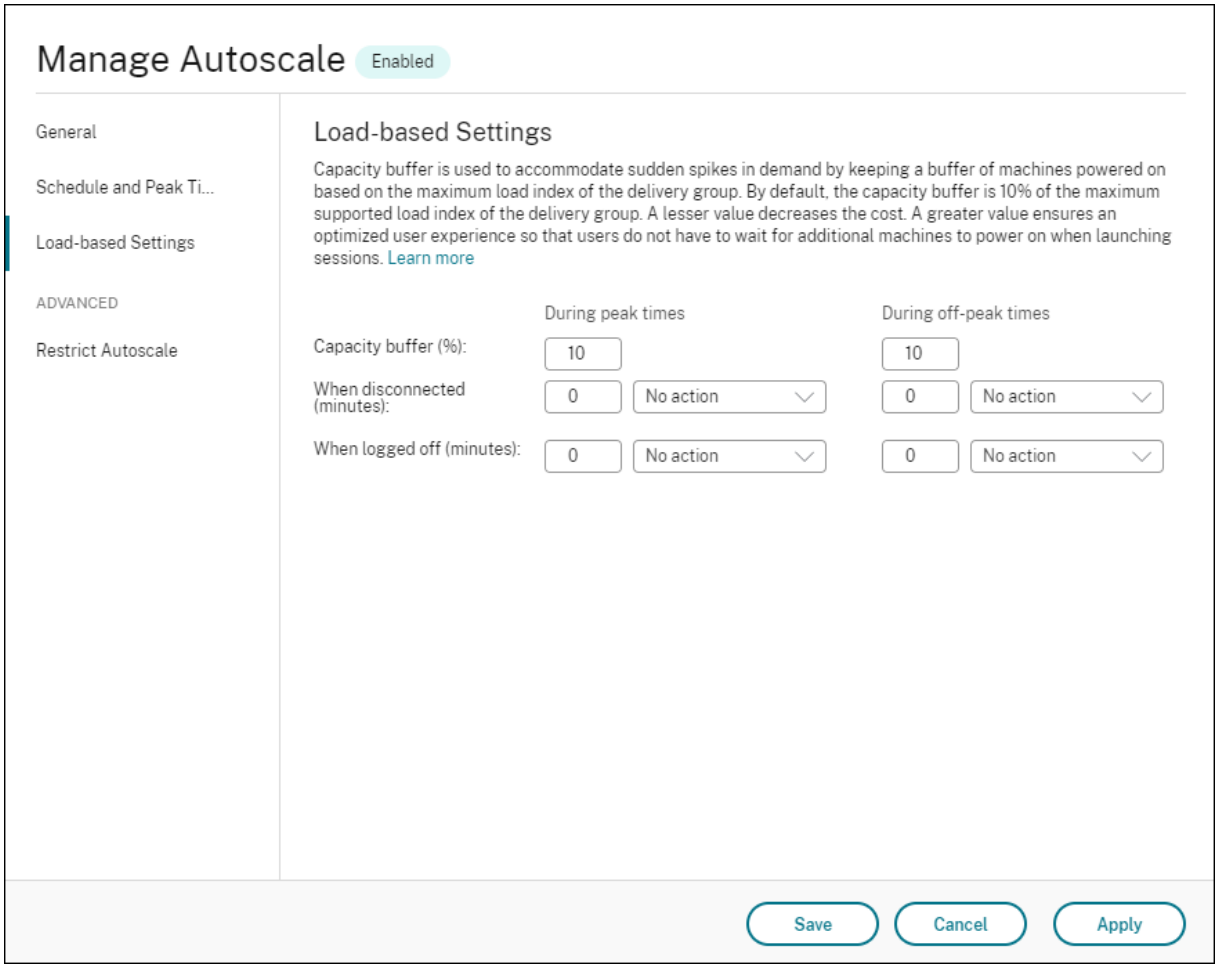
> **Remarque :**
>
> Autoscale traite uniquement les machines enregistrées sur le site comme faisant partie de la capacité disponible dans les calculs qu'il effectue. « Enregistré » signifie que la machine est disponible ou déjà utilisée. Cela garantit que seules les machines qui acceptent les sessions utilisateur sont incluses dans la capacité du groupe de mise à disposition.

Interfaces utilisateur

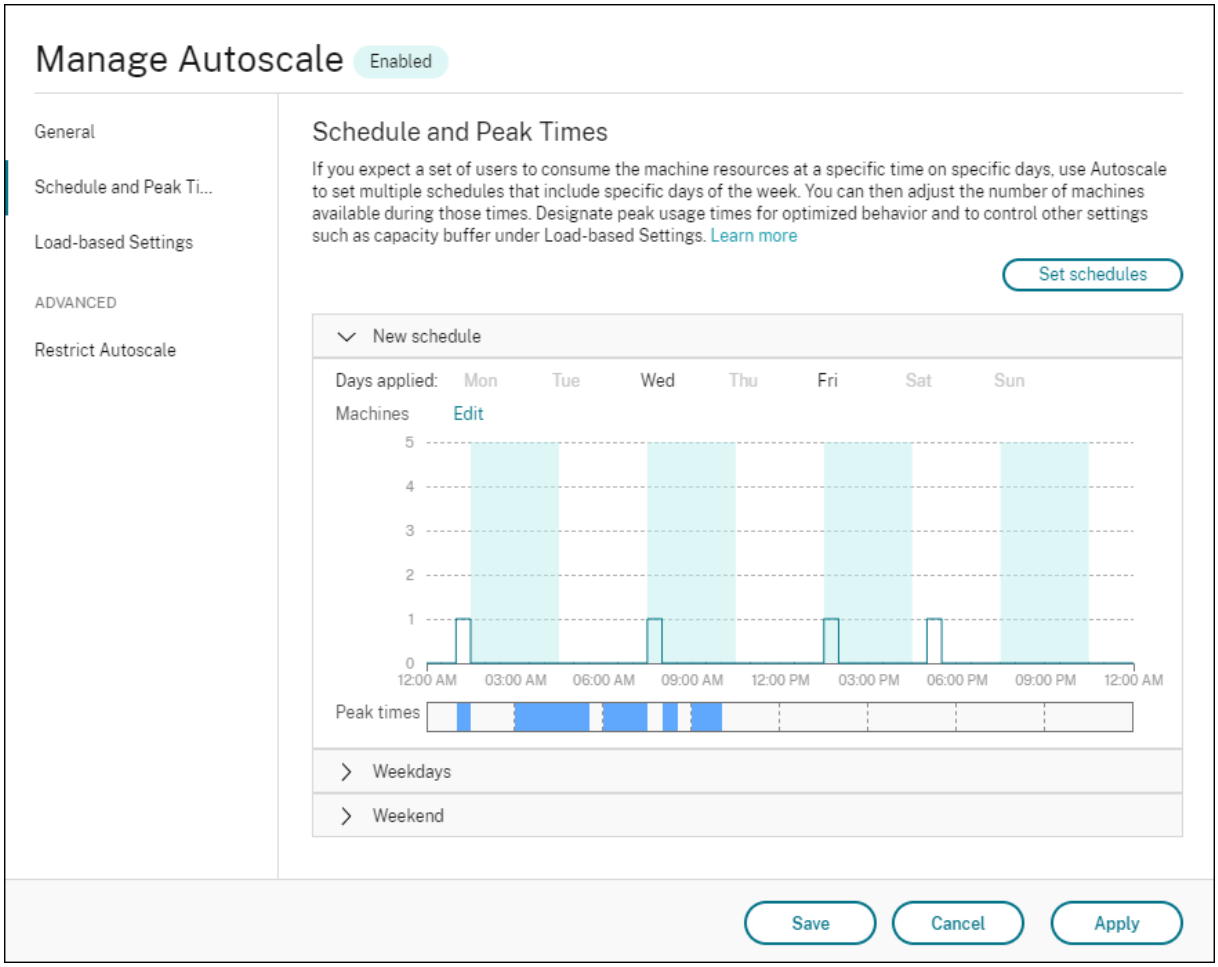
Il existe trois types d'interfaces utilisateur.

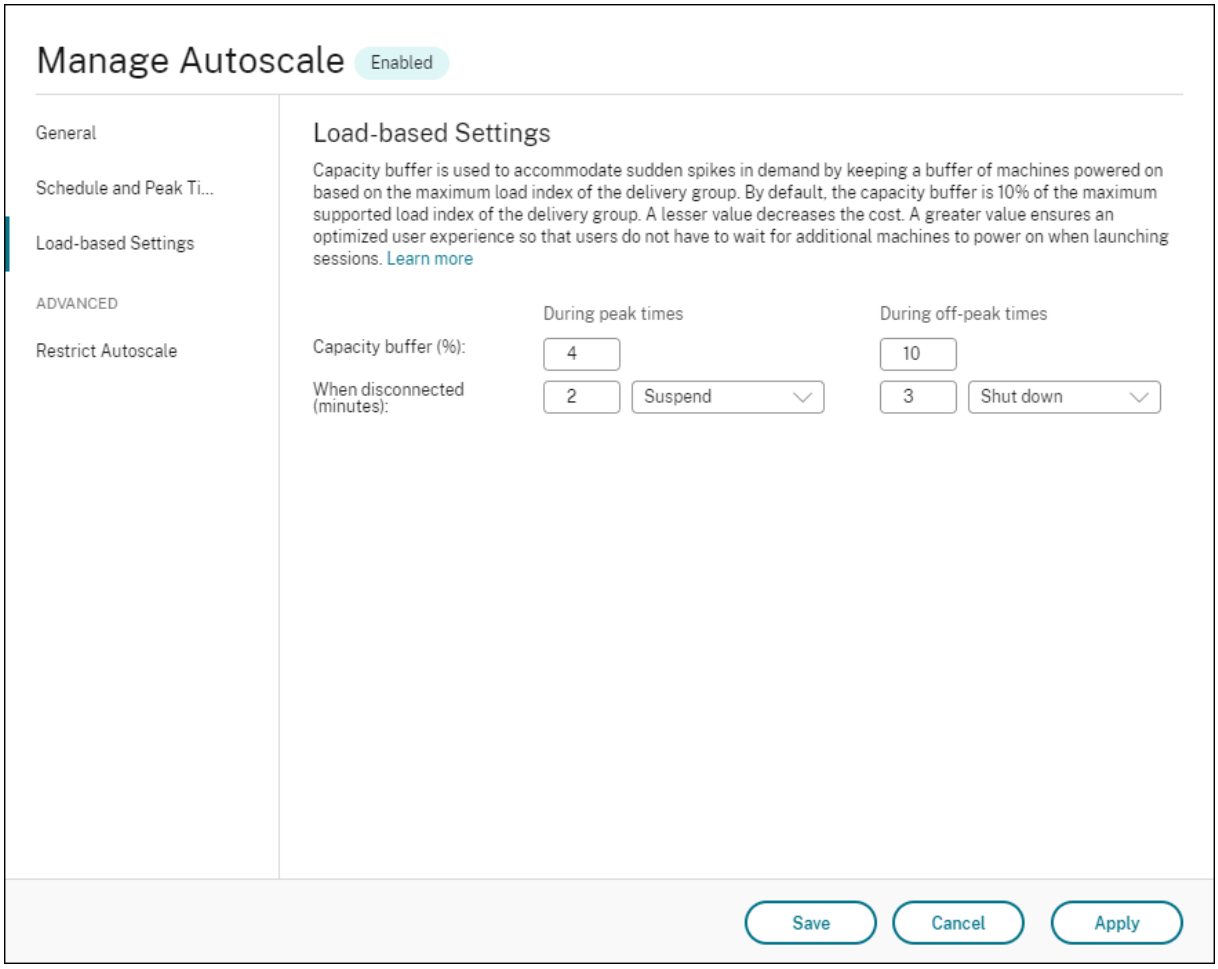
Interface utilisateur pour *groupes de mise à disposition statiques OS mono-session* :



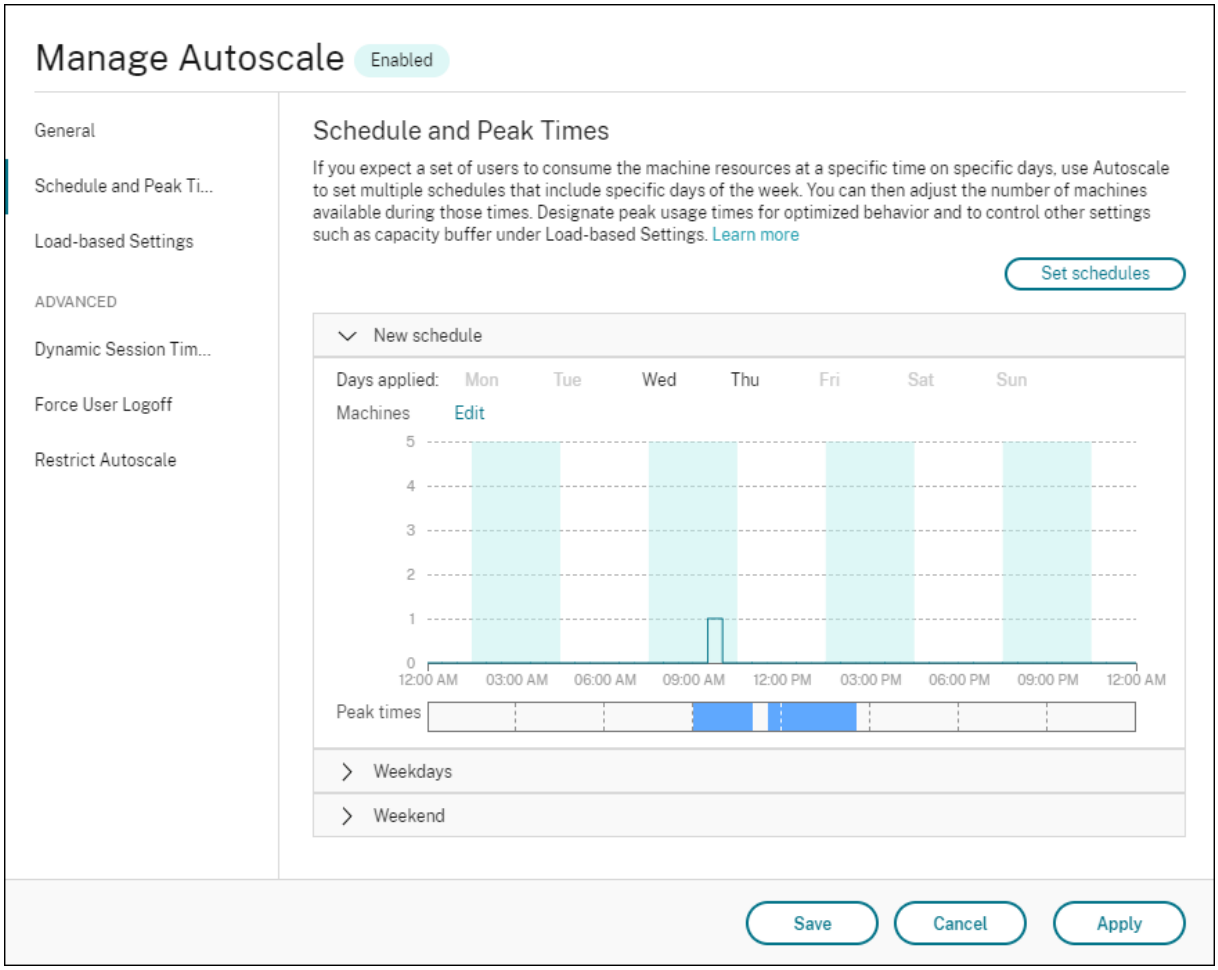


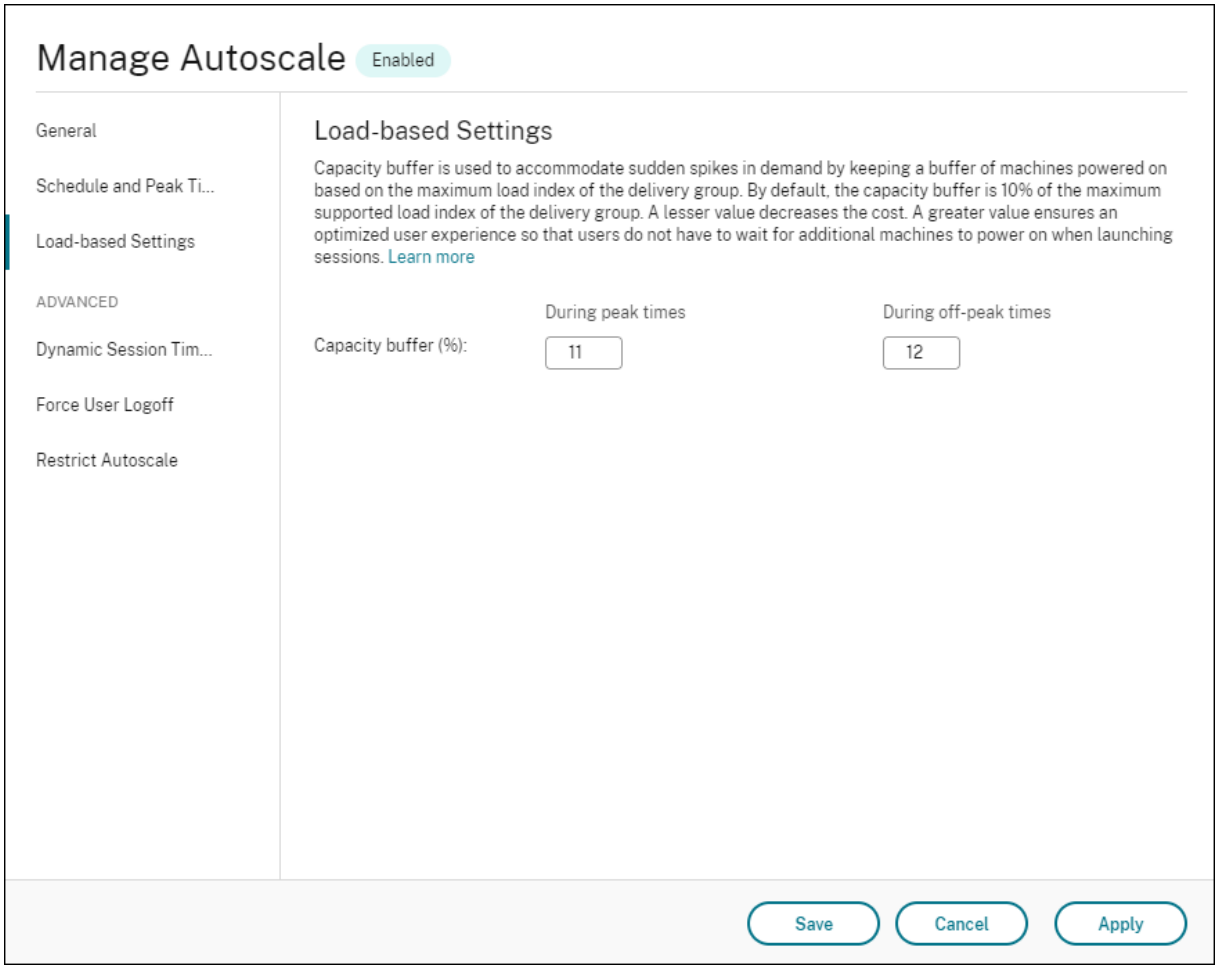
Interface utilisateur Autoscale pour *groupes de mise à disposition aléatoires OS mono-session* :





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.

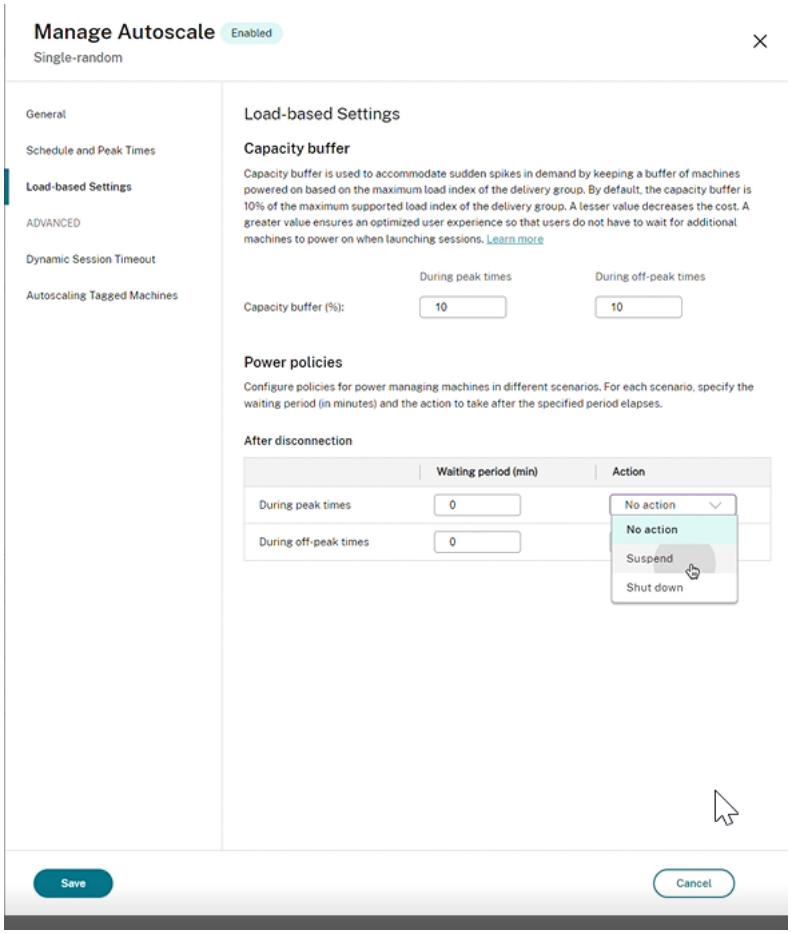
Groupes de mise à disposition aléatoires OS mono-session

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.

Stratégies d'alimentation

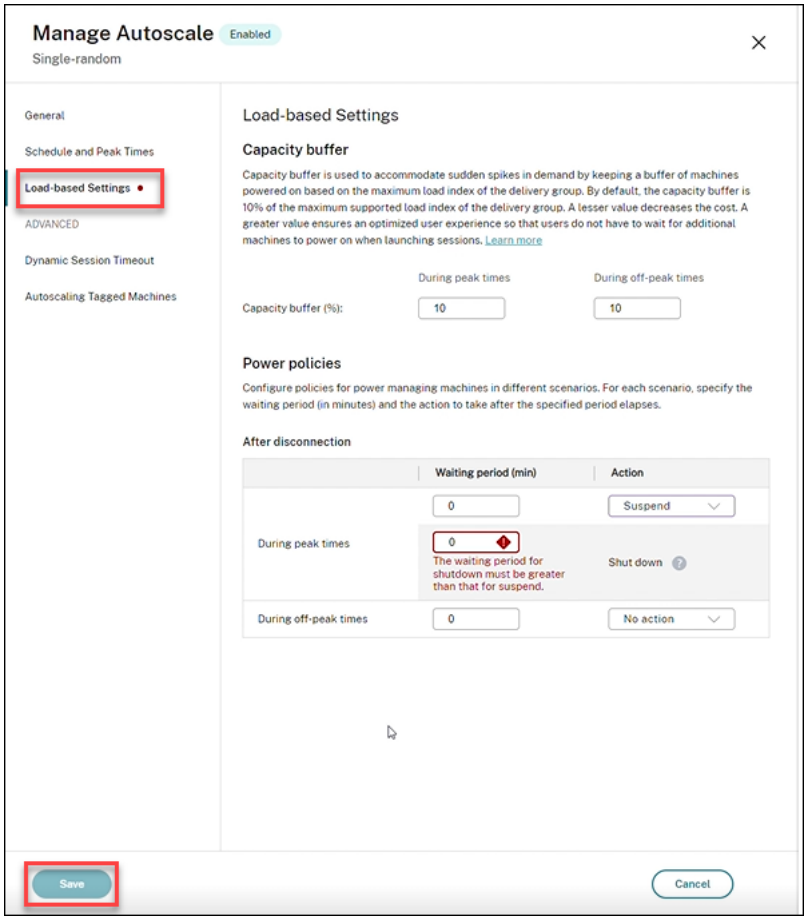
Configurez des stratégies pour gérer l'alimentation des machines selon différents scénarios. Pour chaque scénario, vous pouvez spécifier le temps d'attente (en minutes) et les mesures à prendre après la fin du délai spécifié. Les stratégies d'alimentation s'appliquent aux groupes de mise à disposition aléatoires OS mono-session et aux groupes de mise à disposition statiques OS mono-session.



Après la déconnexion, les paramètres suivants s'appliquent aux heures de pointe et aux heures creuses :

- Vous pouvez définir le temps d'attente en minutes et des actions telles que l'absence d'action, la suspension ou l'arrêt dans le menu déroulant.
- Si vous sélectionnez l'action de suspension, configurez un temps d'attente supplémentaire pour arrêter la machine.

> **Remarque :**
>
> - Pendant les heures de pointe et les heures creuses, le temps d'attente pour l'arrêt doit être supérieur au temps d'attente pour la suspension.
> - Les machines suspendues ne sont accessibles qu'aux utilisateurs déconnectés lorsqu'ils se reconnectent. Pour mettre les machines suspendues à la disposition des nouveaux utilisateurs, arrêtez-les.
> - Si les paramètres d'heure ne sont pas correctement configurés pour les champs de suspension et d'arrêt, l'option **Enregistrer** est désactivée et un point rouge apparaît également à côté des éléments de navigation indiquant des erreurs de réglage.



Par exemple

- Si vous réglez le temps d'attente sur 12 minutes et que vous choisissez comme première action l'absence d'action, la machine restera allumée au bout de 12 minutes.
- Si vous réglez le temps d'attente sur 15 minutes et que vous choisissez comme première action la suspension et réglez le deuxième temps d'attente sur 20 minutes, la machine sera suspendue au bout de 15 minutes. Après la fin du deuxième temps d'attente, la machine sera arrêtée.
- Si vous réglez le temps d'attente sur 18 minutes et que vous choisissez comme première action l'arrêt, la machine sera arrêtée au bout de 18 minutes.

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.

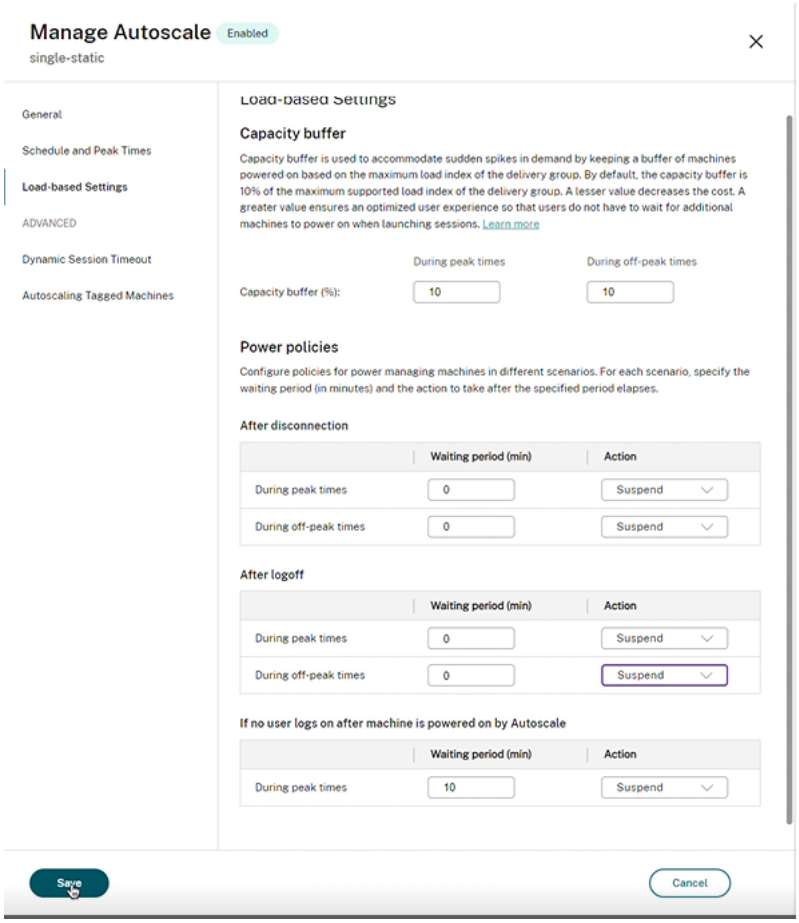
Pour comprendre le fonctionnement du tampon de capacité avec les machines attribuées, tenez compte des points suivants :

- 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.

Stratégies d'alimentation

Configurez des stratégies pour gérer l'alimentation des machines selon différents scénarios. Pour chaque scénario, vous pouvez spécifier le temps d'attente (en minutes) et les mesures à prendre après la fin du délai spécifié. Les stratégies d'alimentation s'appliquent aux groupes de mise à disposition aléatoires d'OS mono-session et aux groupes de mise à disposition statiques d'OS mono-session.



Pour **Après la déconnexion** et **Après la fermeture de session**, les paramètres suivants s'appliquent aux heures de pointe et aux heures creuses :
Vous pouvez définir le temps d'attente en minutes et des actions telles que l'absence d'action, la

suspension ou l'arrêt dans le menu déroulant.

Si aucun utilisateur ne se connecte après la mise sous tension de la machine par Autoscale, les paramètres suivants ne s'appliquent qu'aux heures de pointe :
Vous pouvez définir le temps d'attente en minutes et des actions telles que l'absence d'action, la suspension ou l'arrêt dans le menu déroulant pendant les heures de pointe.

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.

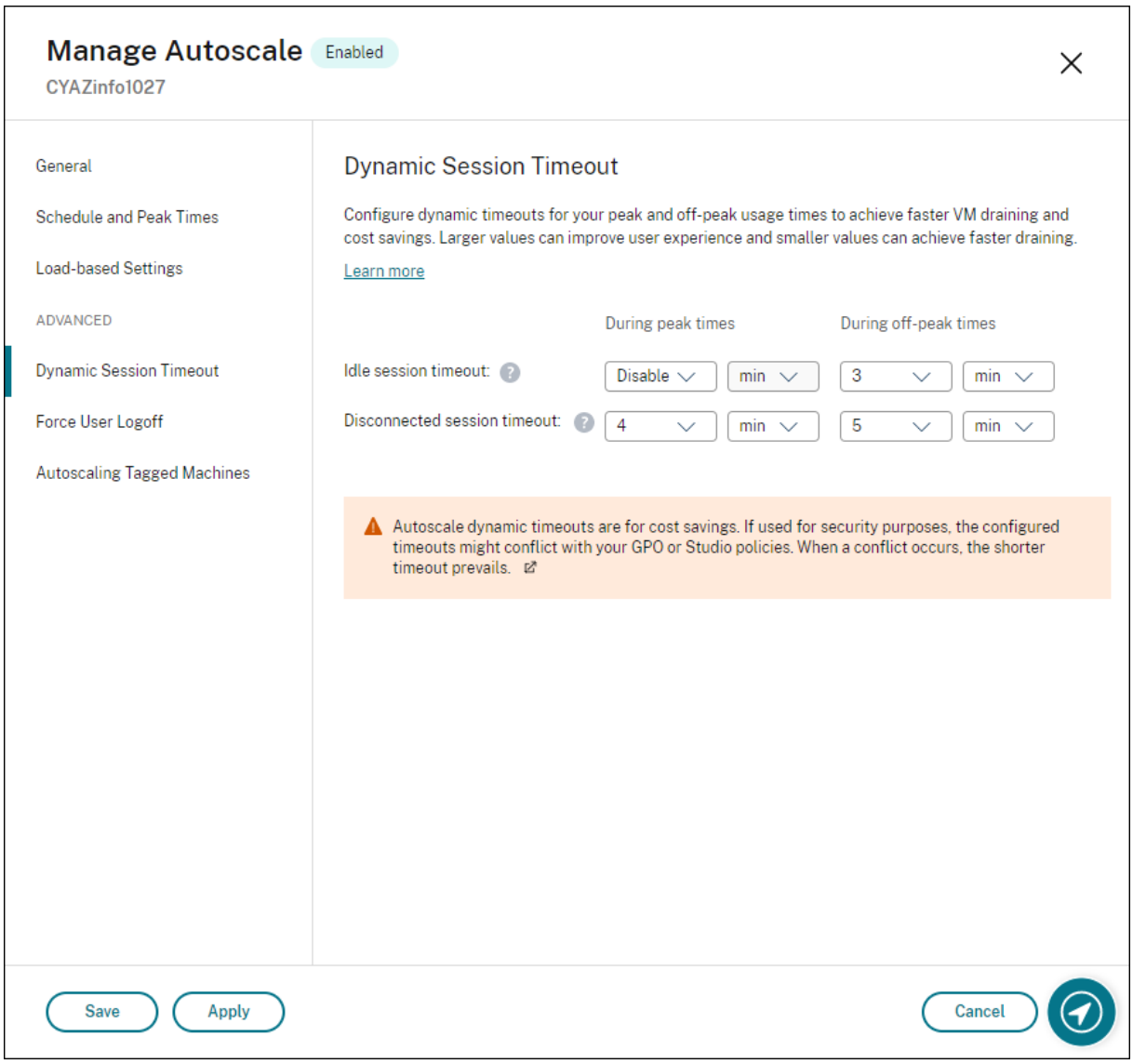
- Début du calendrier —09h00
  - Autoscale allume les machines M1 à M3.
  - Autoscale allume une machine supplémentaire (par exemple, M4) en raison du tampon de capacité configuré. La machine M4 n'est pas affectée.
- Un premier utilisateur ouvre une session
  - La première fois qu'un utilisateur ouvre 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

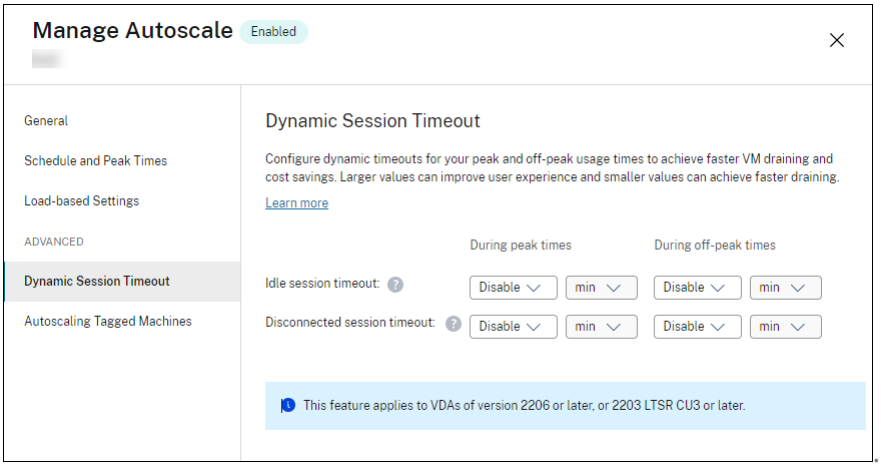
June 22, 2023

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 fonctionnalité n'est pas disponible, le message suivant apparaît sur l'interface utilisateur :



- 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)

March 8, 2023

> **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.

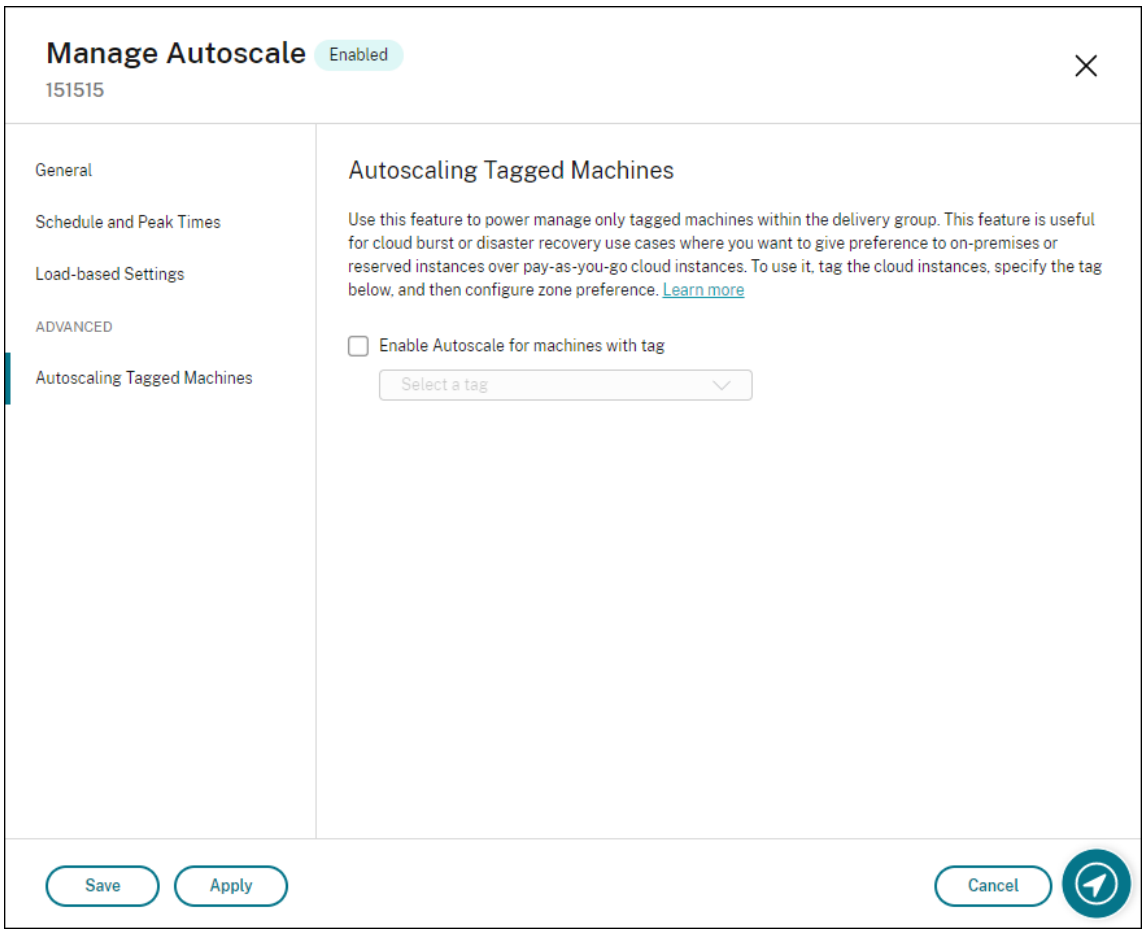
Pour activer Autoscale sur certaines machines balisées, vous pouvez utiliser la console Gérer ou PowerShell.

Utiliser la console Gérer pour activer Autoscale sur certaines machines balisées

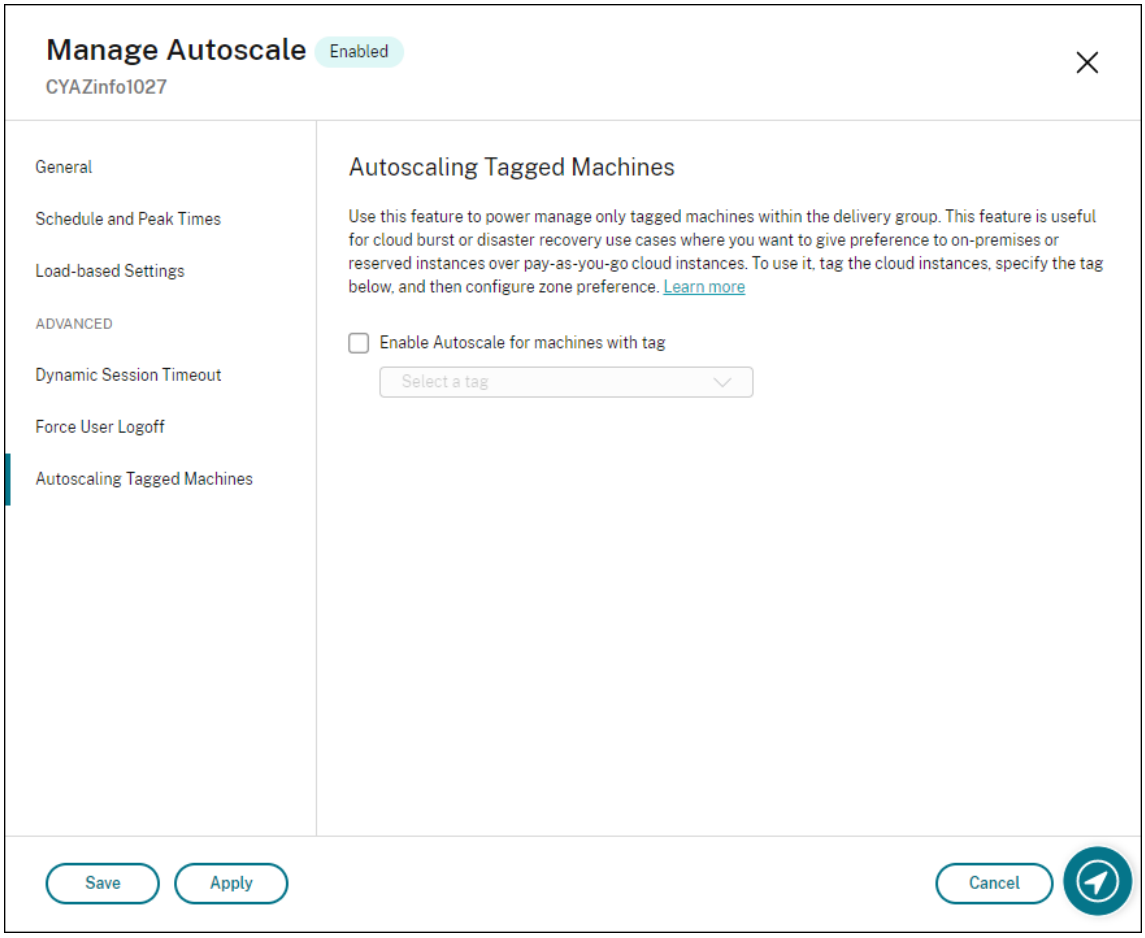
Pour activer Autoscale sur certaines machines balisées, procédez comme suit :

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,

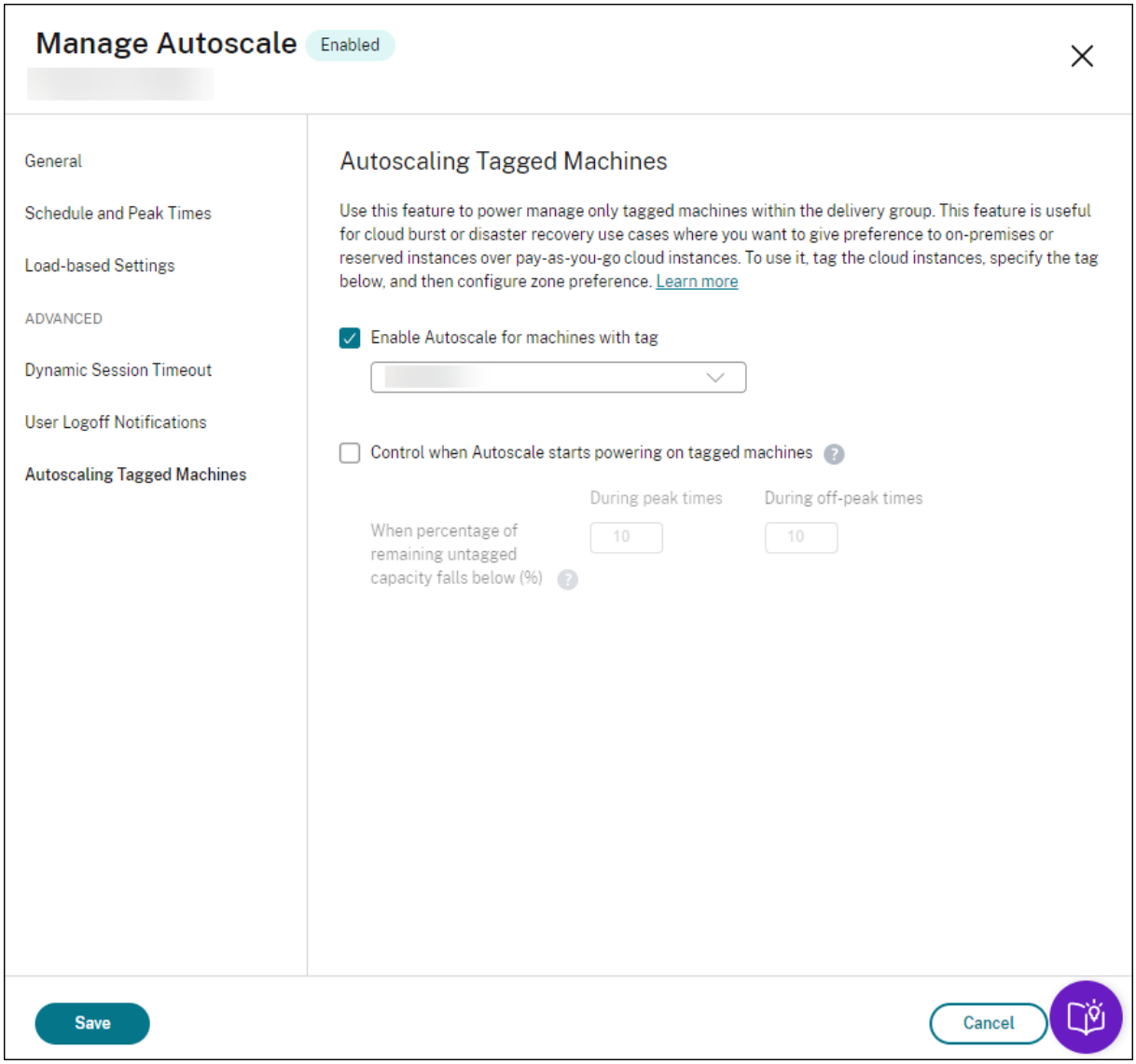
> il est possible qu'Autoscale n'ait plus de machines à gérer car la balise spécifiée dans Autoscale est devenue invalide. Pour effacer l'avertissement, accédez à la page **Autoscaling des machines balisées**, supprimez la balise non valide, puis cliquez sur **Appliquer** pour enregistrer vos modifications.

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.

Provisionner dynamiquement les machines

November 24, 2022

Autoscale permet de créer des machines et de les supprimer dynamiquement. Vous pouvez optimiser cette fonctionnalité en utilisant un script PowerShell. Le script vous permet d'augmenter ou de réduire dynamiquement le nombre de machines dans le groupe de mise à disposition en fonction des conditions de charge actuelles.

Le script offre les avantages suivants (et plus) :

- **Réduction des coûts de stockage**. Différent de la fonctionnalité Autoscale, qui contribue à réduire vos coûts informatiques, le script fournit une solution plus économique pour provisionner les machines.
- **Gestion efficace des changements de charge**. Le script vous aide à gérer les modifications de chargement en redimensionnant automatiquement le nombre de machines en fonction de la charge actuelle du groupe de mise à disposition.

Télécharger le script

Le script PowerShell est disponible à l'adresse https://github.com/citrix/Powershell-Scripts/tree/master/XAXD/AutoscaleMcs.

Fonctionnement du script

> **Important :**
>
> - Vous ne pouvez pas spécifier un même catalogue de machines dans plusieurs groupes de mise à disposition qui doivent être gérés par le script. En d'autres termes, si plusieurs groupes de mise à disposition partagent le même catalogue de machines, le script ne fonctionne avec aucun de ces groupes de mise à disposition.
> - Vous ne pouvez pas exécuter simultanément le script pour le même groupe de mise à disposition à partir de plusieurs emplacements.

Le script fonctionne au niveau du groupe de mise à disposition. Il mesure la charge (en utilisant l'indice de charge), puis détermine s'il faut créer ou supprimer des machines.

Les machines créées via ce script sont balisées de façon unique (via le paramètre `ScriptTag`) afin qu'elles puissent être identifiées ultérieurement. La création ou la suppression de machines repose sur les éléments suivants :

- **Pourcentage maximal de charge d'un groupe de mise à disposition**. Spécifie le niveau maximal auquel créer des machines pour Autoscale pour traiter des charges supplémentaires. Lorsque ce seuil est dépassé, les machines sont créées par lots pour s'assurer que la charge actuelle diminue jusqu'au seuil ou en dessous.
- **Pourcentage minimal de charge d'un groupe de mise à disposition**. Spécifie le niveau minimum auquel supprimer les machines créées via ce script qui n'ont pas de session active. Lorsque ce seuil est dépassé, les machines créées via ce script qui n'ont pas de session active sont supprimées.

Ce script est destiné à surveiller l'ensemble d'un groupe de mise à disposition et à créer ou supprimer des machines lorsque le critère de déclenchement est rempli. Il fonctionne par exécution. Cela signifie que vous devez exécuter le script régulièrement afin qu'il puisse fonctionner comme prévu. Nous vous recommandons d'exécuter le script à un intervalle minimum de cinq minutes. Cela améliore la réactivité globale.

Le script s'appuie sur les paramètres suivants pour fonctionner :

Paramètre	Type	Valeur par défaut	Description
DeliveryGroupName	Chaîne	X	Nom du groupe de mise à disposition à surveiller pour déterminer la charge actuelle. Vous pouvez fournir une liste de noms séparés par des points-virgules. Par exemple : `Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName 'dg1;dg2;dg3' -XdProfileName profile`.
XdProfileName	Chaîne	X	Nom du profil à utiliser pour l'authentification auprès de serveurs distants. Pour plus d'informations sur l'authentification auprès de serveurs distants à l'aide de ce paramètre, reportez-vous à la section API d'authentification.
HighWatermark	Nombre entier	80	Pourcentage maximal de charge (en termes d'indice de charge) auquel créer des machines pour Autoscale pour traiter des charges supplémentaires.

Paramètre	Type	Valeur par défaut	Description
LowWatermark	Nombre entier	15	Pourcentage minimal de charge (en termes d'indice de charge) auquel supprimer des machines créées par ce script qui n'ont pas de session active.
MachineCatalogName	Chaîne	X	Nom du catalogue de machines dans lequel les machines doivent être créées.
MaximumCreatedMachines	Nombre entier	-1	Nombre maximal de machines pouvant être créées dans un groupe de mise à disposition spécifié. Si la valeur est égale ou inférieure à 0, le script ne traite pas ce paramètre.
ScriptTag	Chaîne	AutoscaledScripted	Balise qui s'applique aux machines créées via le script.
EventLogSource	Chaîne	X	Nom de source qui apparaît dans l'Observateur d'événements Windows.

> **Remarque :**
>
> Un « X » indique qu'aucune valeur par défaut n'est spécifiée pour ce paramètre.

Par défaut, le script requiert tous les paramètres (sauf le paramètre `ScriptTag`) la première fois qu'il s'exécute. Lors des exécutions suivantes, seuls les paramètres `DeliveryGroupName` et `XdProfileName` sont requis. Le cas échéant, vous pouvez choisir de mettre à jour les charges minimales et maximales en pourcentage.

Notez que vous devez spécifier un seul groupe de mise à disposition la première fois que vous exécutez le script. Par exemple, le script ne fonctionne *pas* si vous utilisez la commande PowerShell suivante pour spécifier deux groupes de mise à disposition la première fois que vous exécutez le script :

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1; dg2'-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

Au lieu de cela, spécifiez d'abord un seul groupe de mise à disposition (dans cet exemple, dg1) à l'aide de la commande suivante :

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1 '-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

Ensuite, utilisez la commande suivante pour exécuter le script pour le deuxième groupe de mise à disposition (dans cet exemple, dg 2) :

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2' -XdProfileName profile`

Conditions préalables

Pour exécuter le script, assurez-vous que les conditions préalables suivantes sont remplies :

- La machine réside dans le domaine où les machines sont créées.
- Le SDK PowerShell distant est installé sur cette machine. Pour plus d'informations sur le SDK Remote PowerShell, reportez-vous à la section SDK et API.
- Autres conditions préalables :
  - Un groupe de mise à disposition pour la surveillance
  - Un catalogue de machines créé via Machine Creation Services (MCS) qui a un schéma de provisioning associé (modèle)
  - Un pool d'identités associé au schéma de provisioning
  - Une source de journal d'événements afin que le script puisse écrire des informations dans le journal des événements Windows
  - Un client sécurisé qui vous permet de vous authentifier auprès de serveurs distants

Autorisations, recommandations et avis

Lorsque vous exécutez le script :

- Pour vous authentifier auprès de serveurs distants à l'aide du paramètre `XdProfileName`, vous devez définir un profil d'authentification à l'aide d'un client sécurisé d'accès API, créé dans la console Citrix Cloud. Pour plus de détails, consultez API d'authentification.

- Vous devez disposer d'autorisations pour créer et supprimer des comptes de machine dans Active Directory.
- Nous vous recommandons d'automatiser le script PowerShell avec le Planificateur de tâches Windows. Pour plus de détails, consultez Créer une tâche automatisée à l'aide du Planificateur de tâches Windows.
- Si vous souhaitez que le script écrive des informations (par exemple, échecs et actions) dans le journal des événements Windows, vous devez d'abord spécifier un nom de source à l'aide de l'applet de commande `New-EventLog`. Par exemple, `New-EventLog -LogName Application –Source <sourceName>`. Vous pouvez alors afficher les événements dans le volet **Application** de l'Observateur d'événements Windows.
- Si des erreurs se sont produites pendant l'exécution du script, exécutez le script manuellement, puis résolvez les problèmes en effectuant des vérifications de script.

API d'authentification

Avant d'exécuter le script, vous devez définir un profil d'authentification à l'aide d'un client sécurisé d'accès API. Vous devez créer un client sécurisé en utilisant le compte sous lequel le script sera exécuté.

Le client sécurisé doit disposer des autorisations suivantes :

- Créer et supprimer des machines à l'aide de MCS.
- Modifier les catalogues de machines (pour ajouter et supprimer des machines).
- Modifier les groupes de mise à disposition (pour ajouter et supprimer des machines).

Lorsque vous créez un client sécurisé, assurez-vous que votre compte dispose des autorisations ci-dessus car le client sécurisé hérite automatiquement des autorisations de votre compte actuel.

Pour créer un client sécurisé, procédez comme suit :

1. Connectez-vous à Citrix Cloud, puis accédez à **Gestion des identités et des accès > Accès aux API**.
2. Tapez le nom de votre client sécurisé, puis cliquez sur **Créer un client**.

Pour vous authentifier auprès de serveurs distants, utilisez la commande PowerShell `Set-XDCredentials`. Par exemple :

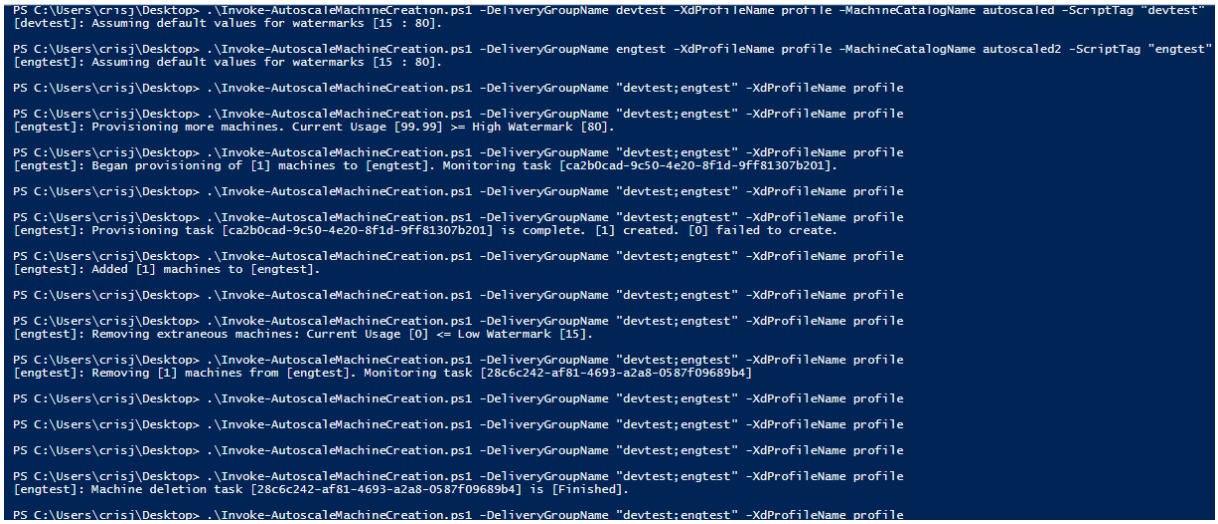
- `Set-XDCredentials -APIKey <key_id> -CustomerId <customer_id> -SecretKey <secret_key> -StoreAs <name specified by the XdProfileName parameter>`

Créer une tâche automatisée à l'aide du Planificateur de tâches Windows

Vous pouvez automatiser le script PowerShell avec le Planificateur de tâches Windows. Cela permet au script de s'exécuter automatiquement à certains intervalles ou lorsque certaines conditions sont remplies. Pour exécuter ce script avec le Planificateur de tâches Windows, veillez à sélectionner **Ne pas démarrer une nouvelle instance** dans l'onglet **Créer une tâche > Paramètres**. Cela empêche le Planificateur de tâches Windows d'exécuter une nouvelle instance du script si le script est déjà en cours d'exécution.

Exemple d'exécution du script

Vous trouverez ci-dessous un exemple d'exécution du script. Notez que le fichier de script est appelé plusieurs fois. Dans cet exemple, pour simuler la charge, une session est lancée, puis terminée.



Liste de vérification de dépannage pour le script

Le script écrit des informations (par exemple, des erreurs et des actions) dans le journal des événements Windows. Ces informations vous aident à résoudre les problèmes que vous rencontrez lors de l'exécution du script. La liste de vérification de dépannage suivante peut être utile :

- Échec de communication avec les serveurs distants. Actions possibles :
  - Vérifiez votre connexion au serveur.
  - Vérifiez que la clé API que vous utilisez est valide.
- Échec de la création de machines. Actions possibles :
  - Vérifiez que le compte d'utilisateur exécutant le script dispose d'autorisations suffisantes pour créer des comptes d'utilisateur dans le domaine.

  - Vérifiez que l'utilisateur qui a créé la clé API dispose d'autorisations suffisantes pour utiliser MCS pour provisionner des machines.
  - Vérifiez la validité du catalogue de machines (c'est-à-dire que son image existe toujours et est en bon état).

- Échec d'ajout de machines à un catalogue de machines ou à un groupe de mise à disposition. Action possible :

  - Vérifiez que l'utilisateur qui a créé la clé API dispose d'autorisations suffisantes pour ajouter et supprimer des machines dans et depuis des catalogues de machines et des groupes de mise à disposition.

Notifications de fermeture de session utilisateur (anciennement Forcer fermeture de la session utilisateur)

June 8, 2023

> **Important :**
>
> Cette fonction est disponible uniquement dans l'interface utilisateur Autoscale pour les groupes de mise à disposition multi-session basés sur les applications.

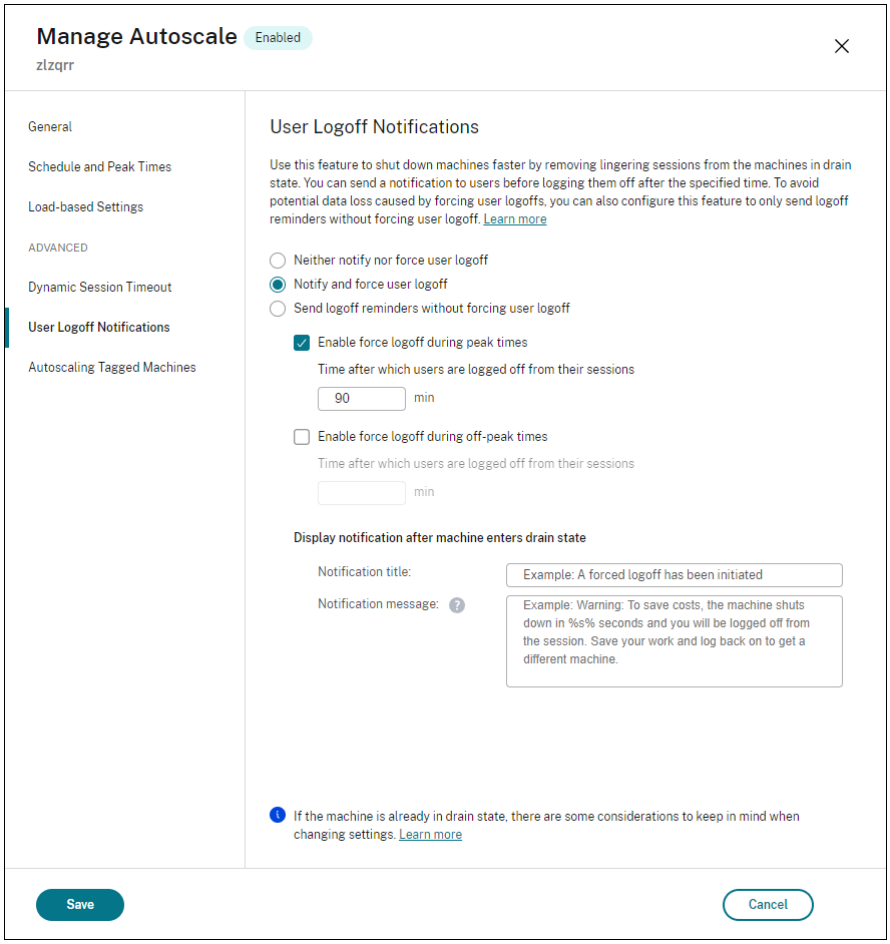
Pour optimiser les économies, la fonction Autoscale vous permet de forcer la fermeture des sessions persistantes. Cette procédure vous permet d'envoyer une notification personnalisée aux utilisateurs, ainsi qu'une période de grâce après laquelle les sessions sont forcées à être déconnectées. Cette procédure 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 options suivantes :

- **Notifier et forcer fermeture de la session utilisateur**
- **Envoyer des rappels de fermeture de session sans forcer l'utilisateur à se déconnecter**
- **Ne pas notifier ni forcer fermeture de la session utilisateur**

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.

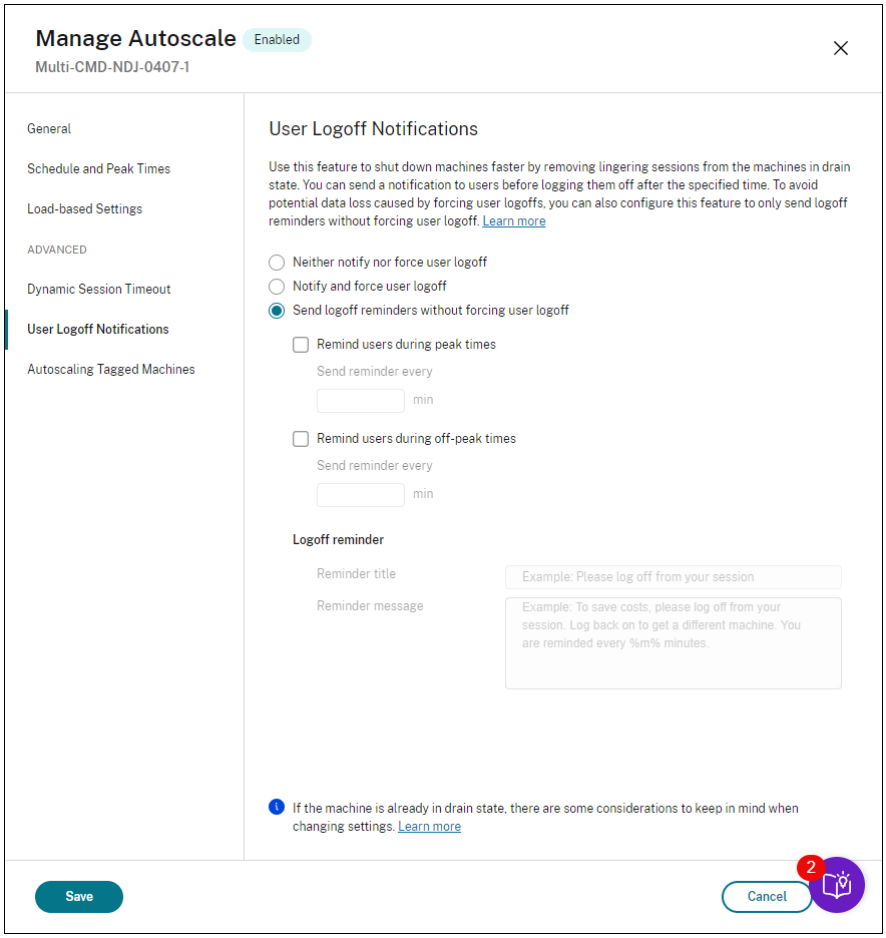
Activer déconnexion forcée pendant les heures creuses. Si cette option est sélectionnée, Autoscale déconnecte ces utilisateurs de leurs sessions pendant les heures creuses lorsque le délai spécifié s'est écoulé.

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.
```

Ne pas notifier ni forcer fermeture de la session utilisateur

Si cette option est sélectionnée, Autoscale ne force pas les utilisateurs à se déconnecter des machines en état de drainage et ne les invite pas à passer manuellement à une autre machine.

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.

Analyser l'efficacité des paramètres Autoscale

February 21, 2024

Pour utiliser cette fonctionnalité, activez l'option **Insights sur Autoscale** dans **DaaS > Accueil > Fonctionnalités préliminaires**. L'affichage de l'option **Insights sur Autoscale** après son activation peut prendre environ 15 minutes.

Vous pouvez analyser l'efficacité des paramètres Autoscale en fonction de l'utilisation de la machine au cours de la semaine précédente. Grâce à l'analyse, vous pouvez obtenir les informations suivantes sur l'efficacité des paramètres Autoscale :

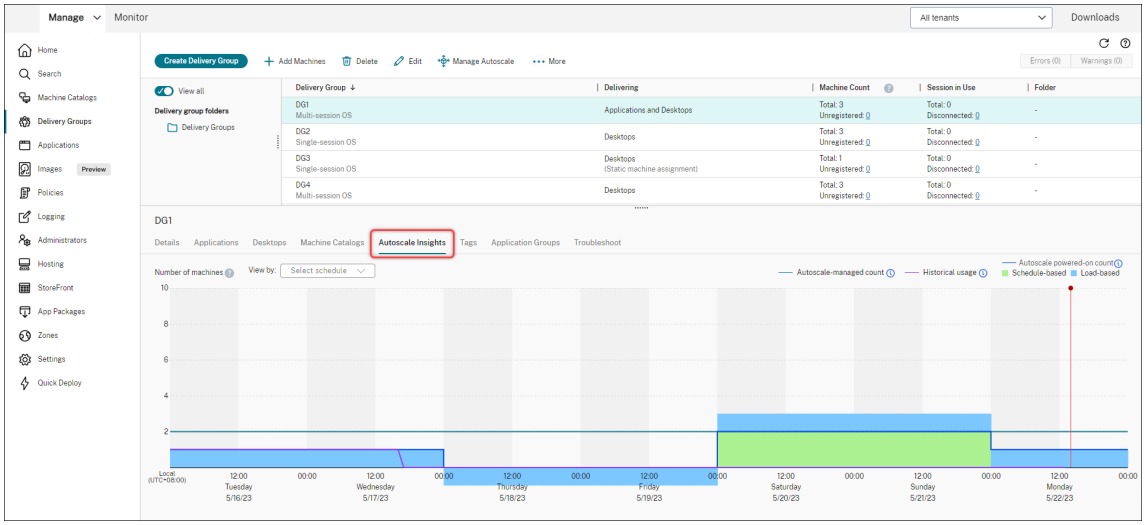
- Identifiez le gaspillage financier résultant d'un provisioning excessif.
- Déterminez si un provisioning insuffisant a un impact négatif sur l'expérience utilisateur.
- Assurez-vous que la capacité allouée est correctement alignée sur l'utilisation de la machine.

Pour atteindre cet objectif, procédez comme suit :

1. Sélectionnez un groupe de mise à disposition pour lequel AutoScale est activé.

2. Dans le volet inférieur, cliquez sur l'onglet **Insights sur Autoscale**.

   Le graphique suivant apparaît, montrant la comparaison entre les données d'utilisation des machines de la semaine précédente et le nombre de machines à mettre sous tension en fonction des paramètres Autoscale.



* La ligne verticale rouge indique l'heure actuelle.

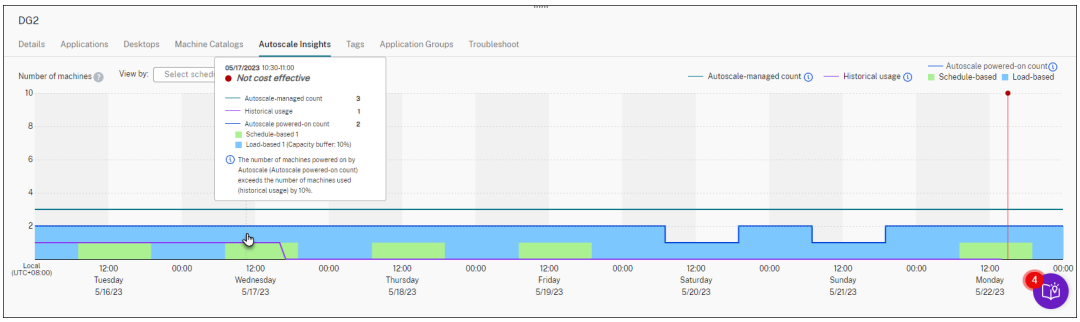
Le tableau suivant décrit les mesures présentées dans ce graphique.

Métrique	Description
Nombre géré par AutoScale	Nombre total de machines gérées par Autoscale. Nombre géré par Autoscale = Nombre total de machines dans le groupe de mise à disposition —Nombre de machines en mode maintenance —Nombre de machines non balisées pour Autoscale (si la fonction de balisage pour Autoscale est activée).
Nombre de machines alimentées par Autoscale	Nombre total de machines alimentées par Autoscale. Nombre de machines alimentées par Autoscale = Nombre de machines basé sur le calendrier + Nombre de machines basé sur la charge.
Utilisation historique	Nombre de machines mises à disposition des utilisateurs.

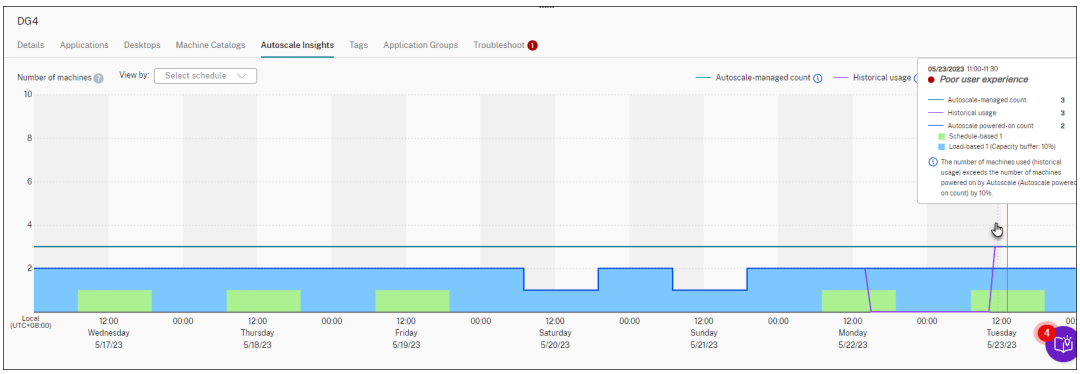
Métrique	Description
Basé sur le calendrier	Nombre de machines mises sous tension en fonction des paramètres basés sur le calendrier Autoscale (**Remarque :** les paramètres basés sur le calendrier ne s'appliquent pas aux groupes de mise à disposition du type OS mono-session statique).
Basé sur la charge	Nombre de machines alimentées en fonction des paramètres basés sur la charge d'Autoscale.

3. Pour vérifier l'efficacité des paramètres Autoscale à un intervalle de temps spécifique, passez votre souris sur ce créneau sur le graphique. Une boîte d'information apparaît, affichant les résultats de la comparaison et le nombre détaillé de machines :

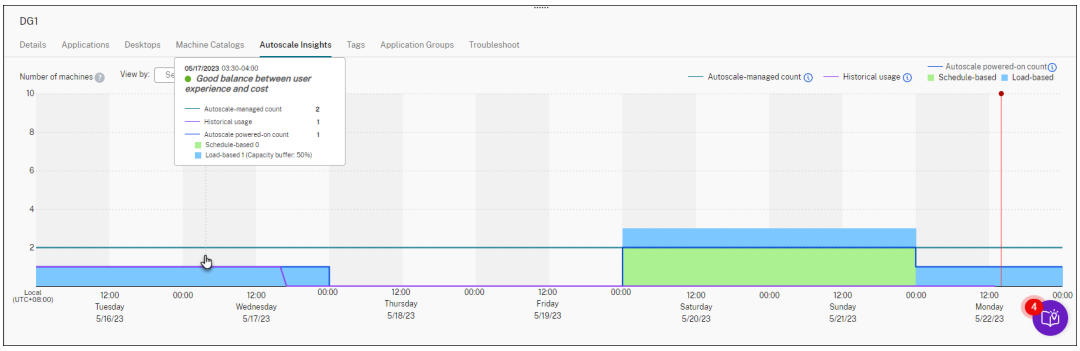
   - **Non rentable**. L'utilisation historique est inférieure à 90 % des paramètres Autoscale (nombre de mises sous tension Autoscale). Par conséquent, il peut y avoir un gaspillage de capacité.



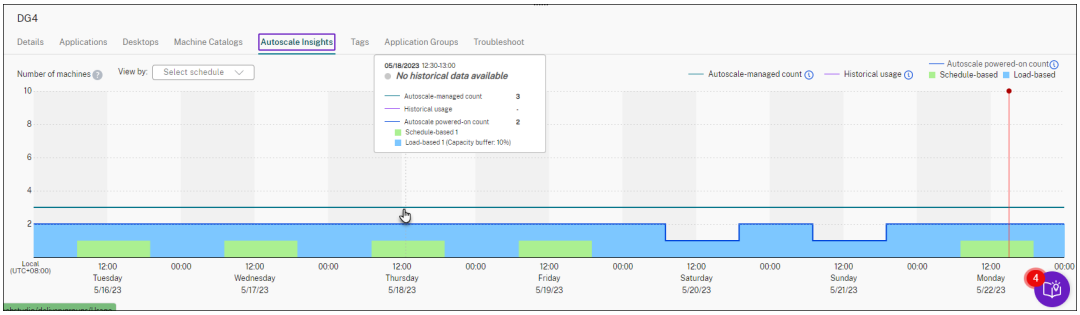
   - **Mauvaise expérience utilisateur**. L'utilisation historique est supérieure à 110 % des paramètres Autoscale (nombre de mises sous tension Autoscale). Par conséquent, les utilisateurs peuvent être confrontés à des temps d'attente plus longs avant la mise en marche des machines.



- **Bon équilibre entre expérience utilisateur et coût**. La différence entre l'utilisation historique et les paramètres Autoscale (nombre de mises sous tension Autoscale) est inférieure à 10 %. Les paramètres Autoscale sont alignés sur l'historique d'utilisation.



- **Aucune donnée historique disponible**. Aucune donnée historique n'est disponible. Les causes possibles incluent le fait qu'Autoscale a été activé pour le groupe de mise à disposition il y a moins d'une semaine.



4. Pour mettre en évidence une plage de dates en fonction d'un calendrier Autoscale, sélectionnez le calendrier dans le champ **Afficher par**.
5. Ajustez les paramètres Autoscale en fonction de votre analyse. Pour plus d'informations, voir Paramètres basés sur le calendrier et sur la charge.

Commandes SDK PowerShell de Broker

November 24, 2023

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 Remote PowerShell SDK version 7.21.0.12 ou ultérieure. Pour plus d'informations sur le SDK Remote PowerShell, reportez-vous à la section 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 ».

Vérification de l'état du cloud

December 9, 2022

> **Remarque :**
>
> L'application Vérification de l'état du cloud est intégrée à Citrix DaaS. L'intégration est disponible sous la forme de l'action Exécuter vérification de l'état dans l'interface de gestion Configuration complète. Pour plus d'informations, consultez Dépanner les problèmes d'enregistrement et de lancement de session VDA.

L'application Vérification de l'état du cloud vous permet d'exécuter des vérifications qui évaluent l'état de santé et la disponibilité du site et de ses composants. Vous pouvez exécuter des vérifications pour Virtual Delivery Agents (VDA), les serveurs StoreFront et Profile Management. Les vérifications de l'état du VDA identifient les causes possibles des problèmes courants d'enregistrement de VDA et de lancement de session.

Si des problèmes sont détectés pendant les vérifications, la vérification de l'état du cloud fournit un rapport détaillé et les actions pouvant résoudre les problèmes. Chaque fois que la vérification de l'état du cloud démarre, il recherche la dernière version des scripts sur le CDN (Content Delivery Network) et télécharge automatiquement les scripts s'ils n'existent pas sur l'ordinateur local. La vérification de l'état du cloud choisit toujours la dernière version locale des scripts pour exécuter des contrôles d'intégrité.

> **Remarque :**
>
> La vérification de l'état du cloud ne se met pas à jour chaque fois qu'elle s'exécute.

Dans un environnement Citrix Cloud, exécutez Vérification de l'état du cloud à partir d'une machine jointe au domaine pour exécuter des vérifications sur un ou plusieurs VDA ou serveurs StoreFront.

> **Remarque :**
>
> Vous ne pouvez pas installer ou exécuter Vérification de l'état du cloud sur un Cloud Connector.

Le journal de l'application Vérification de l'état du cloud est stocké dans `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`. Vous pouvez utiliser ce fichier pour le dépannage.

Consultez une présentation de Vérification de l'état du cloud.

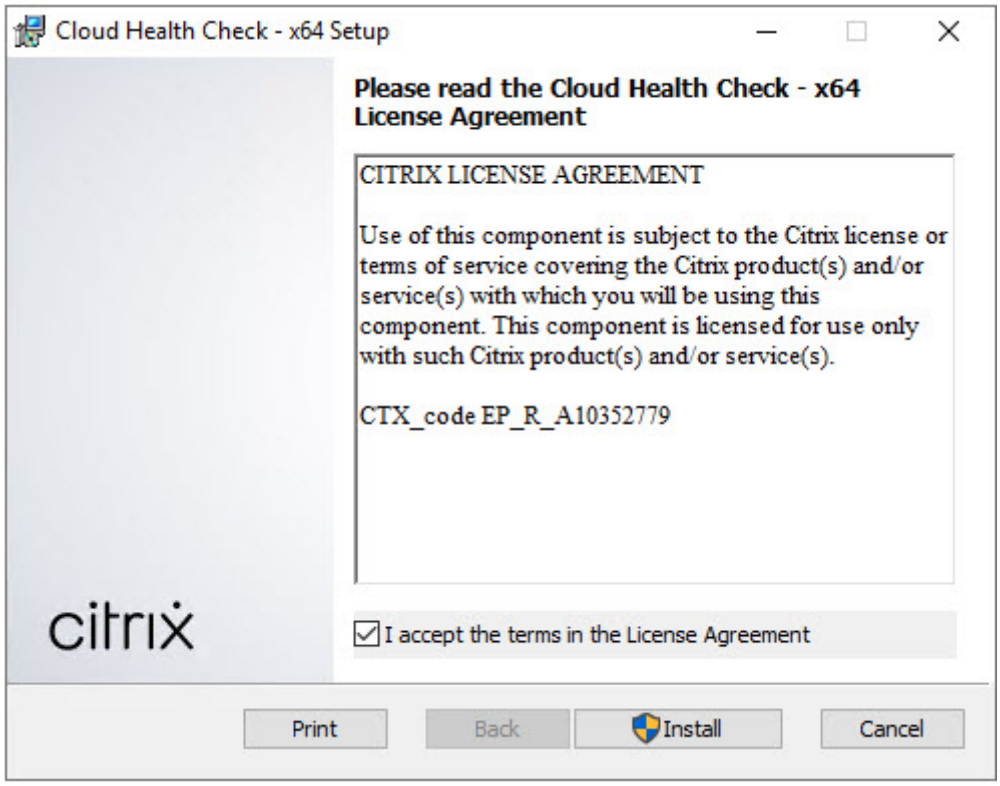
Apprenez quand utiliser Vérification de l'état du cloud.

Installation

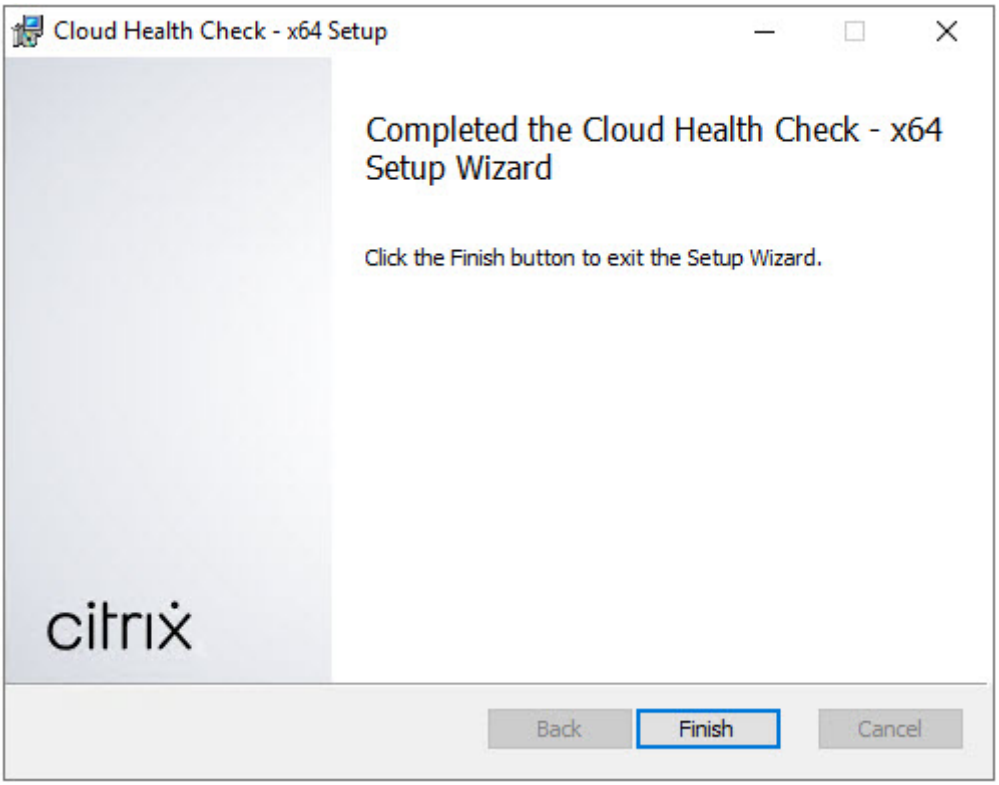
Pour préparer votre environnement pour l'installation de l'application Vérification de l'état du cloud, vous devez disposer d'une machine Windows rattachée au domaine.

> **Remarque :**
>
> Vous ne pouvez pas installer ou exécuter Vérification de l'état du cloud sur Cloud Connector.

1. Sur l'ordinateur joint au domaine, téléchargez le programme d'installation d'Analyse de l'état de santé du cloud.
2. Double-cliquez sur le fichier CloudHealthCheckInstaller_x64.msi.
3. Cliquez sur la case pour accepter les conditions.
4. Cliquez sur Installer.



5. Une fois l'installation terminée, cliquez sur **Terminer**.



Autorisations et conditions requises

Autorisations :

- 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 autorisations d'exécution de scripts peuvent également fonctionner.
- Utilisez **Exécuter en tant qu'administrateur** lorsque vous lancez la vérification de l'état du cloud.

Pour chaque machine VDA ou StoreFront sur laquelle vous exécutez des vérifications :

- Le système d'exploitation doit être de 64 bits.
- La vérification de l'état du cloud 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.
- L'accès WMI (Windows Management Infrastructure) doit être activé sur la machine.

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\`.

Vérifications d'état de santé du VDA

Pour l'enregistrement sur le VDA, la vérification de l'état du cloud 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 de l'enregistrement de VDA

Pour les lancements de session sur les VDA, la vérification de l'état du cloud vérifie :

- Disponibilité du port de communication de lancement de session
- État des services de lancement de session
- 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
- État du pilote CTXUVI

Pour Profile Management sur les VDA, la vérification de l'état du cloud 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

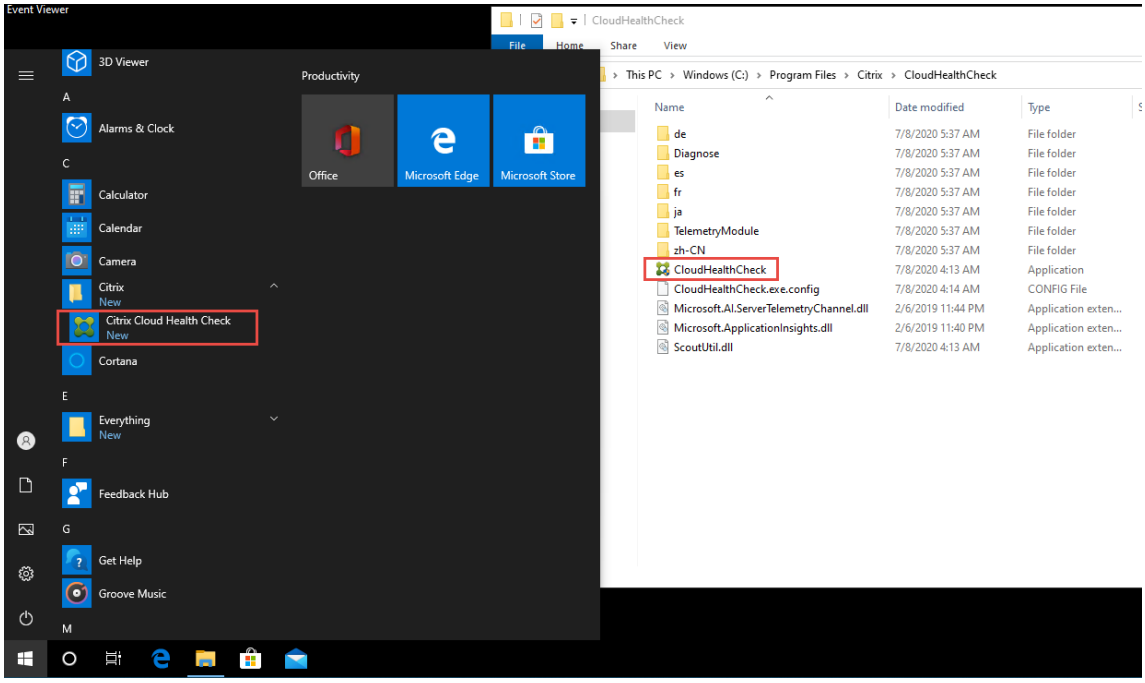
Les contrôles StoreFront vérifient si :

- Le service de domaine par défaut Citrix est en cours d'exécution
- Le service Citrix Credential Wallet est en cours d'exécution
- la connexion du serveur StoreFront à Active Directory s'effectue via le port 88 ;
- la connexion du serveur StoreFront à Active Directory s'effectue via le port 389 ;
- la connexion du serveur StoreFront à Active Directory s'effectue via le port 464 ;
- 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 certificats est complète ;
- les certificats ont expiré ;
- un certificat expire dans les 30 jours.

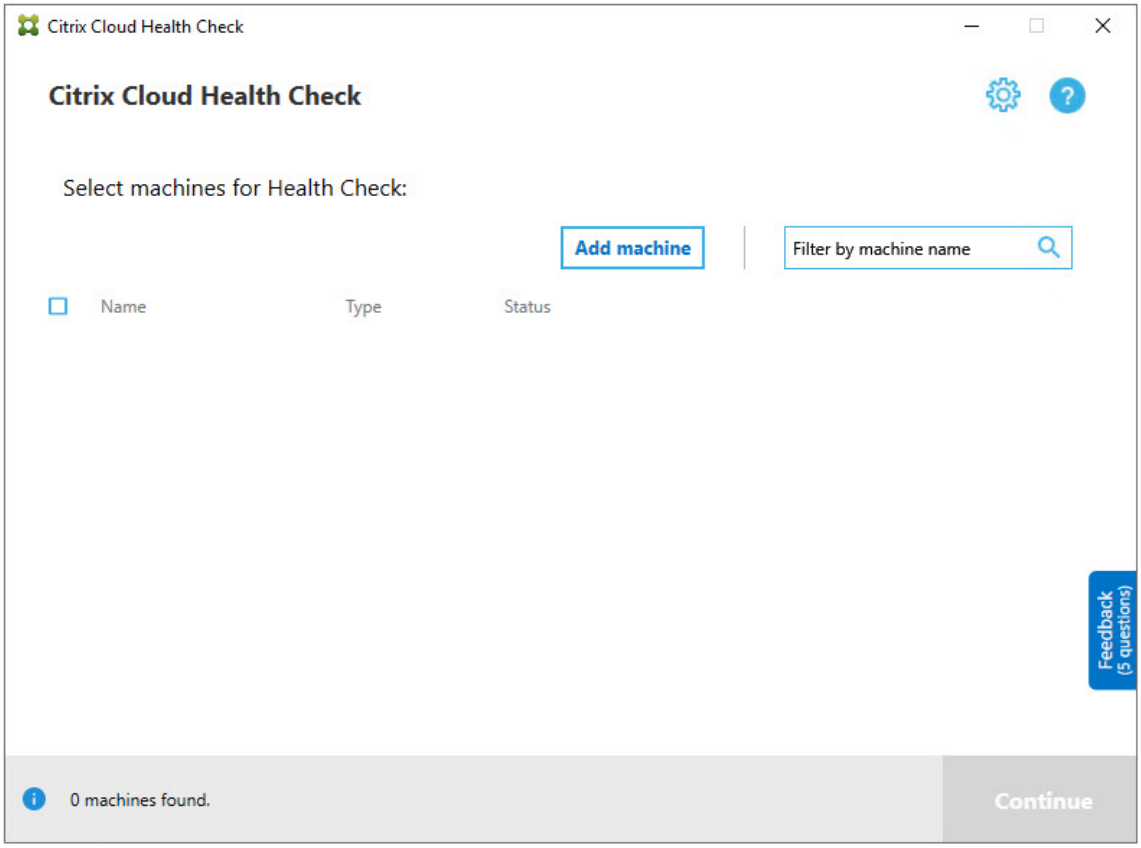
Exécution de Vérification de l'état du cloud

Pour exécuter la vérification de l'état du cloud :

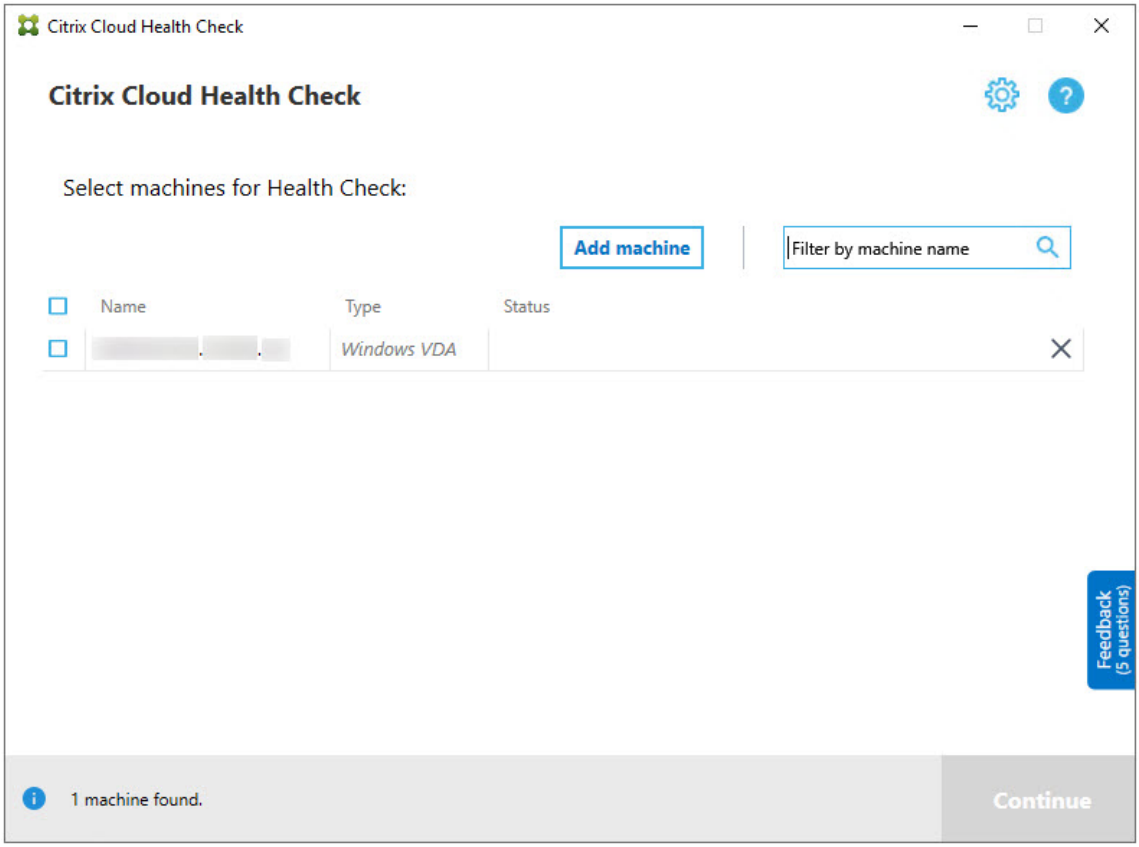
1. Sélectionnez **Citrix > Vérification de l'état du cloud** dans le menu Démarrer de la machine, ou exécutez `CloudHealthCheck.exe` dans `C:\Program Files\Citrix\CloudHealthCheck`.



2. Dans l'écran principal de Vérification de l'état du cloud, cliquez sur **Ajouter une machine**.



3. Tapez le nom de domaine complet de la machine à ajouter. **Remarque :** bien que la saisie d'un alias DNS au lieu d'un nom de domaine complet puisse paraître valide, les vérifications peuvent échouer.
4. Cliquez sur **Continuer**.
5. Répétez cette opération pour ajouter d'autres machines, si nécessaire.



6. Pour supprimer une machine ajoutée manuellement, cliquez sur le **X** à droite de la ligne et confirmez la suppression. Répétez cette opération pour supprimer d'autres machines ajoutées manuellement.

L'application Vérification de l'état du cloud se souvient des machines ajoutées manuellement jusqu'à ce que vous les supprimez. Lorsque vous fermez puis rouvrez Vérification de l'état du cloud, les machines ajoutées manuellement sont toujours répertoriées en haut de la liste.

Importer des machines VDA

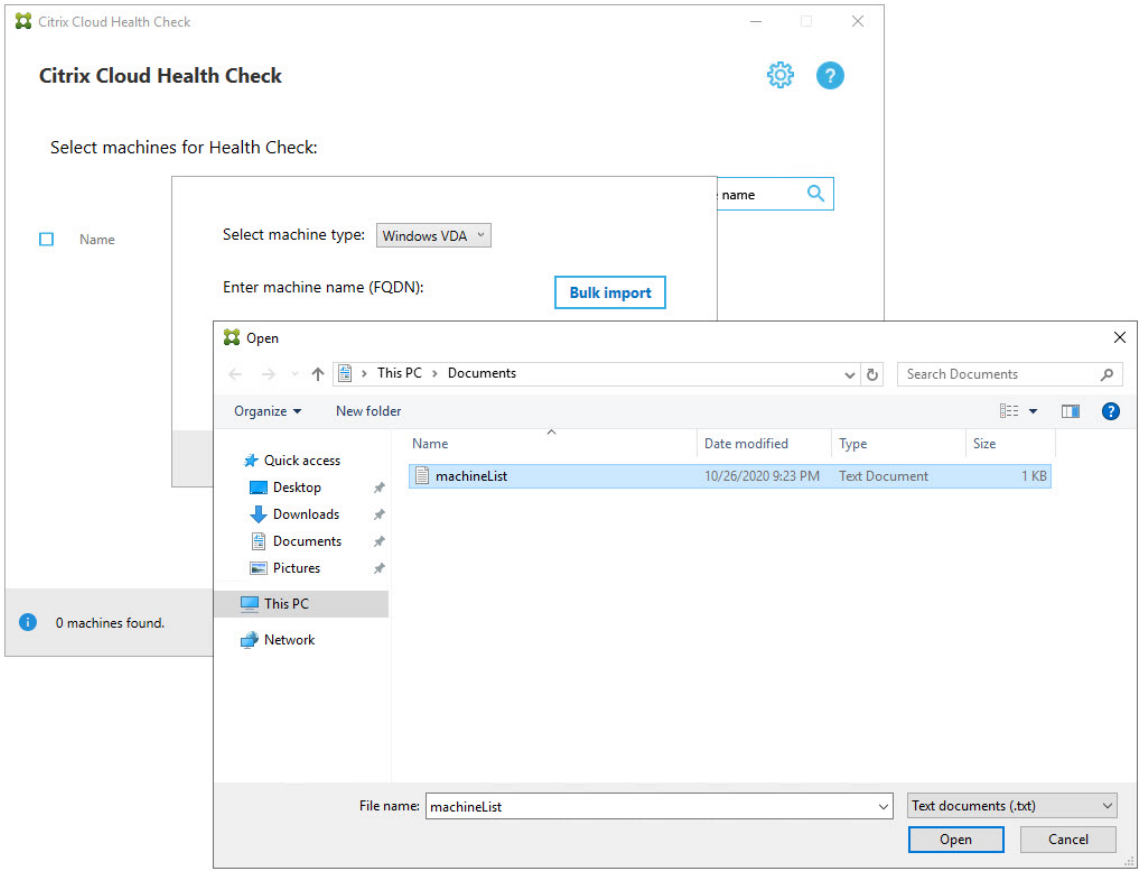
Vous pouvez importer des machines VDA dans le déploiement lors de l'exécution des vérifications.

1. Sur le Connector, générez le fichier de liste de machines à l'aide de la commande PowerShell suivante. 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
```

1. Copiez le fichier machineList.txt sur la machine jointe au domaine sur laquelle vous souhaitez exécuter Vérification de l'état du cloud.

2. Sur la page Vérification de l'état du cloud, cliquez sur **Ajouter une machine**.
3. Sélectionnez le type de machine VDA Windows.
4. Cliquez sur **Importer des machines VDA**.
5. Sélectionnez le fichier machineList.txt.
6. Cliquez sur **Ouvrir**.



Les machines VDA importées sont répertoriées sur la page Vérification de l'état du cloud.

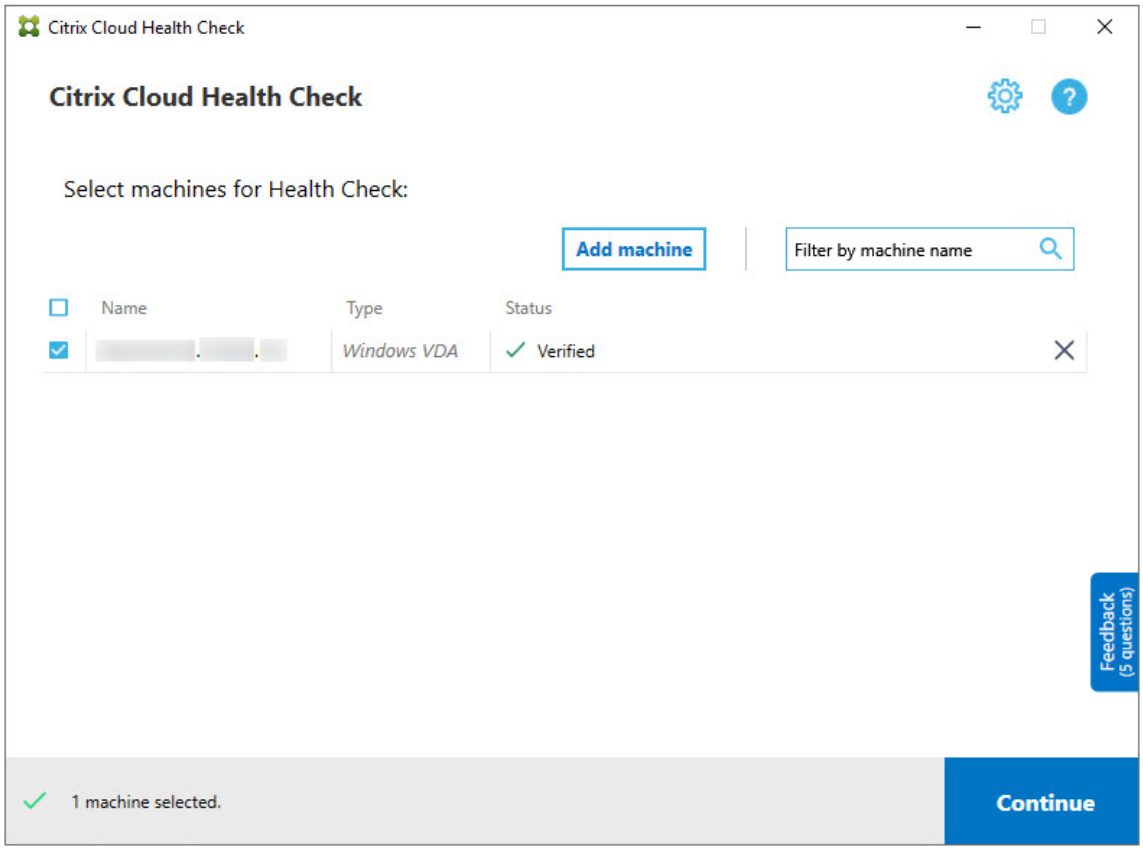
7. Activez la case à cocher en regard de chaque machine sur laquelle vous souhaitez exécuter des vérifications.

   La vérification de l'état du cloud démarre automatiquement des tests de vérification sur chaque machine que vous avez sélectionnée, s'assurant ainsi que celle-ci remplit les critères répertoriés dans les 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 alors :

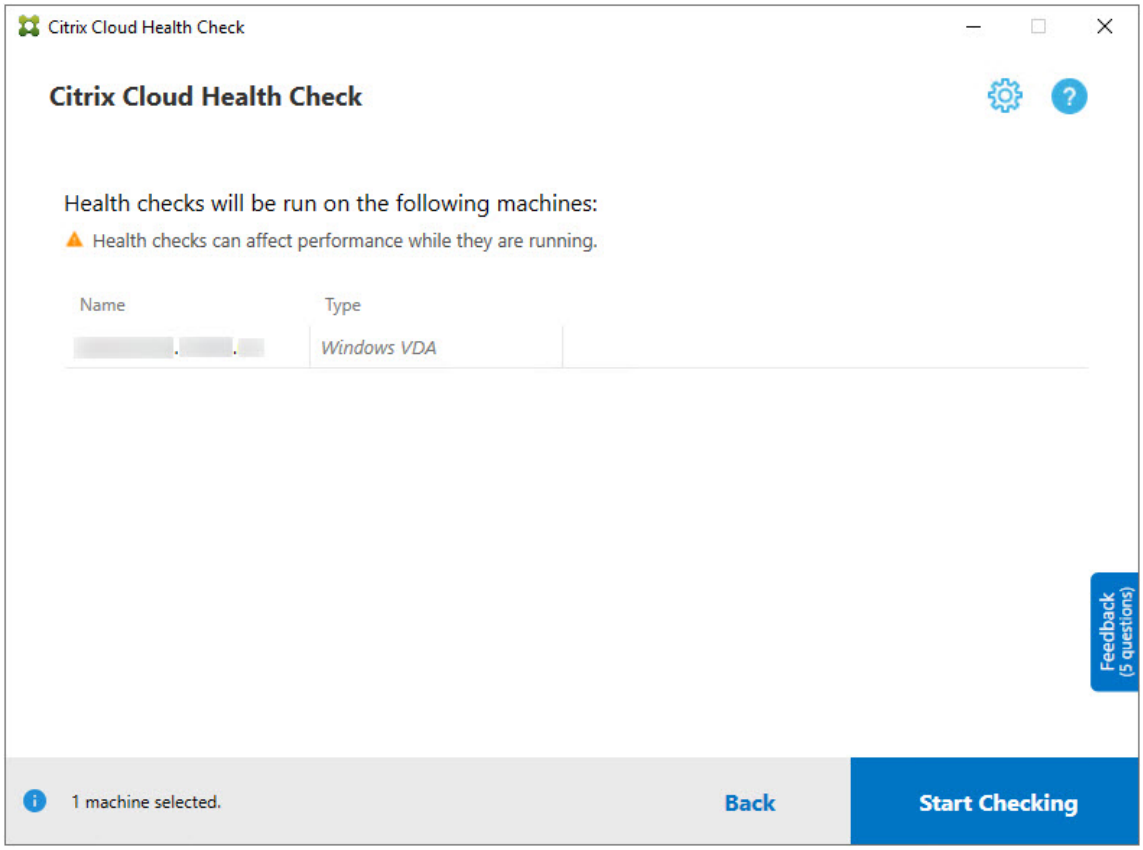
   - Corriger le problème, puis sélectionner de nouveau la case à cocher de la machine. Cela déclenche une nouvelle tentative de tests de vérification.

- Ignorer cette machine (en laissant la case à cocher non sélectionnée). Les vérifications ne seront pas exécutées pour cette machine.

8. Une fois les tests de vérification terminés, cliquez sur **Continuer**.

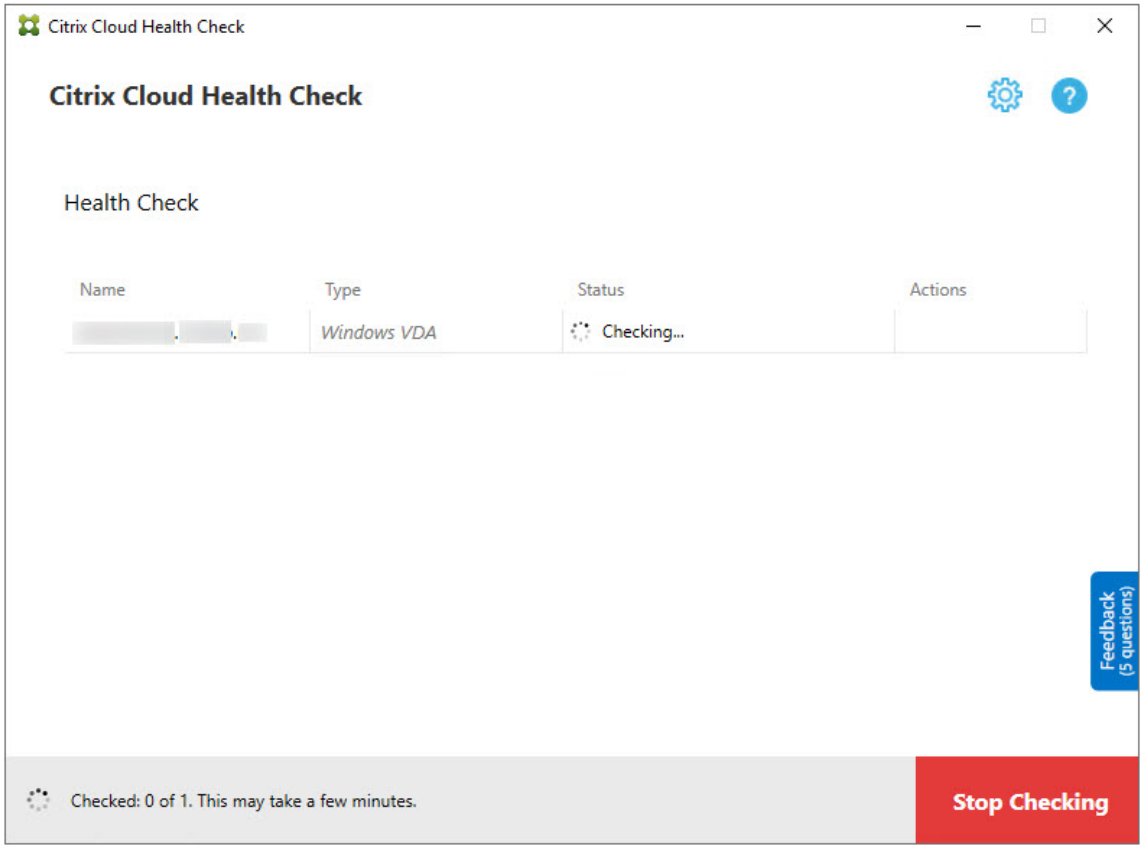


9. Exécuter les vérifications de l'état de santé sur les machines sélectionnées. Le résumé répertorie les machines sur lesquelles les tests sont exécutés (les machines que vous avez sélectionnées et qui ont réussi les tests de vérification).
10. Cliquez sur **Démarrer la vérification**.

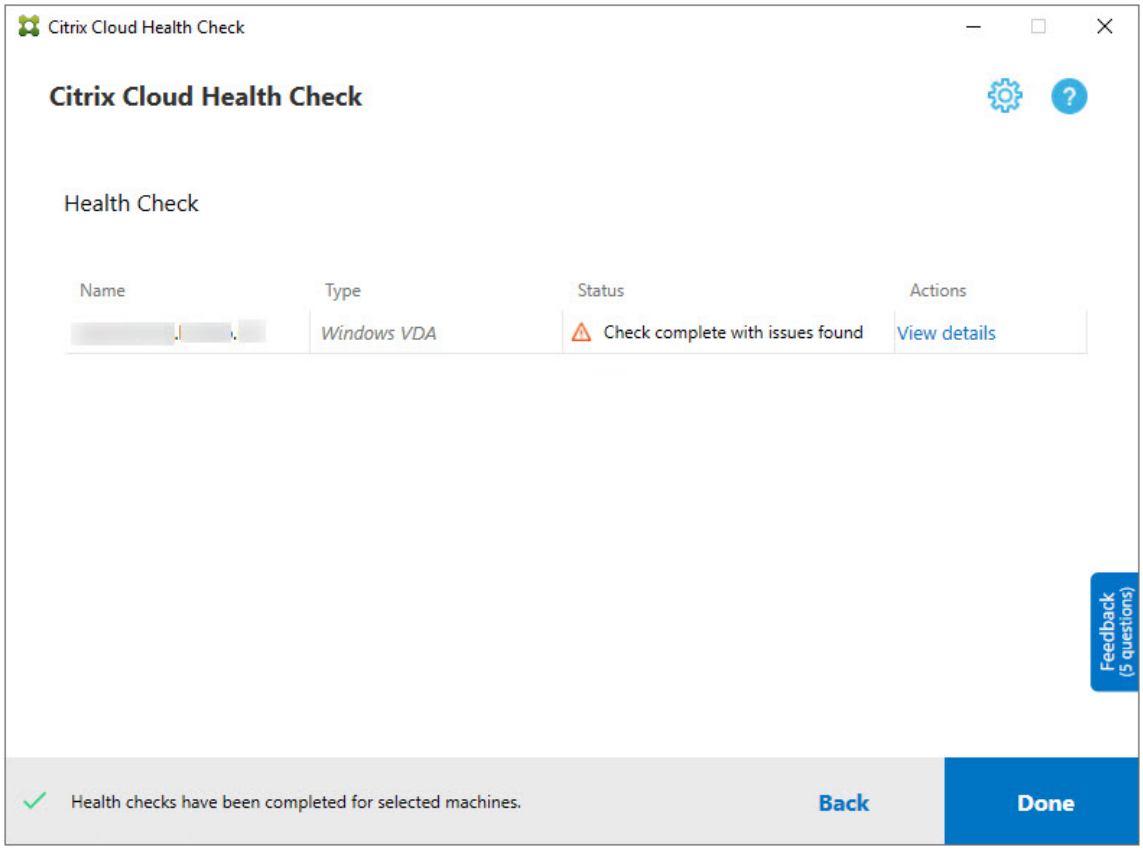


Pendant et après la vérification, la colonne **État** indique l'état de vérification actuel d'une machine.

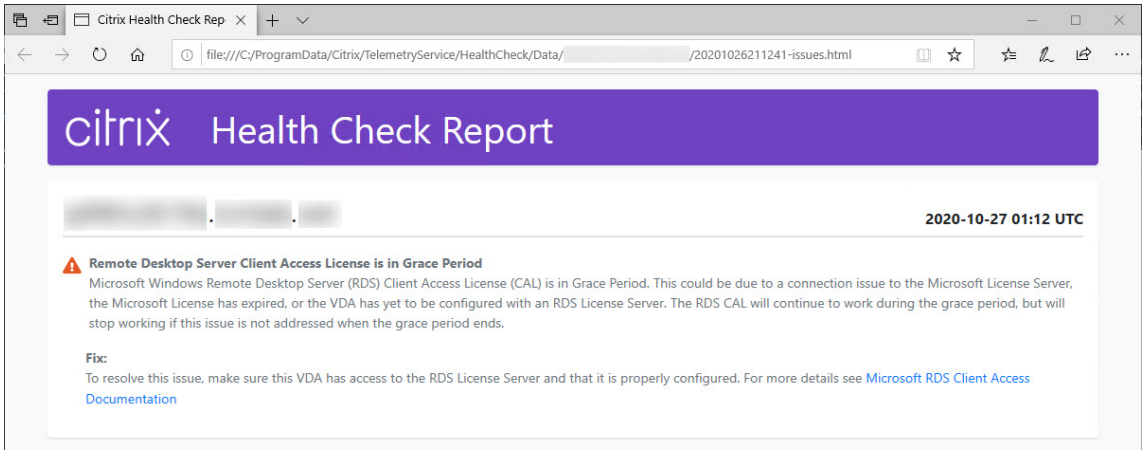
11. Pour arrêter toutes les vérifications en cours, cliquez sur **Arrêter la vérification** dans le coin inférieur droit de la page. Vous ne pouvez pas annuler la vérification de l'état d'une seule machine, vous ne pouvez annuler la vérification que pour toutes les machines sélectionnées.



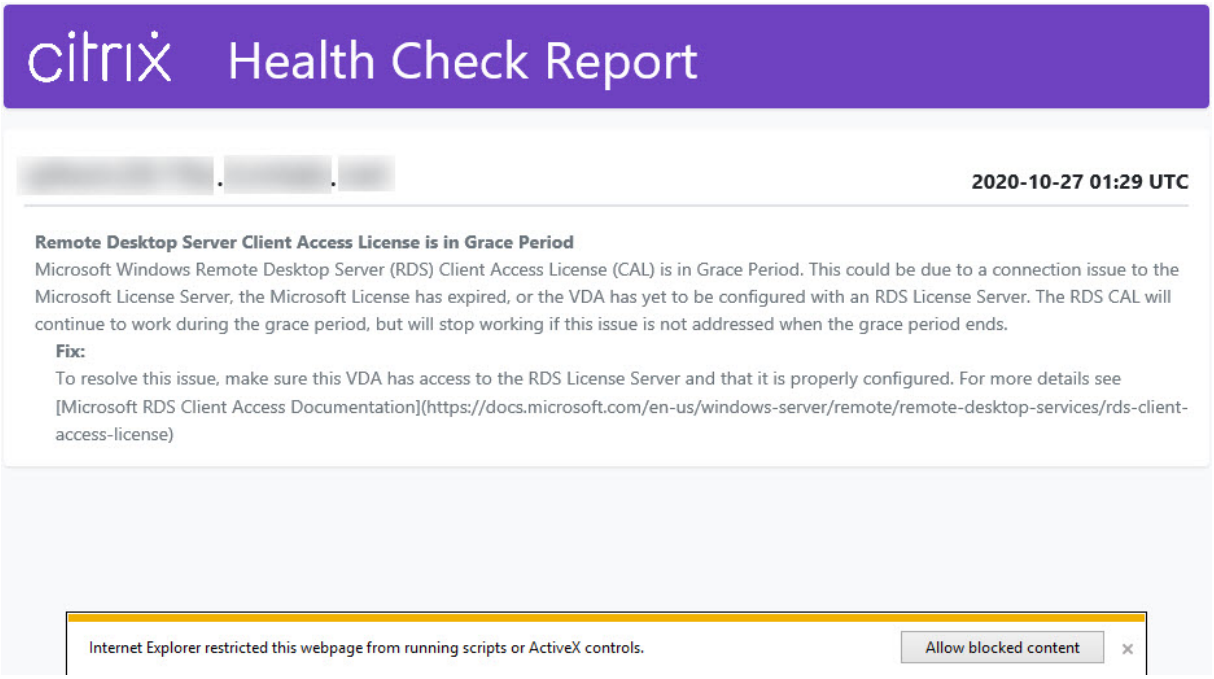
12. Lorsque les vérifications sont terminées pour toutes les machines sélectionnées, le bouton **Arrêter la vérification** dans le coin inférieur droit devient **Terminé**.



- 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.



Si vous utilisez Internet Explorer pour afficher le rapport, vous devez cliquer sur **Autoriser le contenu bloqué** pour afficher le lien hypertexte.



Une fois la vérification terminée pour toutes les machines sélectionnées, le fait de cliquer sur **Précédent** entraîne la perte des résultats de la vérification.

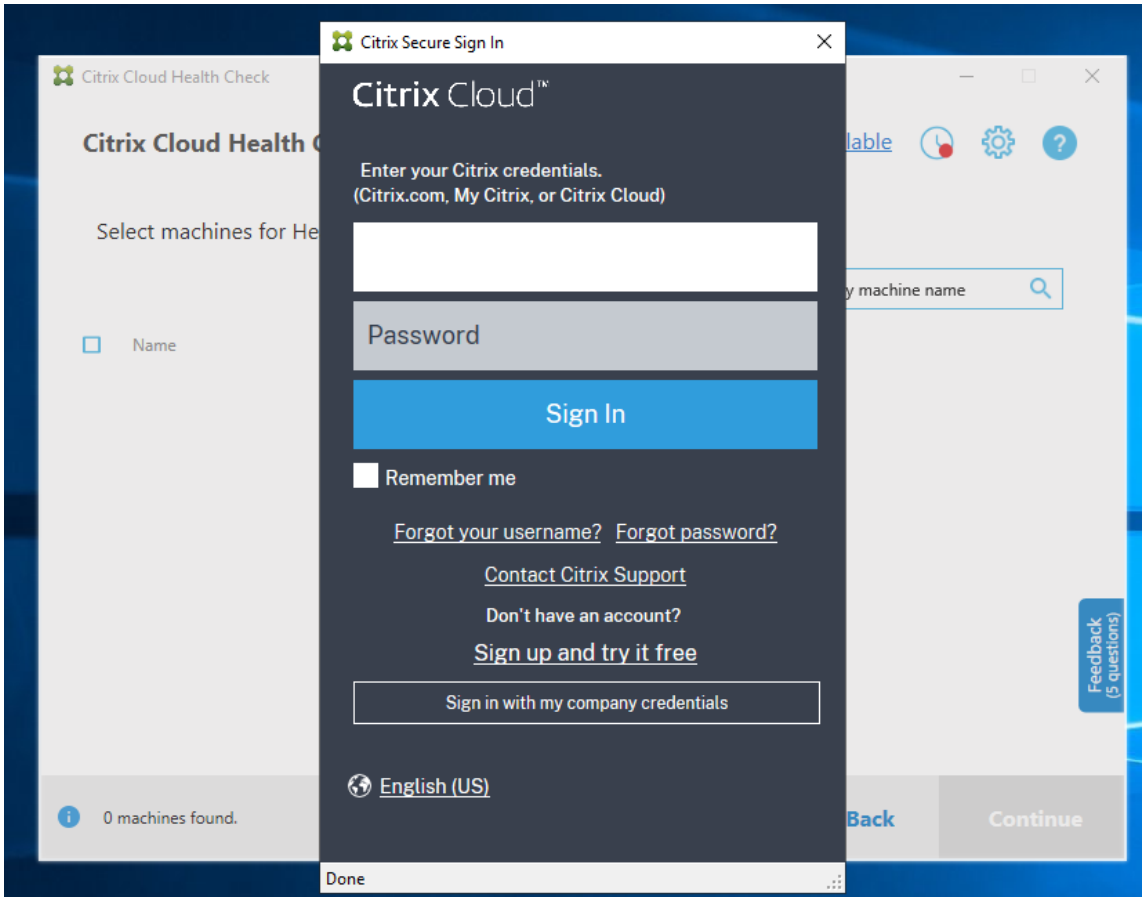
Lorsque les vérifications sont terminées, cliquez sur **Terminé** pour revenir à l'écran principal de Vérification de l'état du cloud.

Récupérer des machines VDA

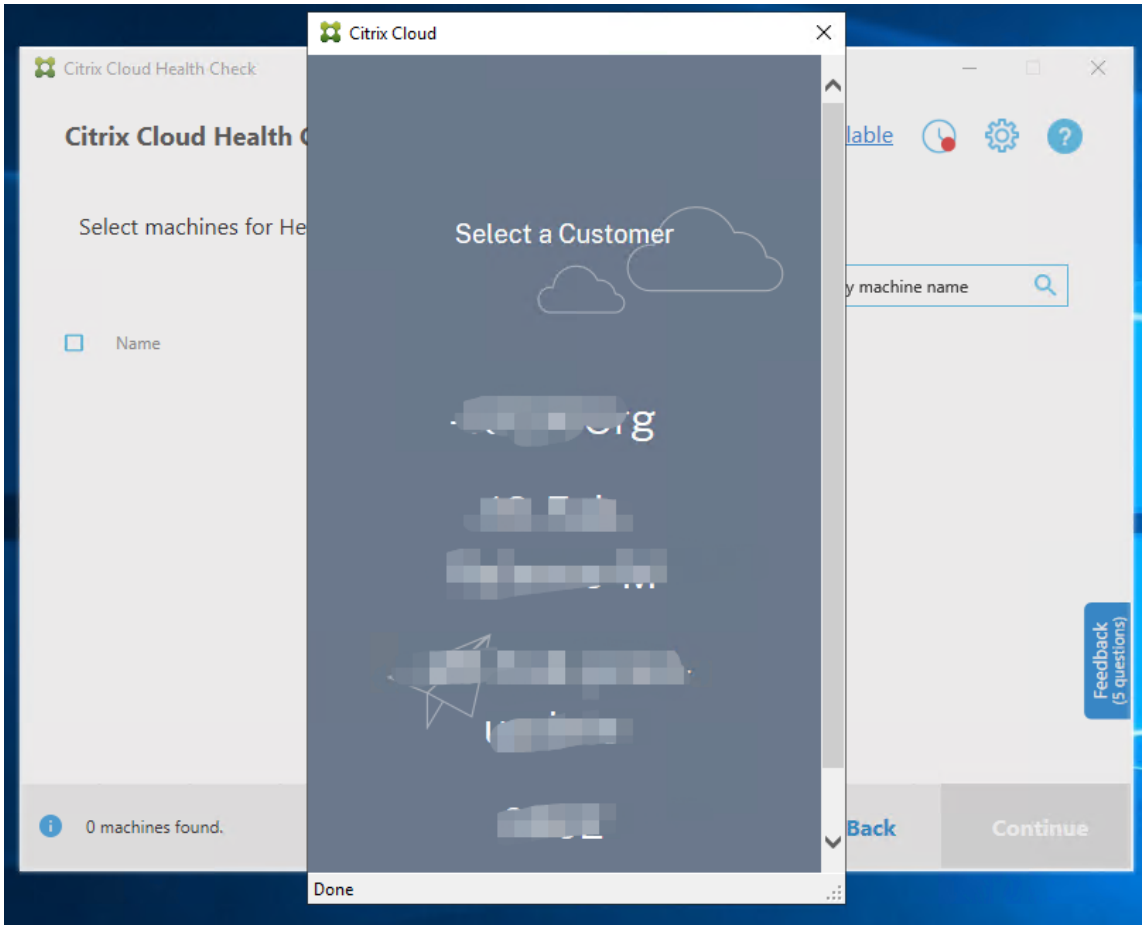
L'outil Vérification de l'état du cloud peut détecter et récupérer automatiquement des VDA à partir de vos déploiements Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).

Pour récupérer vos VDA :

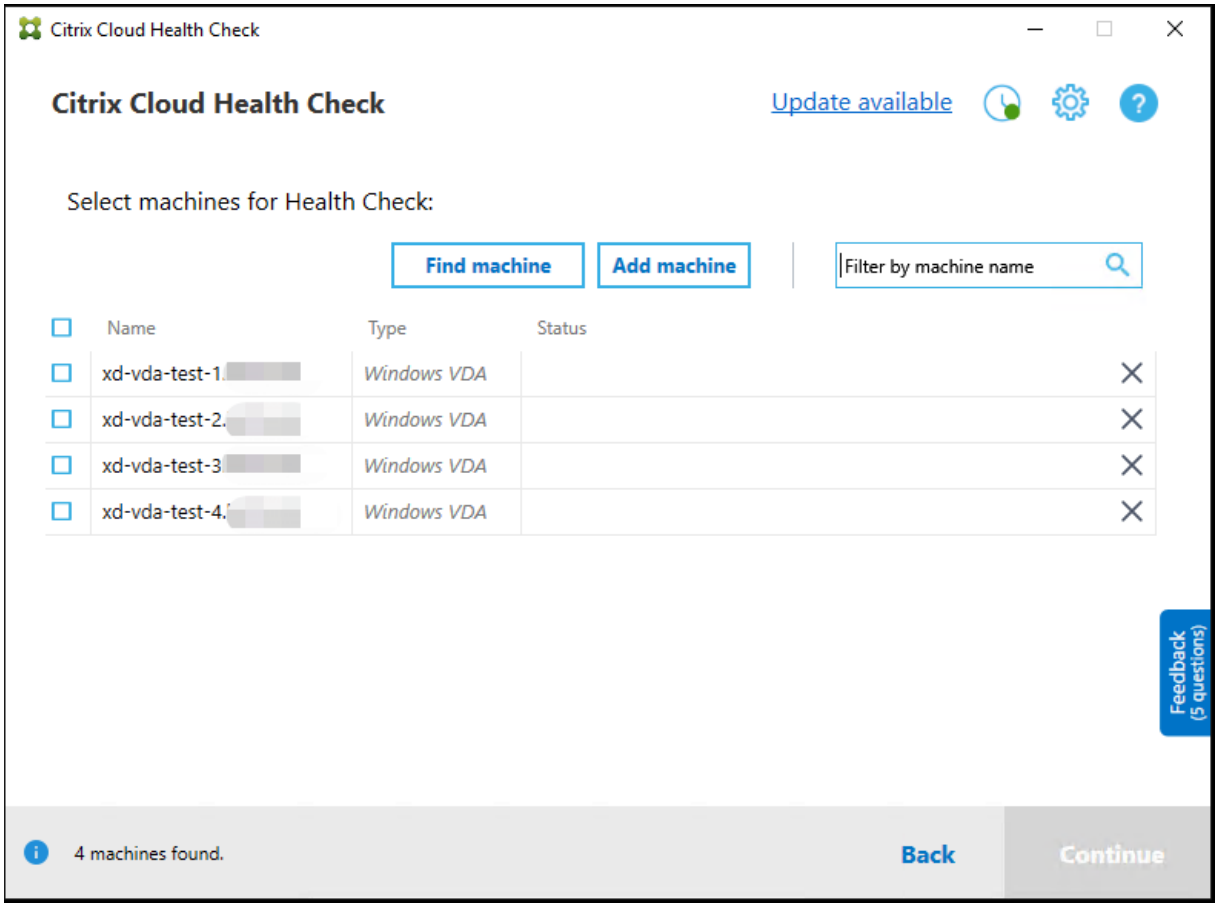
1. Préparez une nouvelle machine qui est jointe à la même forêt de domaine que l'ordinateur sur lequel s'exécute Vérification de l'état du cloud.
2. Ouvrez Vérification de l'état du cloud et cliquez sur **Rechercher machine** pour vous connecter à Citrix Cloud.



3. Sélectionnez le client avec le site cloud que vous souhaitez récupérer.

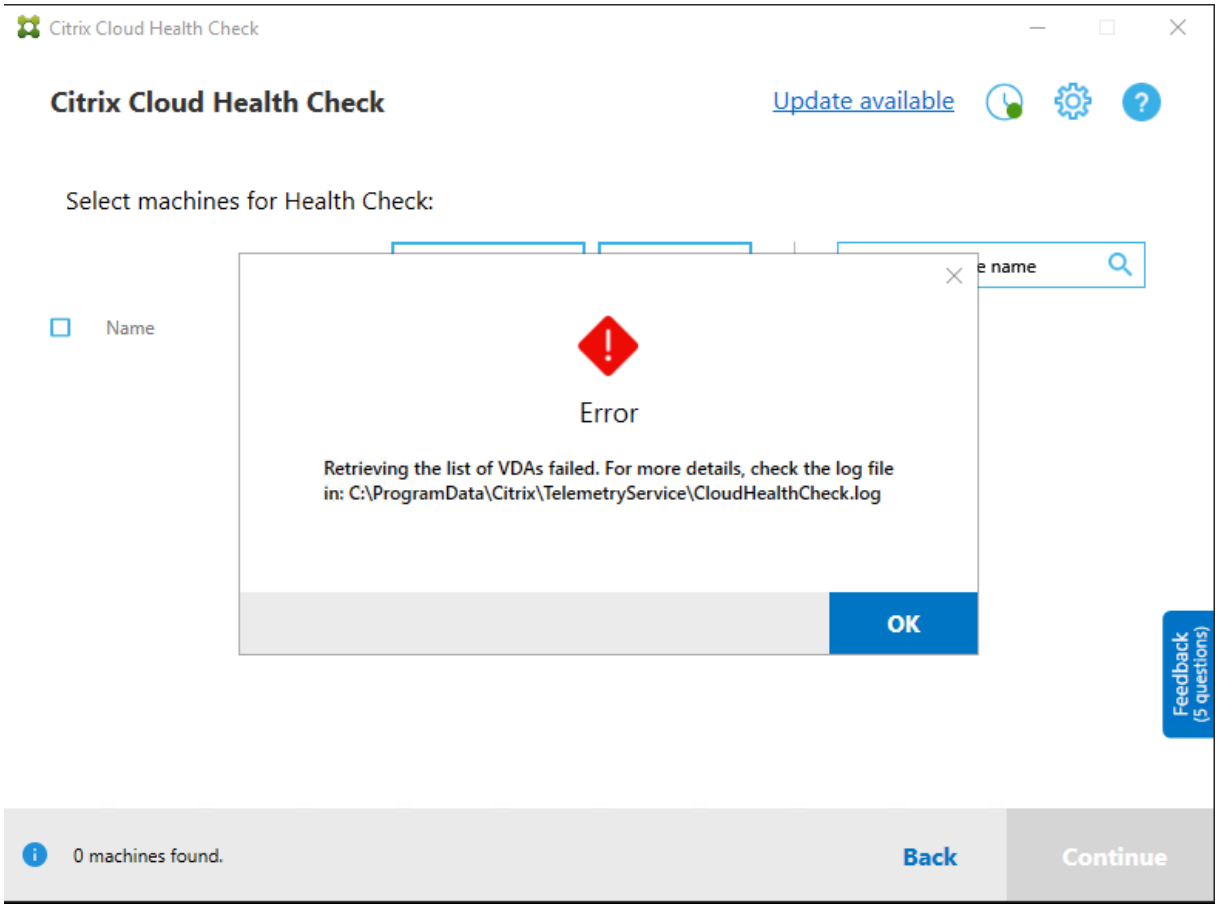


La liste des VDA s'affiche dans Vérification de l'état du cloud. La liste est également enregistrée dans un fichier local situé dans `\ProgramData\Citrix\TelemetryService\ChcDiscovery\ChcDiscoveredMachineList.json`.



Votre liste de machines charge le cache local lorsque vous ouvrez à nouveau Vérification de l'état du cloud. Si vous avez effectué des mises à jour dans votre déploiement, vous devez cliquer sur **Rechercher machine** pour actualiser la liste des machines.

> **Remarque :**
>
> - Vérification de l'état du cloud recherche uniquement les machines dans la même forêt de domaine que la machine sur laquelle Vérification de l'état du cloud s'exécute.
> - Les sessions Citrix Cloud expirent au bout d'une heure. Après une heure, vous devez cliquer à nouveau sur **Rechercher machine** pour obtenir la dernière liste de VDA.
> - Un message d'erreur apparaît si la récupération de la liste de VDA échoue. Vous pouvez vérifier les détails dans `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.



Résultats de la vérification

Les vérifications de l'état qui génèrent des rapports contiennent les éléments suivants :

- Heure et date à laquelle le rapport de résultats a été généré
- Noms de domaines complets des machines analysées
- Conditions vérifiées sur les machines cibles

Exécution de Vérification de l'état du cloud sur la ligne de commande

Vérification de l'état Citrix Cloud peut être exécuté sur la ligne de commande pour aider les clients à effectuer des contrôles d'intégrité. Pour utiliser Vérification de l'état du cloud sur la ligne de commande, vous devez être un administrateur sur la machine sur laquelle la vérification est exécutée.

> **Remarque :**
>
> Lorsque vous utilisez Vérification de l'état du cloud sur la ligne de commande, une seule machine peut être vérifiée à la fois. Une seule instance de `CloudHealthCheck.exe` peut être exécutée

> simultanément sur la machine cible. Si vous souhaitez vérifier plusieurs machines, les machines doivent être vérifiées une par une, en enveloppant les applets de commande dans une boucle dans les scripts Cmdlet/PowerShell. Toute instance d'interface utilisateur ouverte de Vérification de l'état du cloud doit également être fermée.

Applets de commande

Les applets de commande de ligne de commande prises en charge sont les suivantes :

- `MachineFQDN` - Cette applet de commande est **obligatoire**. Il s'agit du nom de domaine complet de la machine cible.
- `MachineType` - Cette applet de commande est facultative. La valeur de l'applet de commande peut être le VDA Windows (valeur par défaut) ou StoreFront.
- `ReportName` - Cette applet de commande est facultative. La valeur de l'applet de commande doit être un nom de fichier valide sous Windows. La valeur par défaut est `HealthCheckReport`.
- `SkipAdminCheck` - Cette applet de commande est facultative. Peut être ajouté pour ignorer les vérifications qui nécessitent des autorisations d'administrateur.
- `UpdateScripts` - Cette applet de commande est facultative. Peut être ajouté pour mettre à jour les scripts de vérification à partir du serveur CDN.
- `DisableCeip` - Cette applet de commande est facultative si le programme CEIP est activé dans l'interface utilisateur, ajoutez-la pour désactiver ce programme.
- `Help` - Affiche les informations d'aide relatives aux paramètres.

Exemples :

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -ReportName
checkreport
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -SkipAdminCheck
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -UpdateScripts
```

```
HealthCheckCLI.exe -MachineFQDN machine1.domain.local,machine2.domain
.local,machine3.domain.local
```

```
HealthCheckCLI.exe -Help
```

> **Remarque :**
>
> Les noms de paramètres ne sont pas sensibles à la casse.

Par défaut, la sortie de la console n'est pas affichée dans la fenêtre de la console de ligne de commande. Vous pouvez afficher manuellement la sortie en ajoutant `|more` à l'applet de commande.

Exemple : `HealthCheckCLI.exe -MachineFQDN machine.domain.local|more`

La valeur par défaut de la ligne de commande nécessite des autorisations d'administrateur pour s'exécuter. Pour passer outre les autorisations d'administrateur, ajoutez le paramètre `-SkipAdminCheck`.

Codes de sortie

Les codes de sortie expliquent le résultat des vérifications de l'état du cloud dans la ligne de commande. Pour obtenir le code de sortie, vous devez ajouter `start /wait` avant l'applet de commande.

Exemple : `start /wait HealthCheckCLI.exe -MachineFQDN machine.domain.local`

Les codes de sortie sont les suivants :

- 0 - Normal, vérification terminée et réussie.
- 1 - Échec, vérification terminée avec des problèmes.
- 2 - Erreur, vérification non terminée avec des erreurs.

Vous pouvez également utiliser l'applet de commande `echo %errorlevel%` pour obtenir le code de sortie de la dernière commande exécutée.

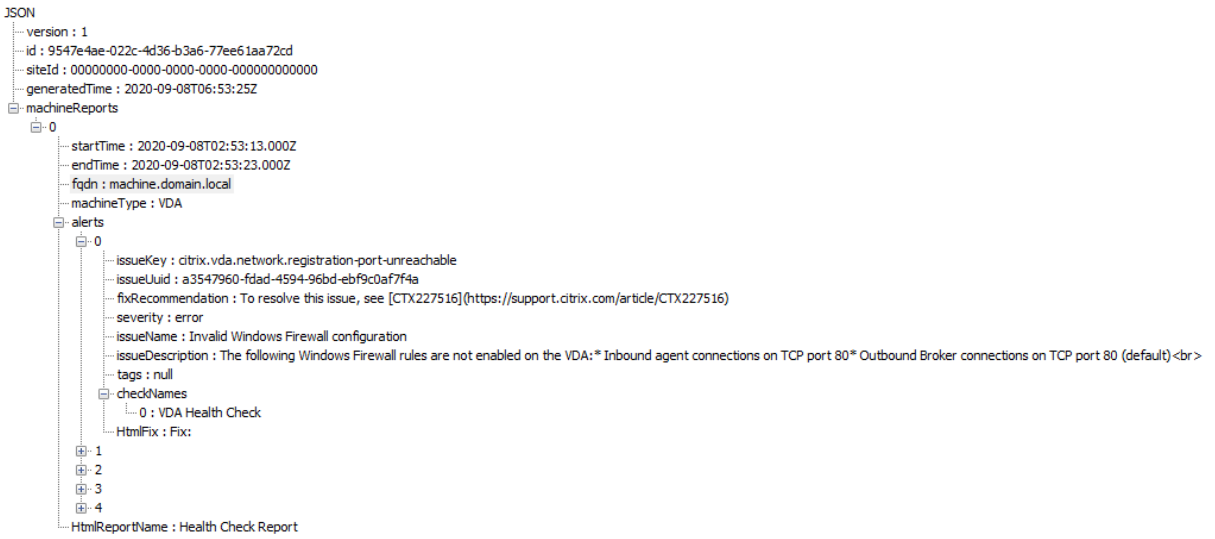
Rapports

Vérification de l'état du cloud crée des dossiers en utilisant le nom de la machine dans `HealthCheckDataFolde` pour la machine cible. Un fichier .html et un fichier .json sont créés sur l'ordinateur sur lequel la fonction Vérification de l'état du cloud est installée. Les rapports de vérification de l'état se trouvent dans le dossier `HealthCheckDataFolder` dans `%ProgramData%\Citrix\TelemetryService\HealthCheck\Data`.

Les rapports ne sont créés que lorsque des problèmes existent sur la machine cible.

> **Remarque :**
>
> Les fichiers de rapport sont remplacés si le nom de rapport spécifié existe.

Les alertes et les informations de base sont stockées dans le rapport .json.

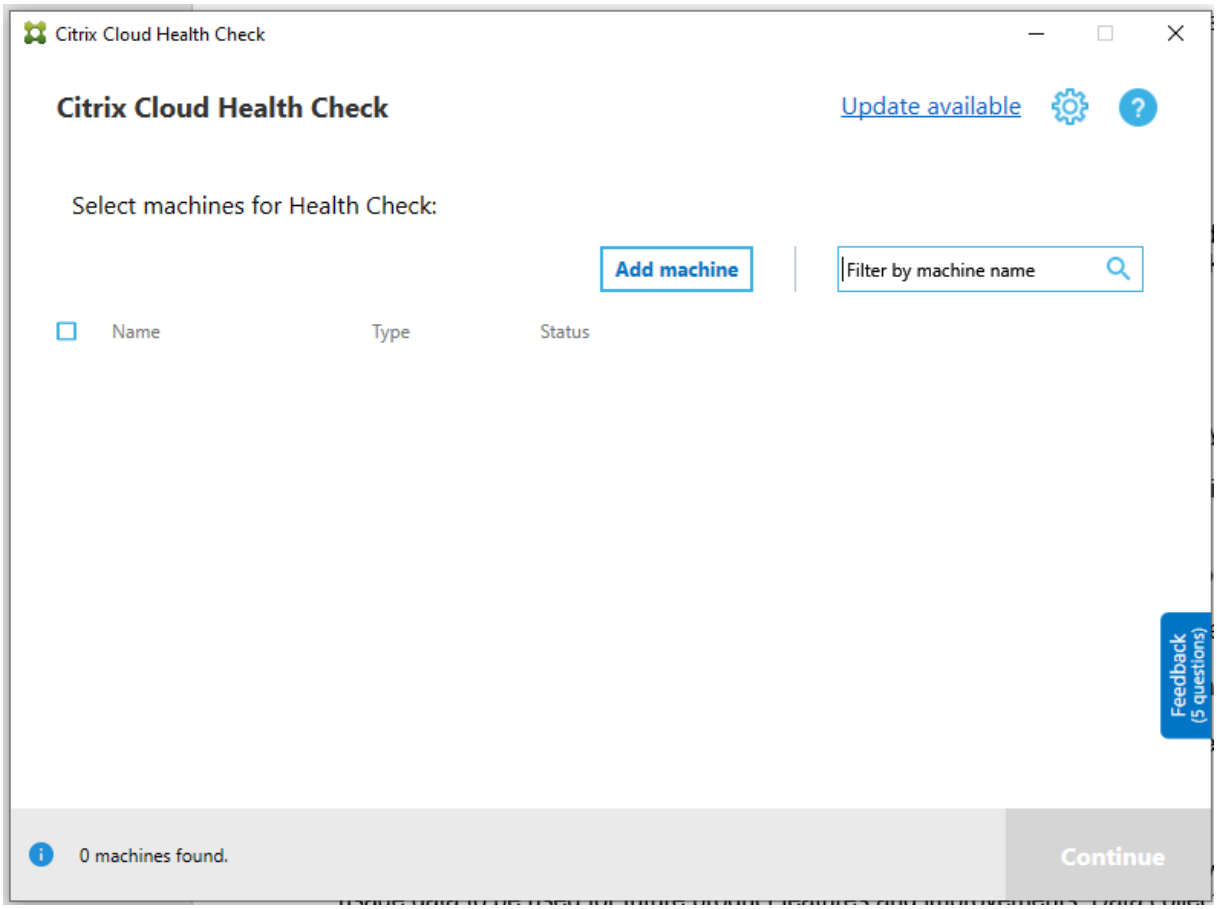


Les codes de rapport sont les suivants :

- **issueKey** : description en texte brut du problème.
- **issueUuiD** : chaîne d'identification unique pour le problème.
- **fixRecommendation** : correction recommandée pour le problème.
- **severity** : indique si le problème doit être résolu. Une erreur peut indiquer que le composant (VDA ou StoreFront) a mal fonctionné, et un avertissement indique que le composant peut fonctionner mais qu'il peut rencontrer des problèmes potentiels.
- **issueName** : titre du problème.
- **issueDescription** : description détaillée du problème.

Mise à jour de Vérification de l'état du cloud

Si une nouvelle version de Vérification de l'état du cloud est disponible, un lien Mise à jour disponible s'affiche en haut à droite de la fenêtre de Vérification de l'état du Cloud. Cliquez sur le lien pour accéder aux téléchargements Citrix pour obtenir la nouvelle version.

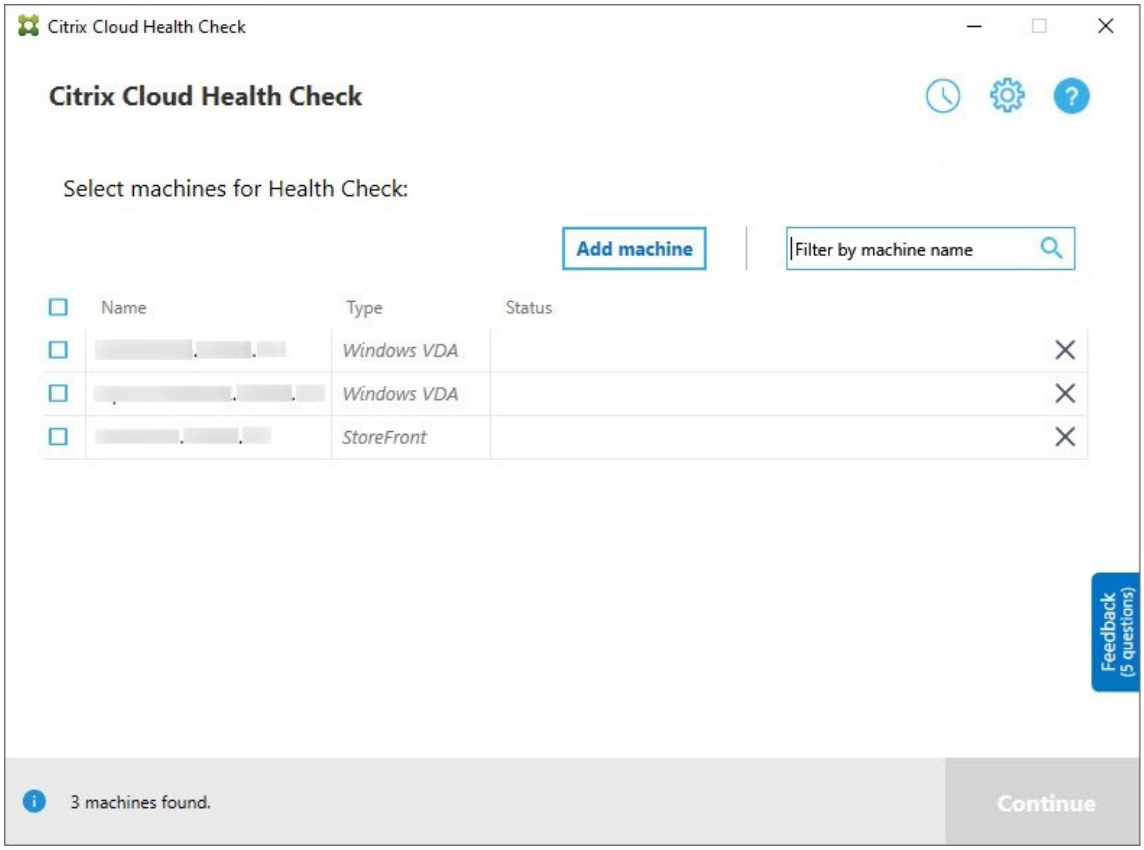


Planificateur Vérification de l'état du cloud

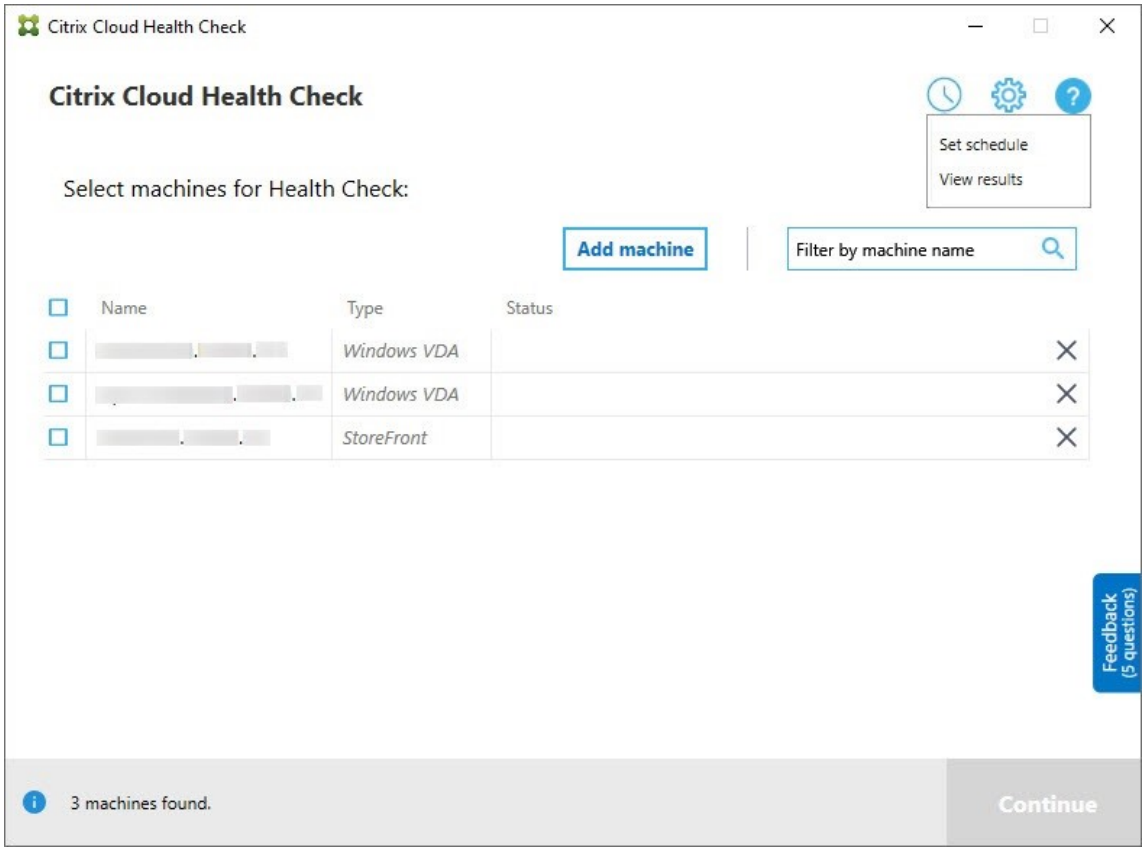
Utilisez le planificateur Vérification de l'état du cloud pour effectuer des vérifications périodiques de l'état.

Configurer le planificateur

1. Cliquez sur **Ajouter machine** dans la fenêtre principale Vérification de l'état du cloud pour ajouter des machines sur lesquelles vous souhaitez exécuter des vérifications périodiques.



2. Cliquez sur l'icône de l'horloge, puis sur **Définir planification**.



3. Sélectionnez une heure pour votre planification, puis cliquez sur **Suivant**. La tâche peut être configurée pour se répéter en activant la case à cocher **Répéter la tâche toute(s) les**.
4. Choisissez de consigner les résultats dans le journal des événements Windows. La tâche peut être définie pour écrire les résultats dans le journal des événements Windows.
5. Choisissez de déclencher un script PowerShell personnalisé une fois l'analyse planifiée terminée, puis cliquez sur **Suivant**.

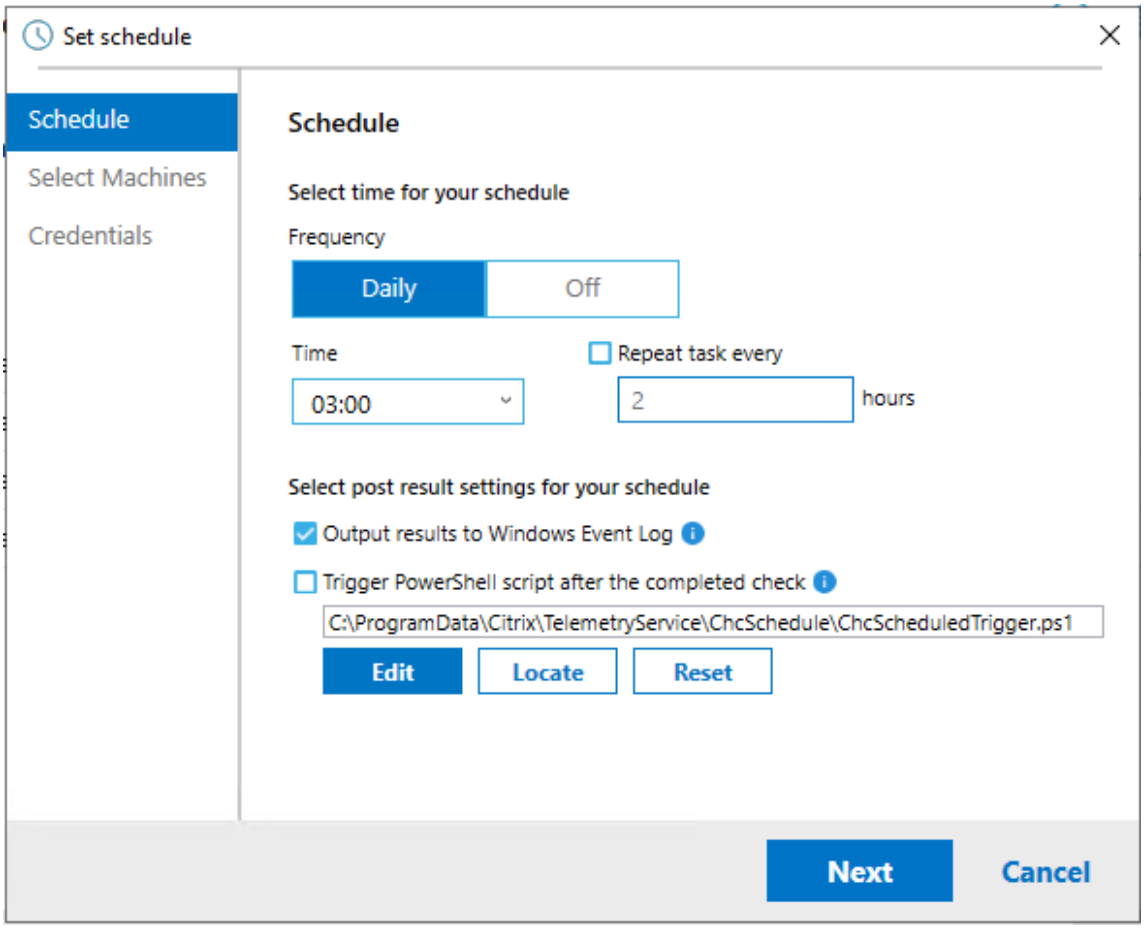
    - Cliquez sur **Modifier** pour modifier le contenu du script dans Windows PowerShell ISE si nécessaire.
    - Cliquez sur **Localiser** pour ouvrir l'emplacement du fichier et utiliser un autre éditeur pour ouvrir le fichier afin de modifier le script.
    - Cliquez sur **Réinitialiser** pour rétablir le paramètre d'origine du script.

    > **Remarque :**
    >
    > – Vous ne pouvez pas modifier le nom ni le chemin d'accès du script.
    > – Vous pouvez implémenter des actions personnalisées à l'aide du script Chc-ShceduledTrigger.ps1, comme l'envoi d'un e-mail une fois que le rapport d'analyse planifiée est prêt. Ajoutez le code suivant à la fin du script. Per-

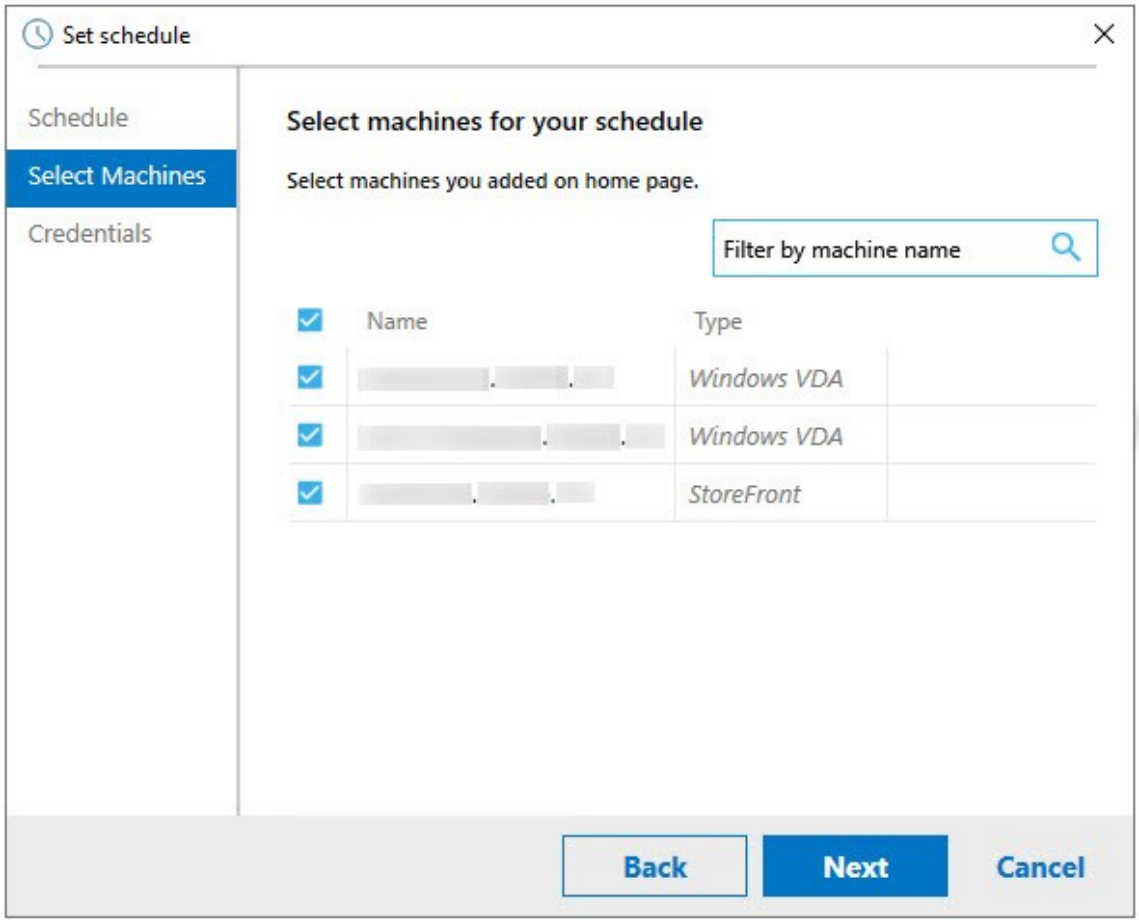
> sonnalisez le code pour ajouter les comptes de messagerie appropriés et l'adresse du serveur SMTP. Une notification par e-mail est envoyée à l'aide des informations d'identification du compte que la tâche planifiée exécute.

```
#Sending email example code:
$body = "CreatedTime: $($report.CreatedTime)"
$body = $body + "`nStatusCode: $($report.StatusCode)"
$body = $body + "`nMachineCount: $($report.MachineReports.Count)"
$from = "mock_email_accout"
$to = "mock_email_accout"
$smtpServer = "mock_smtp_server"

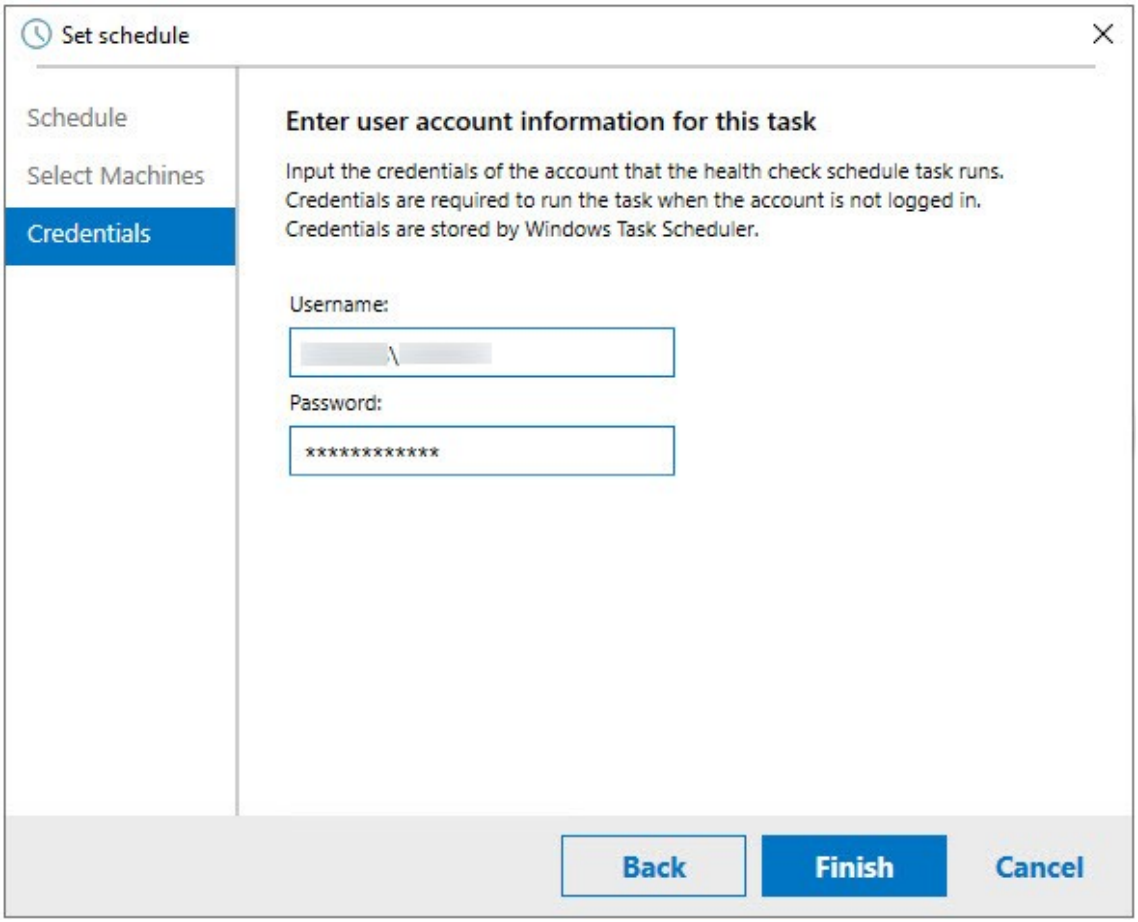
Send-MailMessage -Subject "Citrix Cloud Health Check Scheduler
   Report" -Body $body -From $from -To $to -SmtpServer $smtpServer
<!--NeedCopy-->
```



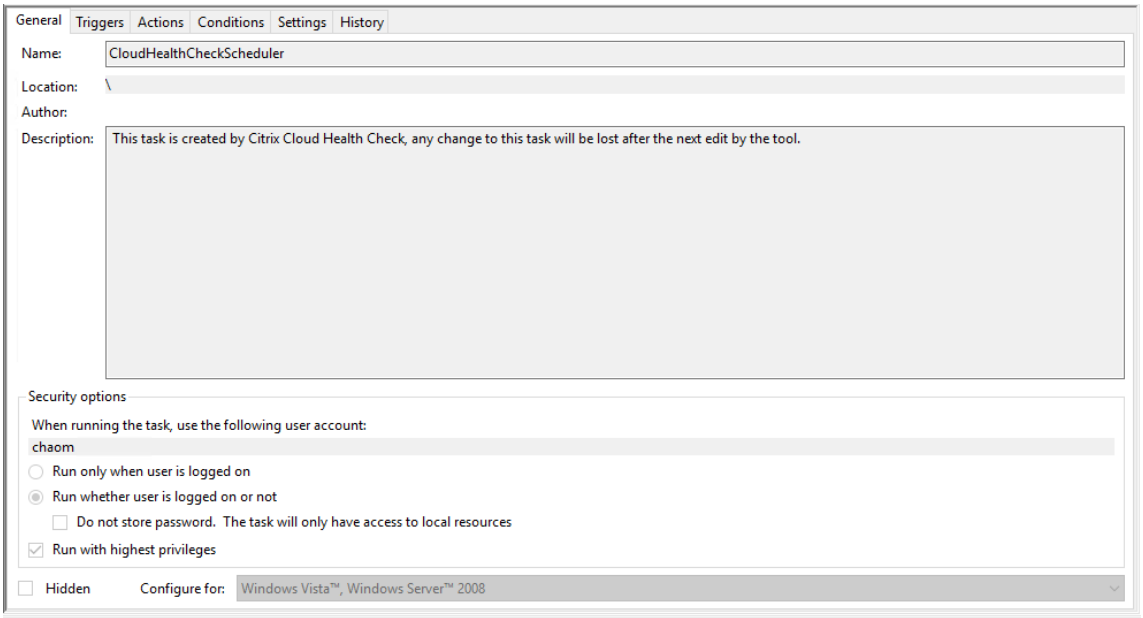
6. Sélectionnez les machines pour votre planification, puis cliquez sur **Suivant**.



7. Entrez les informations d'identification du compte sur lequel la tâche s'exécute, puis cliquez sur **Terminer**.

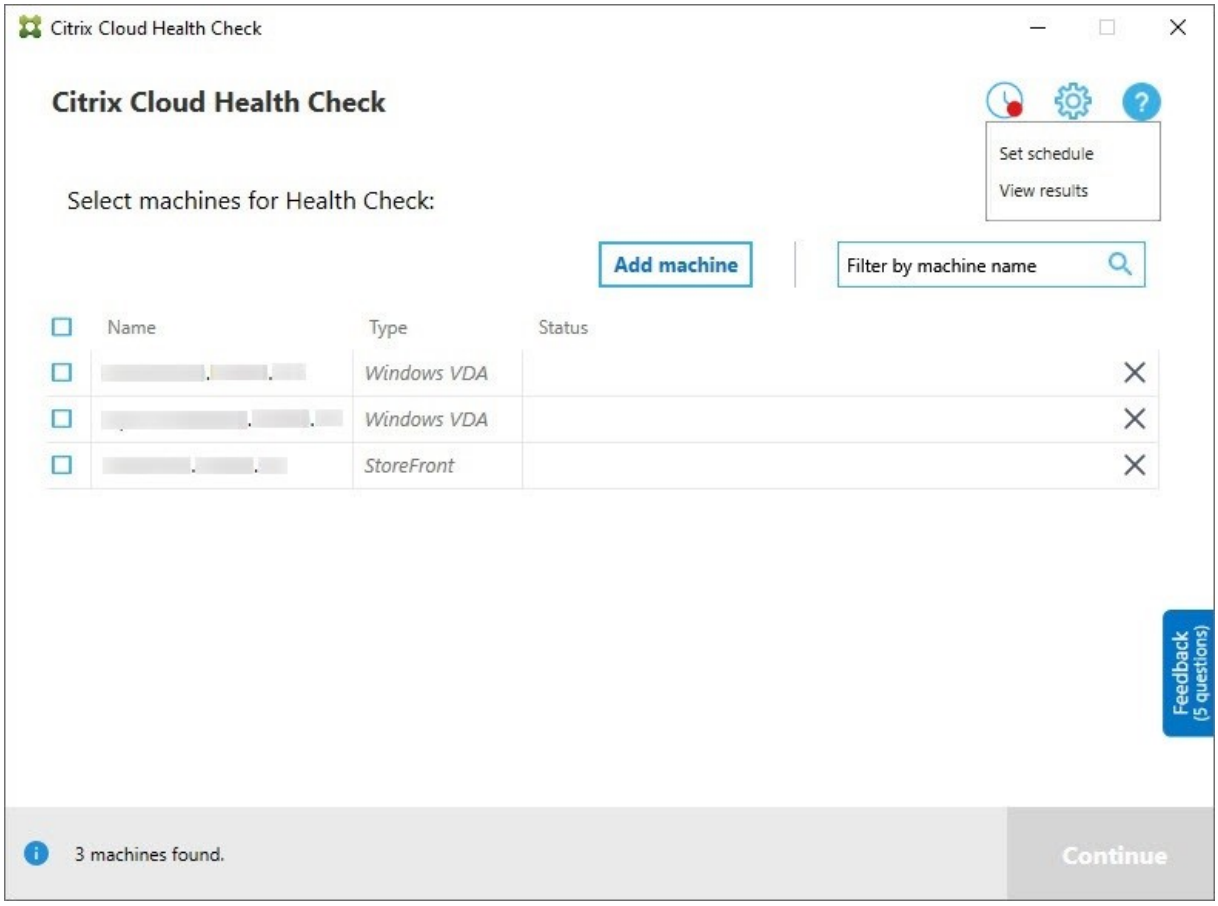


8. Une tâche CloudHealthCheckScheduler est créée dans le Planificateur de tâches Windows.

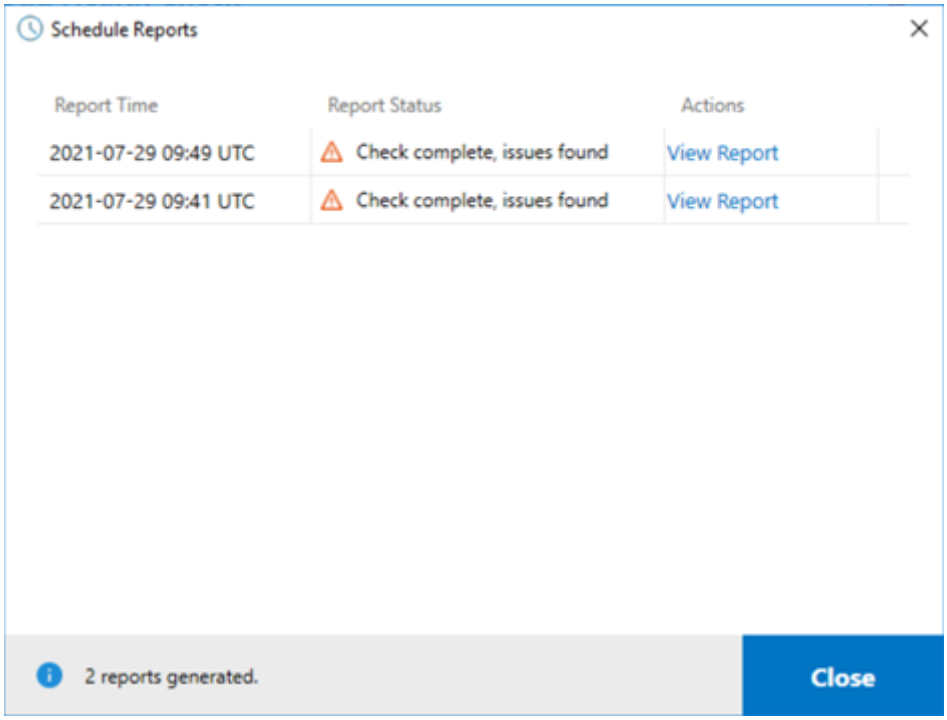


Afficher les résultats du planificateur

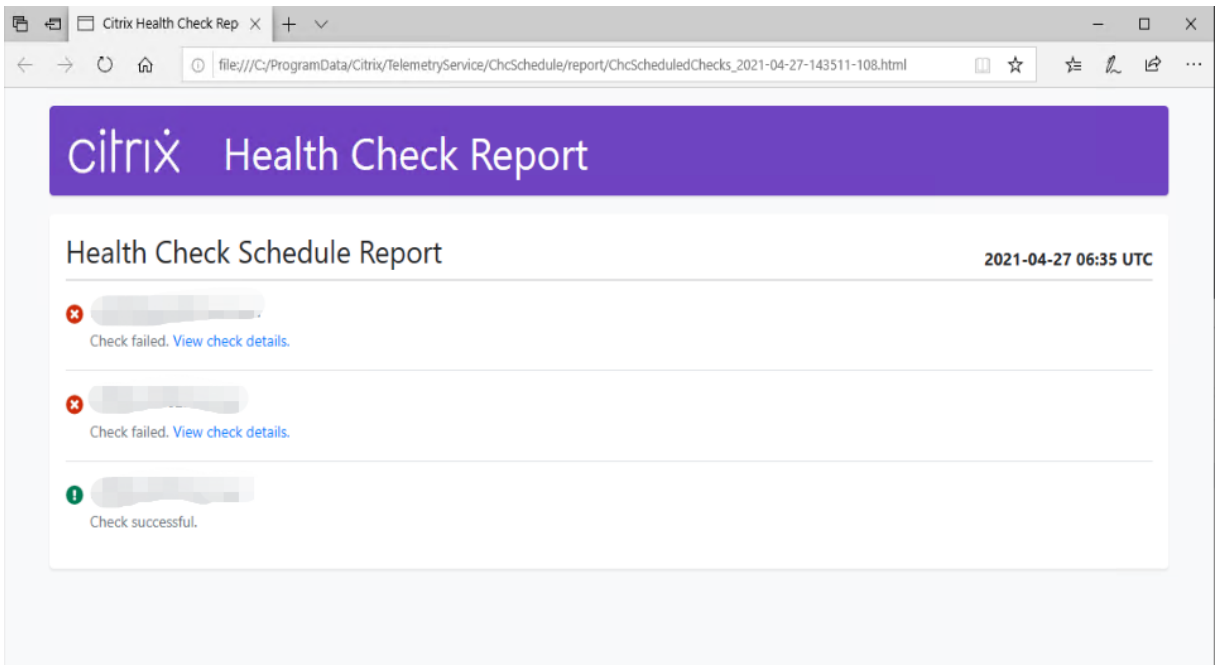
L'icône d'horloge avec un point rouge indique que des problèmes ont été détectés lors de la dernière vérification. Pour afficher les résultats, cliquez sur l'icône d'horloge, puis sur **Afficher les résultats**.



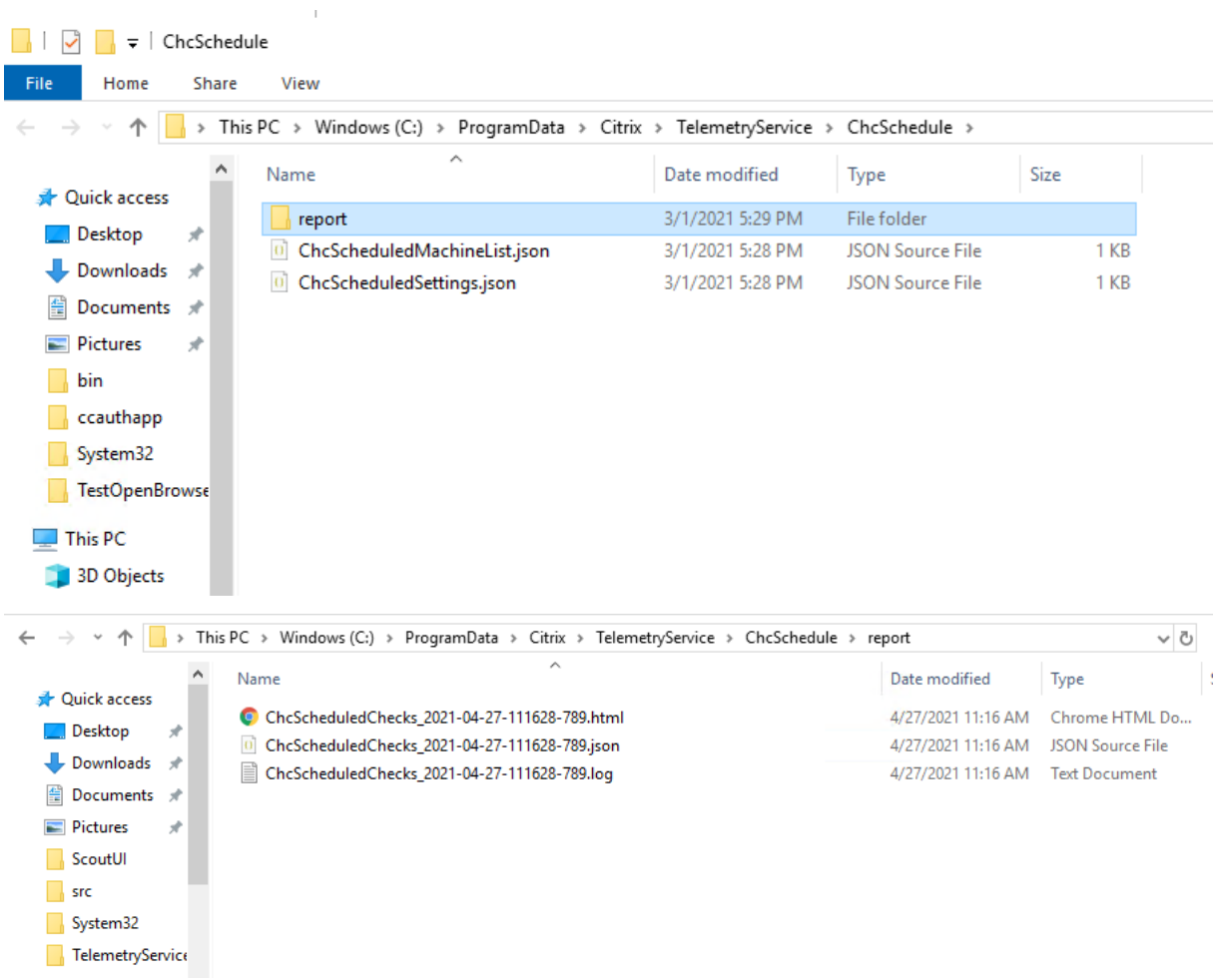
La page Rapports de planification affiche les résultats de toutes les tâches de vérification de l'état planifiées. Cliquez sur **Afficher le rapport** pour vérifier le rapport pour chaque planification.



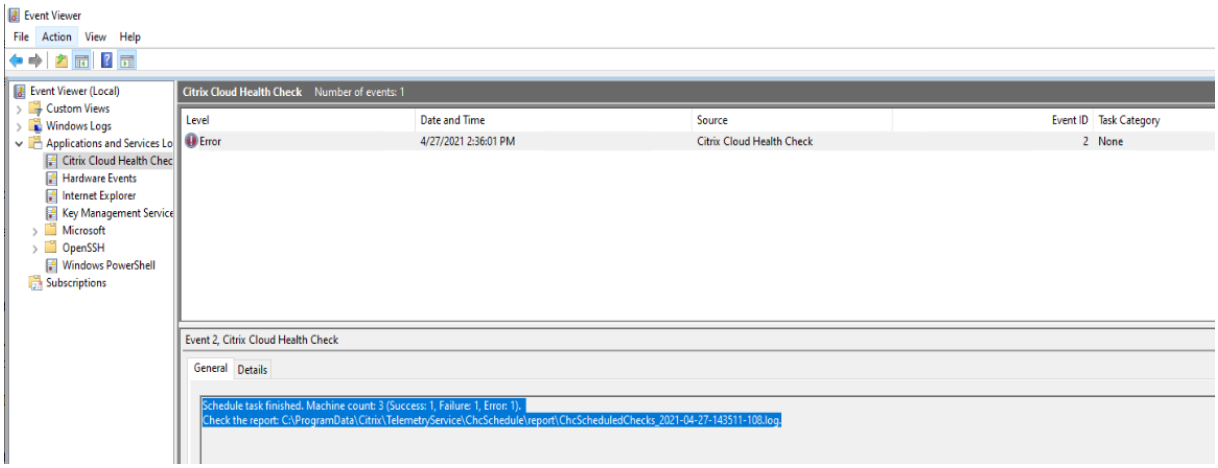
Le rapport html répertorie le rapport global pour chaque planification. Voici un exemple de rapport :



Tous les résultats de la vérification sont stockés dans un dossier appelé ChcSchedule. Vérification de l'état du cloud crée trois fichiers lors de chaque exécution de la vérification. Jusqu'à 500 journaux d'itération sont conservés.

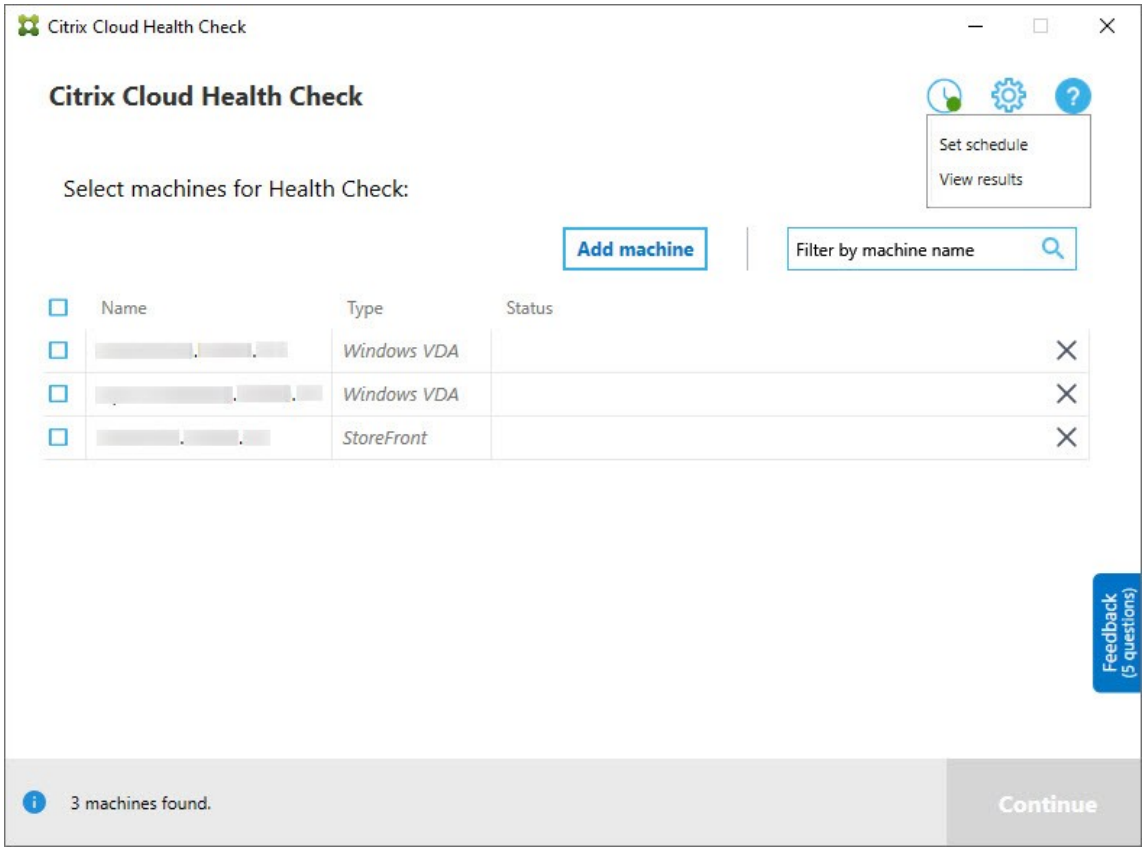


Si la case **Consigner les résultats dans le journal des événements Windows** est cochée, le résultat de la vérification est également envoyé au journal des événements de fenêtre.

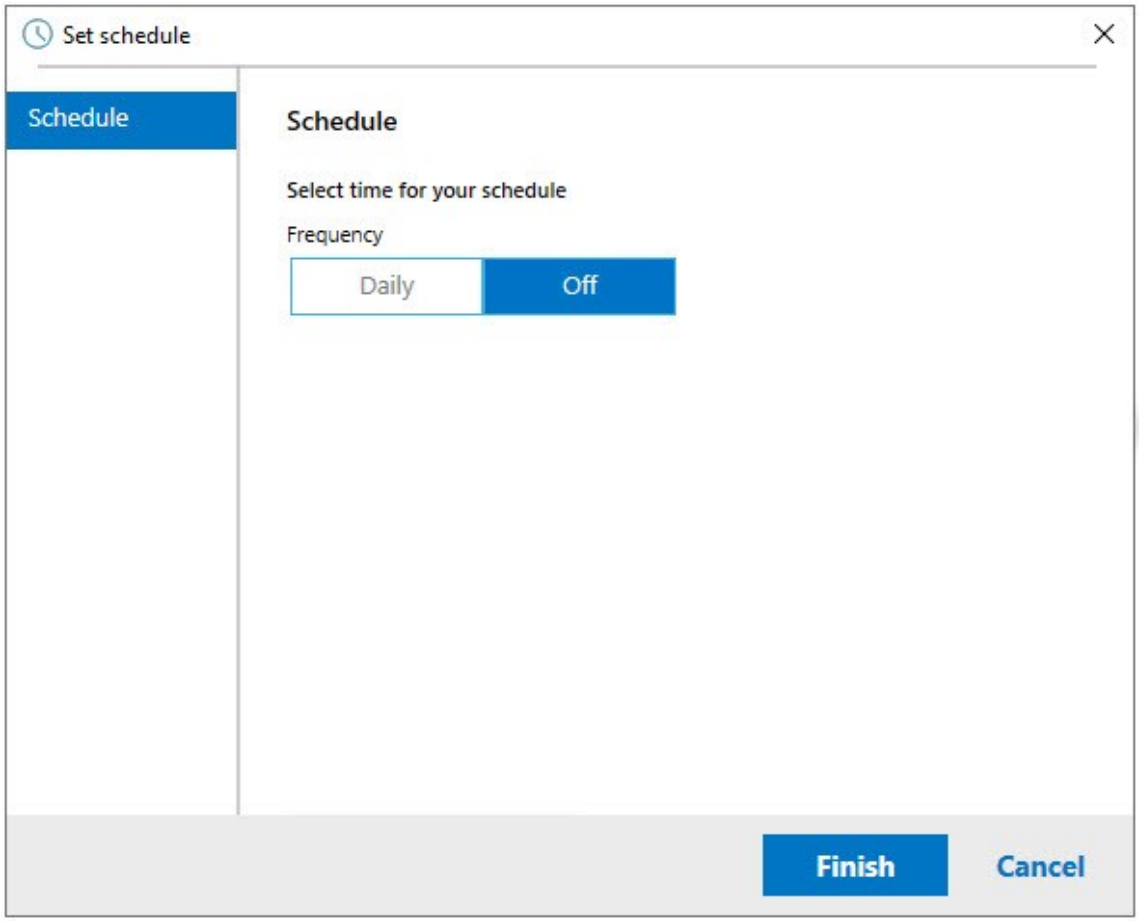


Désactiver les planifications

1. Cliquez sur l'icône de l'horloge, puis sur **Définir planification**.



2. Cliquez sur **Désactivé**, puis sur **Terminer** pour désactiver le planificateur.



Informations supplémentaires

- Vous devez d'abord ajouter ou importer des VDA dans Vérification de l'état du cloud. Pour plus d'informations, consultez Importer des machines VDA.
- Le planificateur Vérification de l'état du cloud ne peut planifier qu'une tâche à la fois sur une machine reliée à un domaine. Si vous définissez la planification plusieurs fois, seule la dernière prend effet.

Tests de vérification

Avant le démarrage d'une vérification d'état, des tests de vérification sont exécutés automatiquement pour chaque machine sélectionnée. Ces tests permettent de s'assurer que les conditions requises sont remplies pour l'exécution d'une vérification de l'état. Si un test échoue pour une machine, Vérification de l'état du cloud affiche un message contenant des actions correctives suggérées.

- **Vérification de l'état du cloud ne peut accéder à cette machine :** assurez-vous que :
  - La machine est allumée.

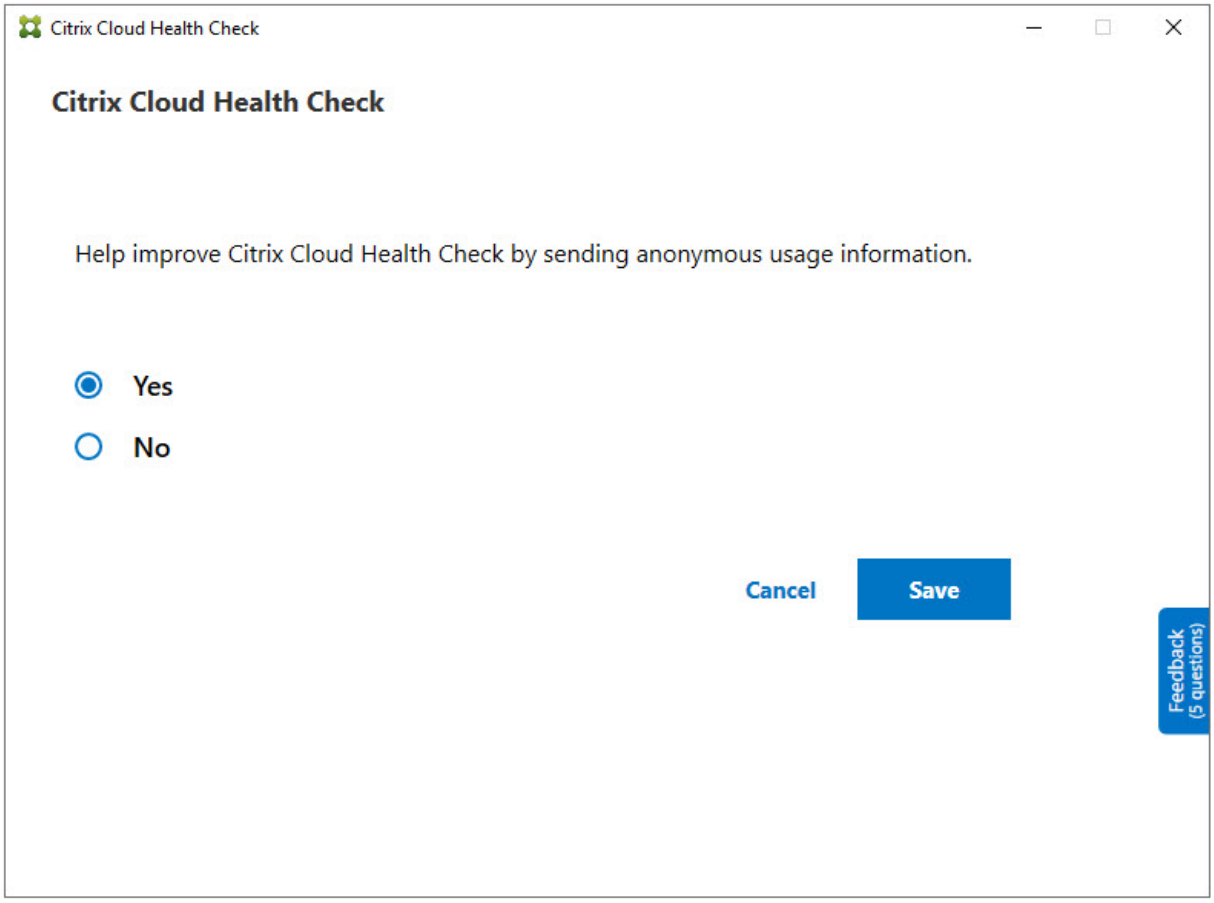
  - La connexion réseau fonctionne correctement. (il peut vérifier que votre pare-feu est correctement configuré.)
  - Le partage de fichiers et d'imprimantes est activé. Consultez la documentation Microsoft pour obtenir des instructions.

- **Activer PSRemoting et WinRM** - Vous pouvez activer l'accès à distance PowerShell et WinRM en exécutant PowerShell en tant qu'administrateur, puis en exécutant l'applet de commande Enable-PSRemoting. Pour de plus amples informations, consultez l'aide de Microsoft pour l'applet de commande.
- **Vérification de l'état du cloud requiert PowerShell 3.0 ou version ultérieure :** installez PowerShell 3.0 (ou version ultérieure) sur la machine et activez la communication à distance PowerShell.
- **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.

Collecte de données d'utilisation

Lorsque vous utilisez Vérification de l'état du cloud, 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 Vérification de l'état du cloud. Vous pouvez ensuite choisir d'envoyer les informations en sélectionnant **Oui** ou **Non**, puis en cliquant sur **Enregistrer**.



Correction automatique

La correction automatique permet à Vérification de l'état du cloud de détecter et de résoudre automatiquement certains problèmes en modifiant les paramètres ou en redémarrant les services.

La correction automatique vérifie les éléments d'enregistrement VDA suivants, avec les corrections recommandées :

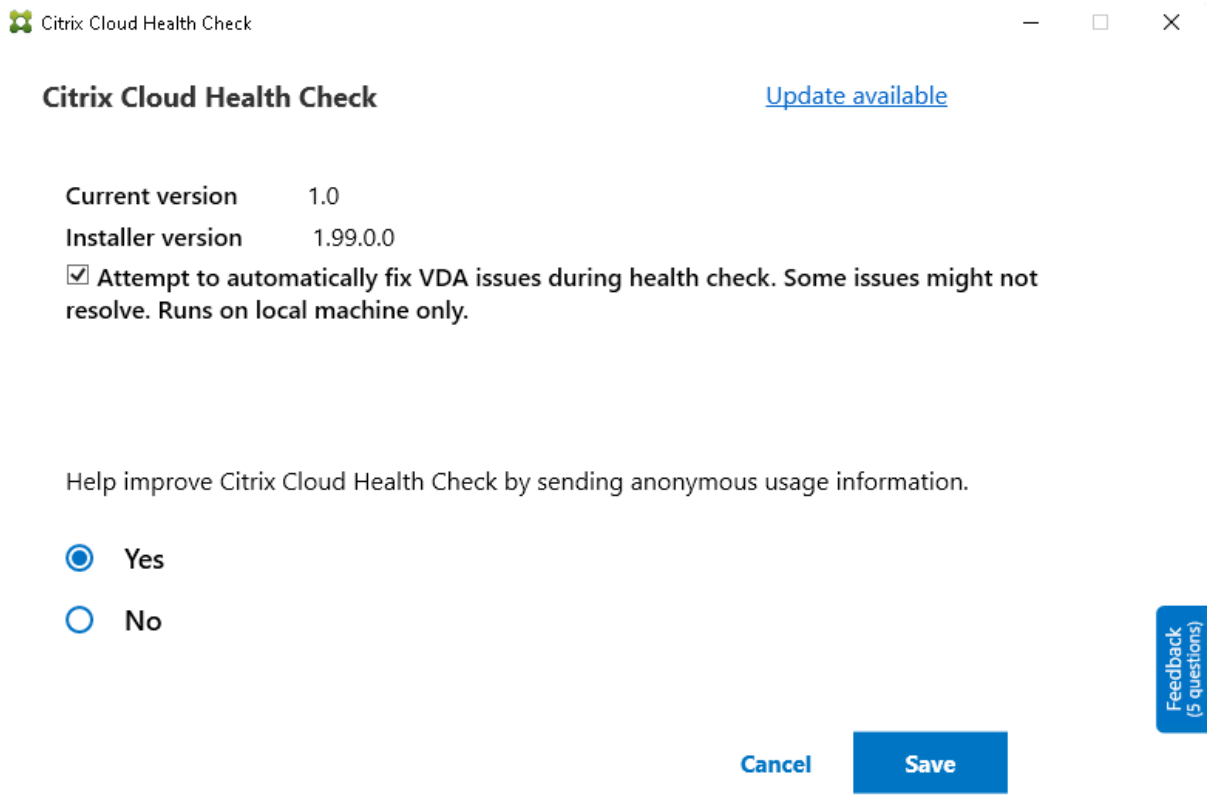
- Appartenance au domaine de la machine VDA
  - Correction : Tester le canal de sécurité de connexion avec un modèle « réparation » pour corriger
- État des services VDA
  - Correction : Redémarrer le service BrokerAgent
- Communication avec le Controller
  - Correction : Redémarrer le service BrokerAgent
- Synchronisation de l'heure avec le Controller

- Correction : Exécuter la commande W32tm

Pour les lancements de session, la correction automatique vérifie l'élément suivant, avec la correction recommandée :

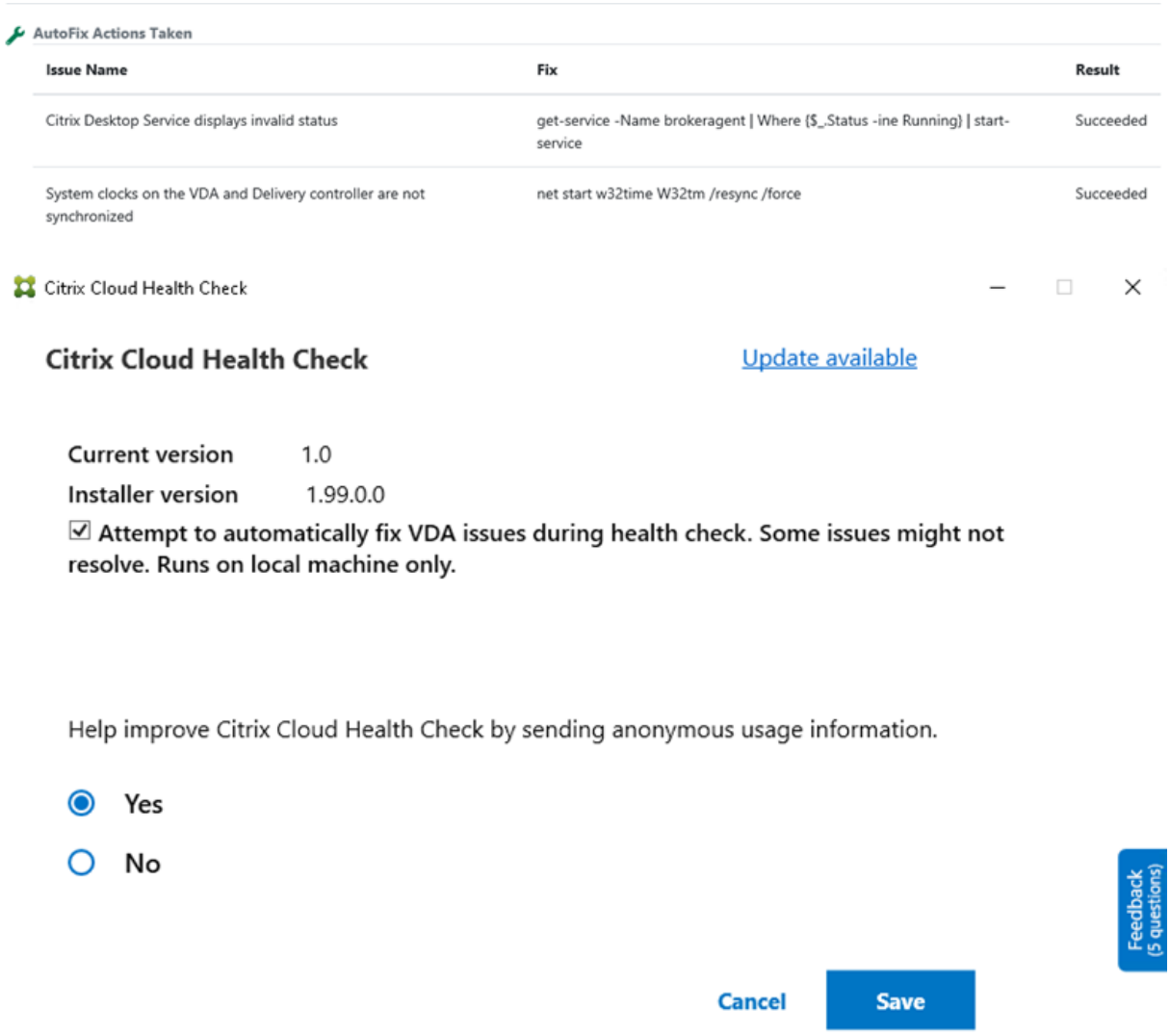
- État du service de lancement de session
  - Correction : Redémarrer le service BrokerAgent

Par défaut, cette fonction est activée. Pour la désactiver, cliquez sur l'icône en forme d'engrenage dans le coin supérieur droit de la fenêtre principale Vérification de l'état du cloud, puis désactivez la case **Essayez de résoudre automatiquement les problèmes liés au VDA pendant la vérification de l'intégrité**.



Rapport des résultats

Une fois la correction automatique effectuée, une section du rapport des résultats de la vérification affiche tous les détails :



Résolution des problèmes

Lorsque Vérification de l'état du cloud ne parvient pas à s'exécuter ou qu'une exception se produit, vérifiez la connexion à Vérification de l'état du cloud dans `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.

Le journal de Vérification de l'état du cloud pour chaque machine cible se trouve dans `C:\ProgramData\Citrix\TelemetryService\HealthCheck\Data\$TargetMachineFQDN\log.txt`.

Pour activer le journal de débogage :

Modifiez `C:\Program Files\Citrix\CloudHealthCheck\CloudHealthCheck.exe.config`, mettez à jour `<add name="TraceLevelSwitch"value="3"/> to <add name`

="TraceLevelSwitch"value="4"/>, enregistrez le fichier et rouvrez Vérification de l'état du cloud.

Commentaires

Pour laisser des commentaires sur la vérification de l'état du cloud, répondez à l'enquête Citrix.

Journalisation de la configuration

May 17, 2024

> **Remarque :**
>
> Les enregistrements du journal de configuration s'affichent uniquement en anglais, quelle que soit la langue que vous sélectionnez pour votre compte Citrix Cloud. Les dates et heures associées à ces enregistrements sont au format MM/JJ/AA, exprimées en temps universel coordonné (UTC).

La journalisation de la configuration est une fonctionnalité qui consigne les modifications apportées à la configuration du déploiement Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service), ainsi qu'aux activités administratives dans une base de données de journalisation de Citrix Cloud. 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.

Dans ce Citrix DaaS, la journalisation de la configuration est toujours activée. Vous ne pouvez pas la désactiver.

À partir de l'interface de gestion Configuration complète, vous pouvez afficher le contenu du journal de configuration, filtré par plages de dates ou par recherche en texte intégral. Vous pouvez également générer un rapport CSV à l'aide de PowerShell. Dans cette console, vous ne pouvez ni modifier ni supprimer le contenu du journal. Vous pouvez utiliser le SDK Remote PowerShell pour planifier la suppression périodique des données du journal.

Mise à jour de la conservation des journaux de configuration DaaS

Afin de maintenir les performances des locataires DaaS, à compter du 9 septembre 2024, la durée de conservation des journaux de configuration sera fixée à 180 jours.

Les journaux datant de plus de 180 jours seront supprimés après le 9 septembre 2024. Alors que nous continuons à augmenter nos limites DaaS pour un seul locataire DaaS, cette mise en œuvre garantit les meilleures performances et la meilleure résilience pour nos clients.

Dans le cadre des meilleures pratiques, nous conseillons à nos clients de disposer d'un mécanisme d'exportation trimestriel. Pour cela, vous pouvez utiliser PowerShell (reportez-vous à la section Générer des rapports). Nous recommandons également à nos clients de planifier la suppression périodique des données (reportez-vous à la section Planifier la suppression périodique des données).

Autorisations requises (voir Administration déléguée) :

- Les administrateurs complets dans Citrix Cloud, ainsi que les administrateurs Cloud et les administrateurs en lecture seule de Citrix DaaS peuvent afficher les journaux de configuration dans la console **Gérer**.
- Les administrateurs complets et les administrateurs Cloud peuvent également télécharger un rapport CSV d'activités de journalisation à l'aide de PowerShell.

Qu'est-ce qui est journalisé

Les opérations suivantes sont enregistrées :

- Modifications de configuration et activités administratives initiées à partir des onglets **Gérer** et **Surveiller**
- Scripts PowerShell
- Demandes d'API REST

> **Remarque :**
>
> Vous ne pouvez pas voir les entrées de journal pour les opérations internes de la plateforme Citrix Cloud, telles que la configuration et la gestion de la base de données.

Les exemples de modifications apportées à la configuration journalisées comprennent l'utilisation de (création, modification, suppression des affectations) :

- 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 via la console **Gérer**

Exemples de modifications administratives journalisées :

- Gestion de la puissance d'une machine virtuelle ou d'un bureau utilisateur

- Fonctions de gestion ou de surveillance envoyant un message à un utilisateur

Les opérations suivantes ne sont pas enregistrées. (Beaucoup ne sont pas disponibles pour les administrateurs clients.)

- Opérations automatiques 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.
- Modifications apportées via le Registre ou à partir de sources autres que l'interface de gestion Configuration complète, Surveiller ou PowerShell.

Afficher le contenu du journal de configuration

Pour afficher le contenu du journal de configuration, procédez comme suit :

1. Connectez-vous à Citrix Cloud. Sélectionnez **Mes services > DaaS** dans le menu supérieur gauche.
2. Dans **Gérer > Configuration complète**, sélectionnez **Journalisation > Événements** dans le volet gauche.

Par défaut, l'affichage dans 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 une période personnalisée, ou en saisissant du texte dans la zone de recherche. Pour revenir à l'affichage standard après la recherche, désactivez le texte dans la zone Rechercher.
- Choisissez les colonnes à afficher à l'écran en sélectionnant l'icône **Colonnes à afficher** dans le coin supérieur droit du tableau. Par exemple, pour afficher l'adresse IP utilisée par l'administrateur pour accéder au DaaS, cliquez sur l'icône et ajoutez la colonne **IP client**.

Caractéristiques d'affichage :

- Les opérations de haut niveau créées lors de la gestion et de la surveillance sont répertoriées dans le volet central supérieur. Une opération de haut niveau se traduit par un ou plusieurs appels de service et de SDK PowerShell, qui sont des opérations de bas niveau. Lorsque vous sélectionnez une opération de haut niveau dans le panneau central supérieur, le panneau inférieur affiche les opérations de bas niveau.
- Si vous créez une opération de bas niveau dans PowerShell sans spécifier une opération de haut niveau parente, la journalisation de la configuration crée une opération de haut niveau de substitution.

- 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'a 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 vous demandez les journaux des cinq derniers jours et qu'un journal avec une heure de début dans les cinq derniers jours n'a pas de date de fin, il est inclus.
- Rappel : vous ne pouvez pas voir les entrées de journal pour les opérations internes de la plateforme Citrix Cloud, telles que la configuration et la gestion de la base de données.

Afficher les tâches liées aux opérations de catalogue de machines

Pour afficher les tâches liées aux opérations de catalogue de machines, accédez à **Gérer > Configuration complète > Journalisation > Tâches**. L'onglet **Tâches** affiche uniquement les tâches liées aux catalogues créés via Machine Creation Services (MCS) ou Provisioning Services (PVS). Plus précisément, vous verrez les tâches associées aux opérations suivantes du catalogue de machines :

- Créer des catalogues
- Cloner des catalogues
- Ajouter des machines
- Supprimer des machines
- Mettre à jour un catalogue (mettre à jour des images ou des machines)
- Restaurer des mises à jour de machines

> **Conseil :**
>
> L'onglet **Tâches** affiche uniquement les tâches liées aux modifications du schéma de provisioning (création ou modification d'un schéma de provisioning).

Une tâche peut être dans l'état suivant :

- Terminé
- Non démarré
- En cours d'exécution
- Annulé
- Échec
- Inconnu

Pour annuler une tâche en cours d'exécution, sélectionnez-la, puis cliquez sur **Annuler**. L'annulation prend un certain temps.

Voici des exemples de tâches consignées :

- Mise à jour de l'image terminée pour un certain catalogue
- Erreur lors de la mise à jour de l'image pour un certain catalogue
- Mise à jour de l'image annulée pour un certain catalogue
- Provisionnement de machines virtuelles sur un certain catalogue
- Suppression de machines virtuelles d'un certain catalogue
- Création d'un certain catalogue

Par défaut, l'affichage dans le panneau central affiche les tâches consignées par ordre chronologique (la plus récente des entrées en premier), en les séparant par date. Vous pouvez trier l'affichage par entête de colonne. Pour effacer les tâches terminées, cliquez sur **Effacer les tâches terminées** sous l'onglet **Tâches**. Pour choisir les colonnes à afficher à l'écran, sélectionnez l'icône **Colonnes à afficher** dans le coin supérieur droit du tableau.

Afficher les journaux d'API

Pour afficher les journaux d'API REST, accédez à **Gérer > Configuration complète > Journalisation > API**. L'onglet **API** affiche les demandes d'API REST effectuées pendant une certaine période.

Prenez en compte les informations suivantes :

- Les journaux d'API REST sont effacés une fois que vous êtes déconnecté de la console. (Ils sont également effacés si vous actualisez la fenêtre de votre navigateur.)
- Les demandes d'API correspondant à toutes les opérations de la console qui entraînent des appels d'API sont affichées dans l'onglet **API**.
- Les demandes d'API sont affichées par ordre chronologique (entrées les plus récentes en premier), séparées par date. Le nombre maximal de demandes d'API affichées est de 1 000.

Afficher les journaux PowerShell

Pour afficher les commandes PowerShell correspondant aux actions de l'interface utilisateur que vous avez effectuées au cours de la journée, accédez à l'onglet **Gérer > Configuration complète > Journalisation > 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.

Générer des rapports

Pour générer un rapport CSV ou HTML contenant des données de journal de configuration, utilisez les applets de commande PowerShell pour le service ConfigLogging dans le SDK Remote PowerShell Citrix Virtual Apps and Desktops. Pour plus de détails, consultez :

- `Export-LogReportCsv`
- `Export-LogReportHtml`

Planifier la suppression périodique des données

Utilisez le SDK Remote PowerShell pour spécifier la durée de conservation des données dans la base de données de journalisation de la configuration. (Cette fonctionnalité n'est pas disponible dans l'interface de gestion Configuration complète.) Dans Citrix DaaS, vous devez disposer d'un accès complet.

Dans l'applet de commande `Set-LogSite`, le paramètre `-LoggingDBPurgeDurationDays` spécifie combien de jours les données de la base de données de journalisation de la configuration sont conservées avant d'être supprimées automatiquement.

- Par défaut, la valeur de ce paramètre est 0. Une valeur zéro signifie que les données de la base de données de journalisation de la configuration ne sont jamais supprimées automatiquement.
- Lorsque vous définissez une valeur différente de zéro, la base de données est vérifiée une fois toutes les 120 minutes. Les données antérieures à la période de rétention sont supprimées.

Utilisez `Get-LogSite` pour afficher la valeur actuelle du paramètre.

Différences par rapport à Citrix Virtual Apps and Desktops sur site

Si vous avez déjà utilisé la journalisation de la configuration dans Virtual Apps and Desktops sur site, la version Citrix Cloud présente plusieurs différences. Dans Citrix Cloud :

- La journalisation de la configuration est toujours activée. Vous ne pouvez pas la désactiver. La journalisation obligatoire n'est pas disponible.
- Vous ne pouvez pas modifier l'emplacement de la base de données de journalisation de la configuration, car la base de données est gérée dans la plate-forme Citrix Cloud.
- Les affichages du journal de configuration n'incluent pas les opérations et les activités effectuées sur la plate-forme Citrix Cloud.
- PowerShell est votre seul choix pour créer un rapport CSV ou HTML des opérations consignées. Dans le produit sur site, les rapports peuvent être générés à partir de Citrix Studio ou de PowerShell.
- Vous ne pouvez pas supprimer le contenu du journal de configuration.

Administration déléguée

March 30, 2024

Vue d'ensemble

L'administration déléguée de Citrix Cloud vous permet de configurer les autorisations d'accès requises par tous vos administrateurs conformément à leur rôle dans votre organisation.

Par défaut, les administrateurs ont un accès complet. Cette configuration permet d'accéder à toutes les fonctions d'administration et de gestion client disponibles dans Citrix Cloud, ainsi qu'à tous les services souscrits. Pour personnaliser l'accès d'un administrateur :

- Configurez un accès personnalisé pour les autorisations de gestion générale d'un administrateur dans Citrix Cloud.

- Configurez un accès personnalisé pour les services souscrits. Dans Citrix DaaS, vous pouvez configurer un accès personnalisé lorsque vous invitez un nouvel administrateur. Vous pouvez modifier l'accès d'un administrateur ultérieurement.

Pour plus d'informations sur l'affichage de la liste des administrateurs et la définition des autorisations d'accès, consultez Gérer l'accès des administrateurs à Citrix Cloud.

Cet article explique comment configurer l'accès personnalisé dans Citrix DaaS.

Administrateurs, rôles et étendues

L'administration déléguée utilise trois concepts pour l'accès personnalisé : les administrateurs, les rôles et les étendues.

- **Administrateurs :** un administrateur représente une personne identifiée par sa connexion Citrix Cloud, qui est généralement une adresse électronique. 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. Ces autorisations permettent certaines tâches uniques à Citrix DaaS. Par exemple, le rôle Administrateur du groupe de mise à disposition est autorisé à créer un groupe de mise à disposition et à supprimer un bureau d'un groupe de mise à disposition, et dispose d'autres autorisations associées. Un administrateur peut avoir plusieurs rôles. Un administrateur peut être Administrateur du groupe de mise à disposition et Administrateur du catalogue de machines.

  Citrix DaaS offre plusieurs rôles intégrés avec accès personnalisé. Vous ne pouvez pas modifier les autorisations de ces rôles intégrés, ni supprimer ces rôles.

  Vous pouvez créer vos propres rôles d'accès personnalisés correspondants aux besoins de votre organisation et déléguer des autorisations avec plus de détails. Utilisez les rôles personnalisés pour allouer des autorisations à la précision d'une action ou d'une tâche. Vous pouvez supprimer un rôle personnalisé uniquement s'il n'est pas affecté à un administrateur.

  Vous pouvez modifier les rôles attribués à un administrateur.

  Un rôle est toujours associé à une étendue.

- **Étendues :** une étendue représente une collection d'objets. Les étendues permettent de regrouper des objets de manière pertinente pour votre organisation. Les objets peuvent être dans plusieurs étendues.

  Il existe une étendue intégrée appelée « Tous » qui contient tous les objets. Les administrateurs Citrix Cloud et Service d'assistance sont toujours associés à l'étendue Tous. Cette étendue ne peut pas être modifiée pour ces administrateurs.

Lorsque vous invitez (ajoutez) un administrateur pour ce service, un rôle est toujours associé à une étendue (par défaut, l'étendue Tous).

Les étendues sont créées et supprimées dans l'interface **Gérer > Configuration complète**. Les paires rôle/étendue sont affectées dans la console Citrix Cloud.

Une étendue n'est pas affichée pour les administrateurs avec accès complet. Par définition, ces administrateurs ont accès à tous les objets de services d'abonnements et Citrix Cloud gérés par le client.

Étendues et rôles intégrés

Citrix DaaS possède les rôles intégrés suivants.

- **Administrateur Cloud :** peut effectuer toutes les tâches pouvant être lancées à partir de Citrix DaaS.

  Peut voir les onglets **Gérer** et **Surveiller** dans la console. Ce rôle est toujours combiné à l'étendue Tous. Vous ne pouvez pas changer l'étendue.

  Le nom de ce rôle peut porter à confusion. Un administrateur cloud avec accès personnalisé ne peut pas effectuer de tâches de niveau Citrix Cloud (les tâches Citrix Cloud nécessitent un accès complet).

- **Administrateur en lecture seule :** peut afficher tous les objets dans les étendues spécifiées (en plus des informations générales), mais ne peut rien modifier. Par exemple, un administrateur en lecture seule avec l'étendue = Londres peut voir tous les objets globaux et les objets appartenant à l'étendue 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).

  Peut voir les onglets **Gérer** et **Surveiller** dans la console.

- **Administrateur du service d'assistance :** peut afficher des groupes de mise à disposition et gérer les sessions et les 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.

  Peut voir l'onglet **Surveiller** dans la console. Ne peut pas voir l'onglet **Gérer**. Ce rôle est toujours combiné à l'étendue Tous. Vous ne pouvez pas changer l'étendue.

- **Administrateur du catalogue de machines :** peut créer et gérer des catalogues de machines et y provisionner les machines. Peut gérer les images de base et installer le logiciel, mais ne peut pas assigner les applications ou bureaux aux utilisateurs.

Peut voir les onglets **Surveiller** et **Gérer** dans la console. Ne peut pas voir l'onglet **Surveiller**. Vous pouvez changer l'étendue.

- **Administrateur du groupe de mise à disposition :** peut mettre à disposition des applications, des bureaux et des machines. Peut également gérer les sessions associées. Il peut gérer les configurations d'applications et de bureaux, telles que les stratégies et les paramètres de gestion de l'alimentation.

  Peut voir les onglets **Surveiller** et **Gérer** dans la console. Vous pouvez changer l'étendue.

  > **Remarque :**
  >
  > Pour changer le nom d'affichage d'un bureau en tant qu'administrateur de groupe de mise à disposition, vous devez disposer de l'autorisation **Mettre à jour une machine**. Cette autorisation est nécessaire, car la modification du nom d'affichage implique la mise à jour des propriétés de la machine.

- **Administrateur hôte :** peut gérer les connexions hôtes et leurs paramètres de ressources associés. Impossible de mettre à disposition des machines, applications ou bureaux aux utilisateurs.

  Peut voir l'onglet **Gérer** dans la console. Ne peut pas voir l'onglet **Surveiller**. Vous pouvez changer l'étendue.

- **Session Administrator :** peut afficher les groupes de mise à disposition surveillés et gérer leurs sessions et machines associées.

  Peut voir l'onglet **Surveiller** dans la console. Ne peut pas voir l'onglet **Gérer**. Vous ne pouvez pas changer l'étendue.

- **Full Administrator :** peut effectuer toutes les tâches et toutes les opérations. Un administrateur complet est toujours associé à l'étendue **Toutes les étendues**.

  Peut voir les onglets **Gérer** et **Surveiller** dans la console. Ce rôle est toujours combiné à l'étendue **Toutes les étendues**. Vous ne pouvez pas changer l'étendue.

- **Full Monitor Administrator :** a un accès complet à toutes les vues et commandes de l'onglet **Surveiller**.

  Peut voir l'onglet **Surveiller** dans la console. Ne peut pas voir l'onglet **Gérer**. Vous ne pouvez pas changer l'étendue.

- **Probe Agent Administrator :** a accès aux API de Probe Agent.

  Peut voir les onglets **Surveiller** et **Gérer** dans la console. A accès en lecture seule à la page **Applications**, mais ne peut accéder à aucune autre vue.

Le tableau suivant récapitule les onglets de la console visibles pour chaque rôle avec accès personnalisé dans Citrix DaaS et indique si le rôle peut être utilisé avec des étendues personnalisées.

Rôle administrateur à accès personnalisé	Peut voir l'onglet **Gérer** dans la console ?	Peut voir l'onglet **Surveiller** dans la console ?	Le rôle peut-il être utilisé avec des étendues personnalisées ?
Administrateur Cloud	Oui	Oui	Non
Administrateur en lecture seule	Oui	Oui	Oui
Administrateur du service d'assistance	Non	Oui	Non
Administrateur du catalogue de machines	Oui	Oui	Oui
Administrateur du groupe de mise à disposition	Oui	Oui	Oui
Administrateur hôte	Oui	Non	Oui
Session Administrator	Non	Oui	Non
Administrateur complet	Oui	Oui	Non
Full Monitor Administrator	Non	Oui	Non
Administrateur Probe Agent	Oui	Oui	Non

> **Remarque :**
>
> Les rôles d'administrateur avec accès personnalisé, à l'exception d'Administrateur Cloud et Administrateur du service d'assistance, ne sont pas disponibles pour Citrix Virtual Apps and Desktops Standard for Azure, Virtual Apps Essentials, and Virtual Desktops Essentials.

Pour afficher les autorisations associées à un rôle :

1. Connectez-vous à Citrix Cloud. Sélectionnez **Mes services > DaaS** dans le menu supérieur gauche.
2. Dans **Gérer > Configuration complète**, sélectionnez **Administrateurs** dans le volet gauche.
3. Sélectionnez l'onglet **Rôles** .
4. Sélectionnez un rôle dans le volet central supérieur. L'onglet **Définition du rôle** dans le volet inférieur répertorie les catégories et les autorisations. Sélectionnez une catégorie pour voir les

autorisations spécifiques. L'onglet **Administrateurs** répertorie les administrateurs auxquels le rôle sélectionné a été attribué.

Problème connu : une entrée Administrateur complet n'affiche pas le jeu d'autorisations correct pour un administrateur Citrix DaaS à accès complet.

Nombre d'administrateurs dont vous avez besoin

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 d'accès personnalisée. Dans ce cas, chaque administrateur dispose d'un accès complet, qui a toujours l'étendue Tous.
- 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 ont un accès complet 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 un certain département. Dans ce cas, créez de nouvelles étendues, ainsi que des administrateurs avec le rôle à accès personnalisé et les étendues appropriés.

Résumé de la gestion des administrateurs

La configuration des administrateurs pour Citrix DaaS suit cette séquence :

1. Si vous souhaitez que l'administrateur ait un rôle autre qu'un administrateur complet (qui couvre tous les services souscrits dans Citrix Cloud) ou un rôle intégré, créez un rôle personnalisé.
2. Si vous souhaitez que l'administrateur ait une étendue autre que Tous (et qu'une autre étendue est autorisée pour le rôle prévu mais qu'elle n'a pas encore été créée), créez des étendues.
3. Depuis Citrix Cloud, invitez un administrateur. Si vous souhaitez que le nouvel administrateur dispose d'un accès autre que l'accès complet par défaut, spécifiez une paire rôle d'accès/étendue personnalisée.

Plus tard, si vous voulez changer l'accès d'un administrateur (rôles et étendue), voir Configurer un accès personnalisé.

Ajouter un administrateur

Pour ajouter (inviter) des administrateurs, suivez les instructions Ajouter des administrateurs à un compte Citrix Cloud. Un sous-ensemble de ces informations est repris ici.

> **Important :**
>
> Ne confondez pas « personnalisé » et « accès personnalisé ».
>
> - Lors de la création d'administrateurs et de l'attribution de rôles pour Citrix DaaS dans la console Citrix Cloud, le terme « accès personnalisé » inclut à la fois les rôles intégrés et les rôles personnalisés supplémentaires créés dans l'interface **Gérer > Configuration complète** du service.
> - Dans l'interface **Gérer > Configuration complète** du service, « personnalisé » différencie simplement ce rôle d'un rôle intégré.

Le workflow général pour l'ajout d'administrateurs est le suivant :

1. Connectez-vous à Citrix Cloud, puis sélectionnez **Gestion des identités et des accès** dans le menu supérieur gauche.
2. Sur la page **Gestion des identités et des accès**, sélectionnez **Administrateurs**. L'onglet **Administrateurs** répertorie tous les administrateurs actuels du compte.
3. Dans l'onglet **Administrateurs**, sélectionnez votre type d'identité, saisissez l'adresse e-mail de l'administrateur, puis cliquez sur **Inviter**.

- Sélectionnez **Accès complet** si vous souhaitez que l'administrateur dispose d'un accès complet. De cette façon, l'administrateur peut accéder à toutes les fonctions d'administrateur client dans Citrix Cloud et à tous les services auxquels il est abonné.
- Sélectionnez **Accès personnalisé** si vous souhaitez que l'administrateur dispose d'un accès limité. Vous pouvez ensuite sélectionner un rôle d'accès personnalisé et une paire d'étendue. De cette façon, l'administrateur dispose des autorisations prévues lorsqu'il se connecte à Citrix Cloud.

1. Cliquez sur **Envoyer invitation**. Citrix Cloud envoie une invitation à l'adresse e-mail et ajoute l'administrateur à la liste une fois que l'administrateur a terminé l'intégration.

Lors de la réception de l'e-mail, l'administrateur clique sur le lien **Se connecter** pour accepter l'invitation.

Pour plus d'informations sur l'ajout d'administrateurs, consultez Gérer les administrateurs Citrix Cloud.

Vous pouvez également accéder à **Gérer > Configuration complète > Administrateurs > Administrateurs** et cliquer sur **Ajouter un administrateur**. Vous accédez directement à **Gestion des identités et des accès > Administrateurs**, qui s'ouvre dans un nouvel onglet de navigateur. Une fois que vous avez fini d'y ajouter des administrateurs, fermez l'onglet et revenez à la console pour poursuivre vos autres tâches de configuration.

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).

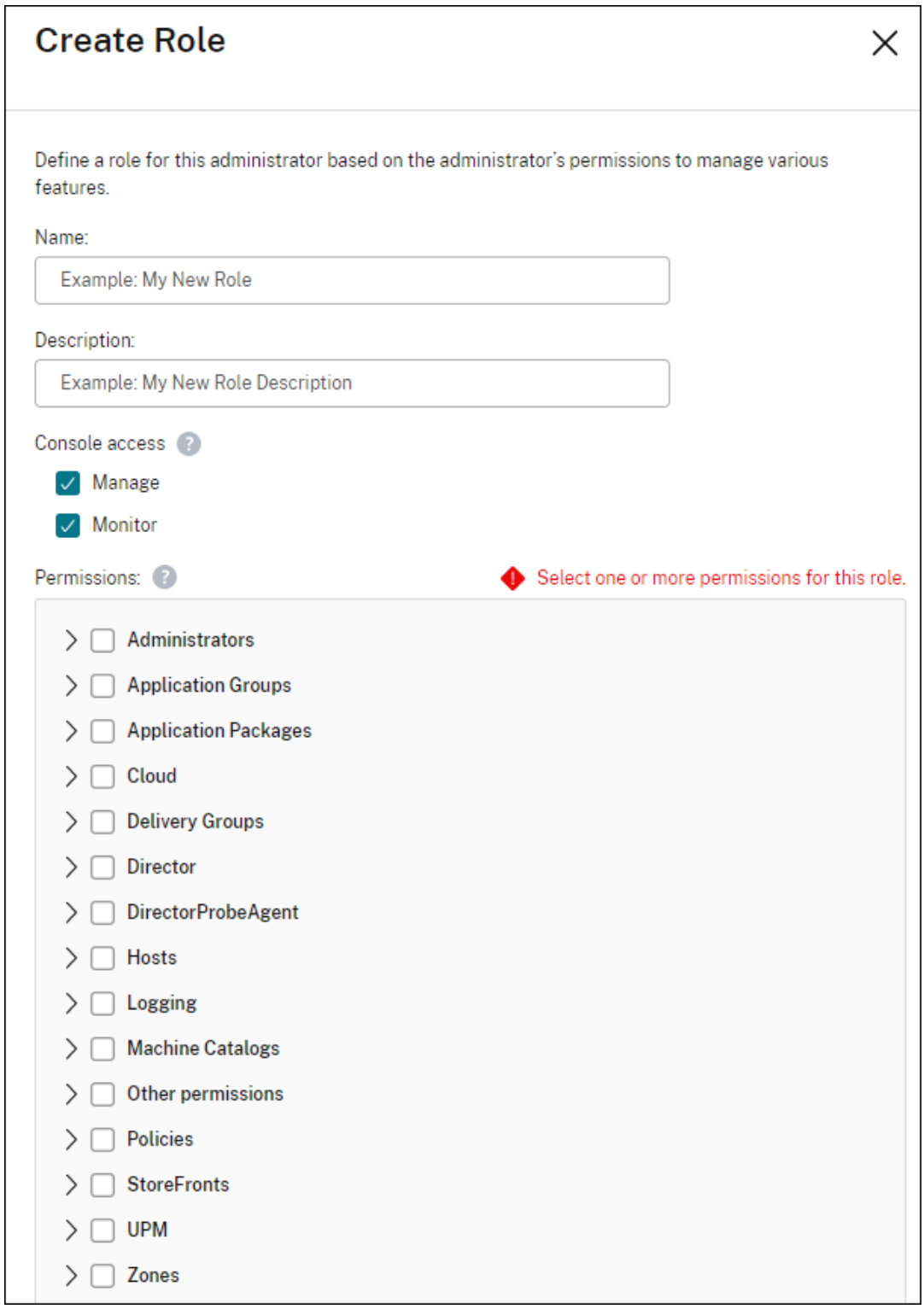
Les noms de rôle personnalisés peuvent contenir jusqu'à 64 caractères Unicode. Les noms ne peuvent pas contenir les caractères suivants : barre oblique inverse, barre oblique, point-virgule, deux-points, symbole de la livre, virgule, astérisque, point d'interrogation, signe égal, flèche gauche, flèche droite, barre verticale, crochet gauche ou droit, parenthèse gauche ou droite, guillemets et apostrophe.

Les descriptions de rôle peuvent contenir jusqu'à 256 caractères Unicode.

1. Connectez-vous à Citrix Cloud si vous ne l'avez pas déjà fait. Sélectionnez **Mes services > DaaS** dans le menu supérieur gauche.
2. Dans **Gérer > Configuration complète**, sélectionnez **Administrateurs** dans le volet gauche.
3. Sélectionnez l'onglet **Rôles** .
4. Suivez les instructions relatives à la tâche que vous souhaitez effectuer :

    - **Afficher les détails d'un rôle :** sélectionnez le rôle dans le volet central. La partie inférieure du panneau central répertorie les types d'objets et les autorisations associées pour le rôle. Sélectionnez l'onglet **Administrateurs** dans le volet inférieur pour afficher une liste des administrateurs détiennent actuellement ce rôle.
    - **Pour créer un rôle personnalisé :** sélectionnez **Créer un rôle** dans la barre d'actions. Configurez les paramètres comme suit :

        - Entrez un nom et une description.
        - Configurez l'accès aux consoles. Déterminez quelles consoles sont visibles par les administrateurs. Vous pouvez continuer sans sélectionner de console. Dans ce cas, les administrateurs ayant le rôle ne peuvent pas accéder à **Gérer** et **Surveiller**, mais peuvent accéder à des objets, les afficher ou les gérer via des kits SDK et des API.
        - Sélectionnez les types d'objets et les autorisations. Pour accorder l'autorisation d'accès complet à un type d'objet, activez sa case à cocher. Pour accorder une autorisation à un niveau granulaire, développez le type d'objet, puis sélectionnez **Lecture seule** ou des objets individuels sous **Gérer** dans le type.



- **Copier un rôle :** sélectionnez le rôle dans le volet central, puis sélectionnez **Copier rôle** dans la barre d'actions. Modifiez le nom, la description, les types d'objet et les autorisations nécessaires. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

- **Modifier un rôle personnalisé :** sélectionnez le rôle dans le volet central, puis sélectionnez **Modifier un rôle** dans la barre d'actions. Modifiez le nom, la description, les types d'objet et les autorisations nécessaires. Vous ne pouvez pas modifier un rôle intégré. Lorsque vous avez terminé, sélectionnez **Enregistrer**.
- **Supprimer un rôle personnalisé :** sélectionnez le rôle dans le volet central, puis sélectionnez **Supprimer un rôle** dans la barre d'actions. Lorsque vous y êtes invité, confirmez la suppression. Vous ne pouvez pas supprimer un rôle intégré. Vous ne pouvez pas supprimer un rôle personnalisé s'il est affecté à un administrateur.

Créer et gérer des étendues

Par défaut, tous les rôles ont l'étendue Tous pour leurs objets pertinents. Par exemple, un administrateur de groupe de mise à disposition peut gérer tous les groupes de mise à disposition. Pour certains rôles d'administrateur, vous pouvez créer une étendue permettant à ce rôle d'administrateur d'accéder à un sous-ensemble d'objets pertinents. Par exemple, vous pouvez souhaiter donner à un administrateur de catalogue de machines un accès aux catalogues contenant un certain type de machines uniquement, plutôt qu'à tous les catalogues.

- Les administrateurs avec accès complet ou les administrateurs cloud avec accès personnalisé peuvent créer des étendues pour les rôles Administrateur en lecture seule, Administrateur du catalogue de machines, Administrateur du groupe de mise à disposition et Administrateur hôte.
- Des étendues ne peuvent pas être créées pour les administrateurs avec accès complet, ni pour les administrateurs cloud ou les administrateurs du centre d'assistance. Ces administrateurs ont toujours l'étendue Tous.

Règles de création et de gestion des étendues :

- Les noms d'étendue peuvent contenir jusqu'à 64 caractères Unicode. Les noms 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 modifiez une étendue, n'oubliez pas que la suppression des objets dans l'étendue peut rendre ces objets inaccessibles à un 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 :

1. Connectez-vous à Citrix Cloud. Sélectionnez **Mes services > DaaS** dans le menu supérieur gauche.

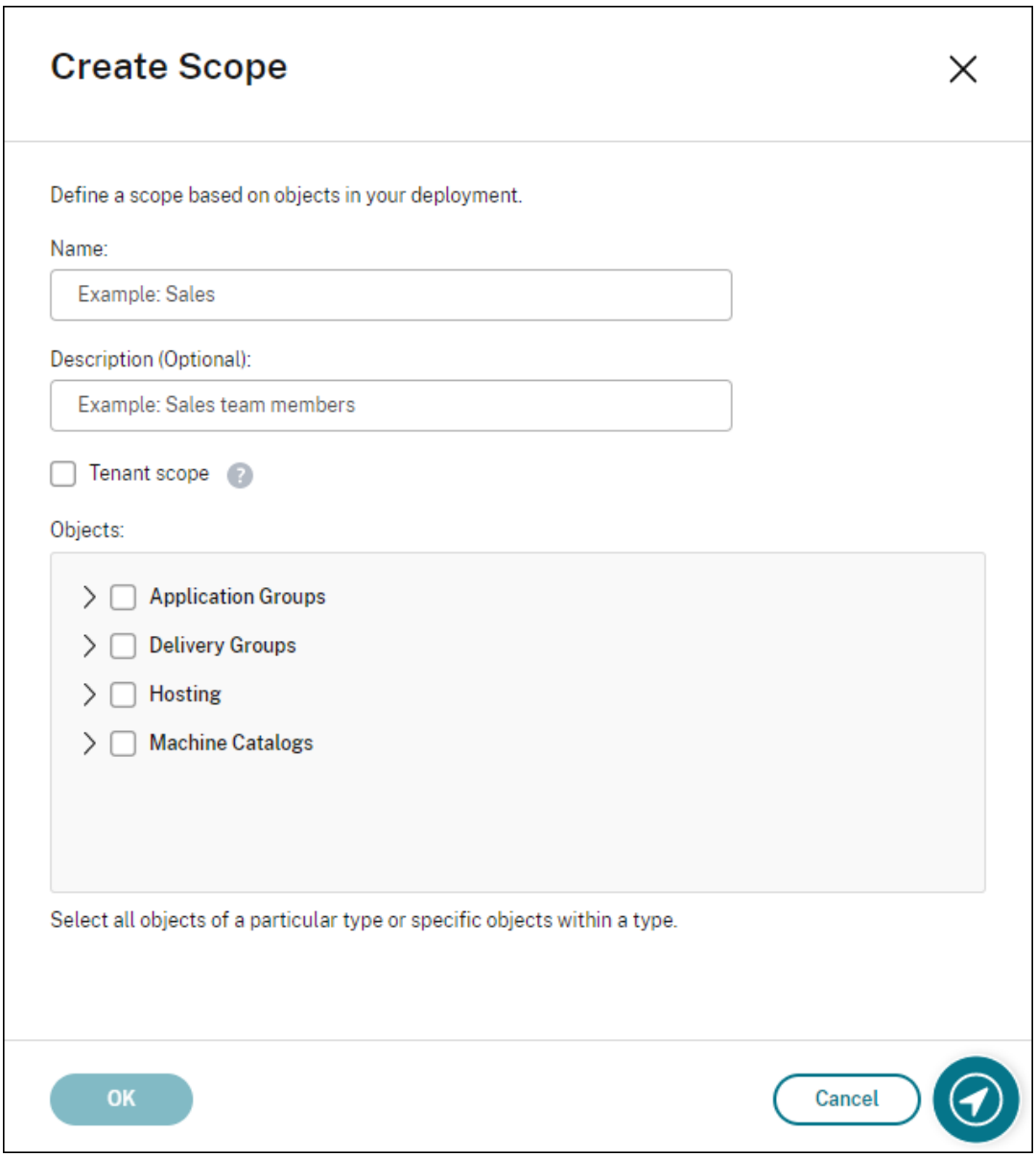
2. Dans **Gérer > Configuration complète**, sélectionnez **Administrateurs** dans le volet gauche.
3. Sélectionnez l'onglet **Étendues** .
4. Suivez les instructions relatives à la tâche que vous souhaitez effectuer :

    - **Afficher les détails de l'étendue :** sélectionnez l'étendue. La partie inférieure du panneau répertorie les objets et les administrateurs disposant de cette étendue.
    - **Créer une étendue :** sélectionnez **Créer une étendue** dans la barre d'actions. Entrez un nom et une description. Les objets sont répertoriés par type, tels que le groupe de mise à disposition et le catalogue de machines.
        - Pour inclure tous les objets d'un type particulier (par exemple, tous les groupes de mise à disposition), sélectionnez la case du type d'objet.
        - Pour inclure des objets individuels d'un type donné, développez le type, puis sélectionnez les cases des objets individuels (par exemple, des groupes de mise à disposition spécifiques).

            > **Remarque :**
            >
            > Les groupes d'applications, les groupes de mise à disposition ou les catalogues de machines sont affichés dans des structures de dossiers conformes à leur gestion dans DaaS. Vous pouvez sélectionner un dossier pour sélectionner tous ses objets ou développer un dossier pour sélectionner des objets spécifiques.

        - Pour créer un client locataire, activez la case à cocher **Étendue du locataire**. Si cette option est sélectionnée, le nom que vous avez saisi pour l'étendue est le nom du locataire. Pour plus d'informations sur l'étendue du locataire, consultez Gestion des locataires.

    Lorsque vous avez terminé, sélectionnez **OK**.



- **Copier une étendue :** sélectionnez l'étendue dans le volet central, puis sélectionnez **Copier étendue** dans la barre d'actions. Modifiez le nom, la description. Modifiez les types d'objets et les objets, si nécessaire. Lorsque vous avez terminé, sélectionnez **Enregistrer**.
- **Modifier une étendue :** sélectionnez l'étendue dans le volet central, puis sélectionnez **Modifier l'étendue** dans la barre d'actions. Modifiez le nom, la description, les types d'objet et les objets, si nécessaire. Lorsque vous avez terminé, sélectionnez **Enregistrer**.
- **Supprimer une étendue :** sélectionnez l'étendue dans le volet central, puis sélectionnez **Supprimer l'étendue** dans la barre d'actions. Lorsque vous y êtes invité, confirmez la suppression.

> Vous ne pouvez pas supprimer une étendue si elle est affectée à un rôle. Si vous tentez de le faire, un message d'erreur indique que vous ne disposez pas de l'autorisation. En fait, l'erreur se produit parce que la paire rôle/étendue qui utilise cette étendue est attribuée à un administrateur. Supprimez d'abord l'attribution de cette paire rôle/étendue pour tous les administrateurs qui l'utilisent. Supprimez ensuite l'étendue dans la console **Gérer**.

Une fois que vous avez créé une étendue, elle apparaît dans la liste **Accès personnalisé** dans la console Citrix Cloud. Vous pouvez ensuite la sélectionner lorsque vous attribuez un rôle à un administrateur.

Par exemple, supposons que vous créez une étendue nommée CAO, puis que vous sélectionnez les catalogues contenant des machines adaptées aux applications de CAO. Lorsque vous revenez à la console Citrix Cloud et que vous sélectionnez **Modifier les étendues** pour un rôle, la liste des étendues disponibles affiche l'étendue CAO que vous avez créée précédemment.

L'administrateur Cloud et l'administrateur du centre d'assistance ont toujours l'étendue Tous, donc l'étendue CAO ne s'applique pas à eux.

Gestion des locataires

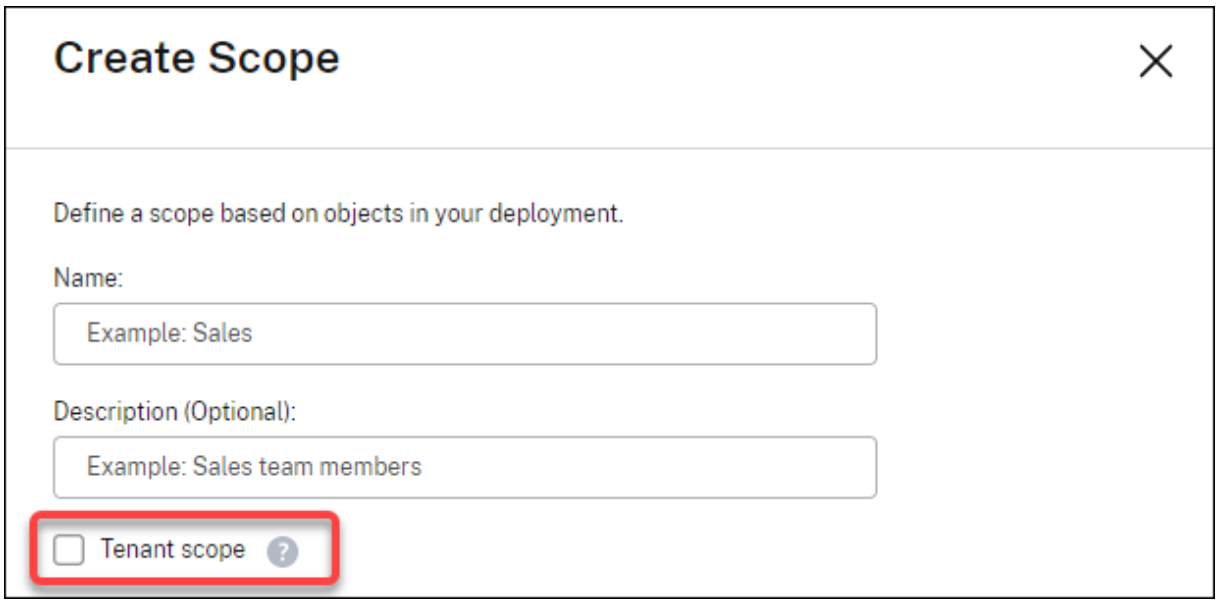
À l'aide de l'interface de gestion Configuration complète, vous pouvez créer des locataires mutuellement exclusifs sous un seul Citrix DaaS. Pour ce faire, créez des étendues de locataire dans **Administrateurs > Étendues** et associez des objets de configuration associés, tels que des catalogues de machines et des groupes de mise à disposition, à ces locataires. Par conséquent, les administrateurs ayant accès à un client peuvent gérer uniquement les objets associés au locataire.

Cette fonctionnalité est utile, par exemple, si votre organisation :

- dispose de différents silos métier (divisions indépendantes ou équipes de gestion informatique distinctes) ou
- possède plusieurs sites et souhaite conserver la même configuration dans une seule instance Citrix DaaS.

L'interface vous permet de filtrer les clients locataires par nom. Par défaut, l'interface affiche des informations sur tous les clients locataires. Pour afficher des informations sur un locataire spécifique, sélectionnez ce locataire dans la liste située dans le coin supérieur droit.

Créer un client locataire Pour créer un client locataire, sélectionnez **Étendue du locataire** lors de la création d'une étendue. En sélectionnant cette option, vous créez un type d'étendue unique qui s'applique aux objets dans les scénarios où vous partagez une instance Citrix DaaS entre différentes unités commerciales, chacune de ces unités commerciales étant indépendante des autres. Une fois que vous avez créé une étendue de locataire, vous ne pouvez pas modifier le type d'étendue.



L'onglet **Étendues** affiche tous les éléments d'étendue. La seule différence entre les étendues standard et les étendues du locataire se trouve dans la colonne **Type**. Un champ de colonne vide indique une étendue normale. Vous pouvez cliquer sur la colonne **Type** pour trier les éléments d'étendue si nécessaire.

Pour afficher les ressources (objets) attachées à une étendue, sélectionnez **Administrateurs** dans le volet gauche. Sous l'onglet **Étendues**, sélectionnez l'étendue, puis sélectionnez **Modifier l'étendue** dans la barre d'actions.

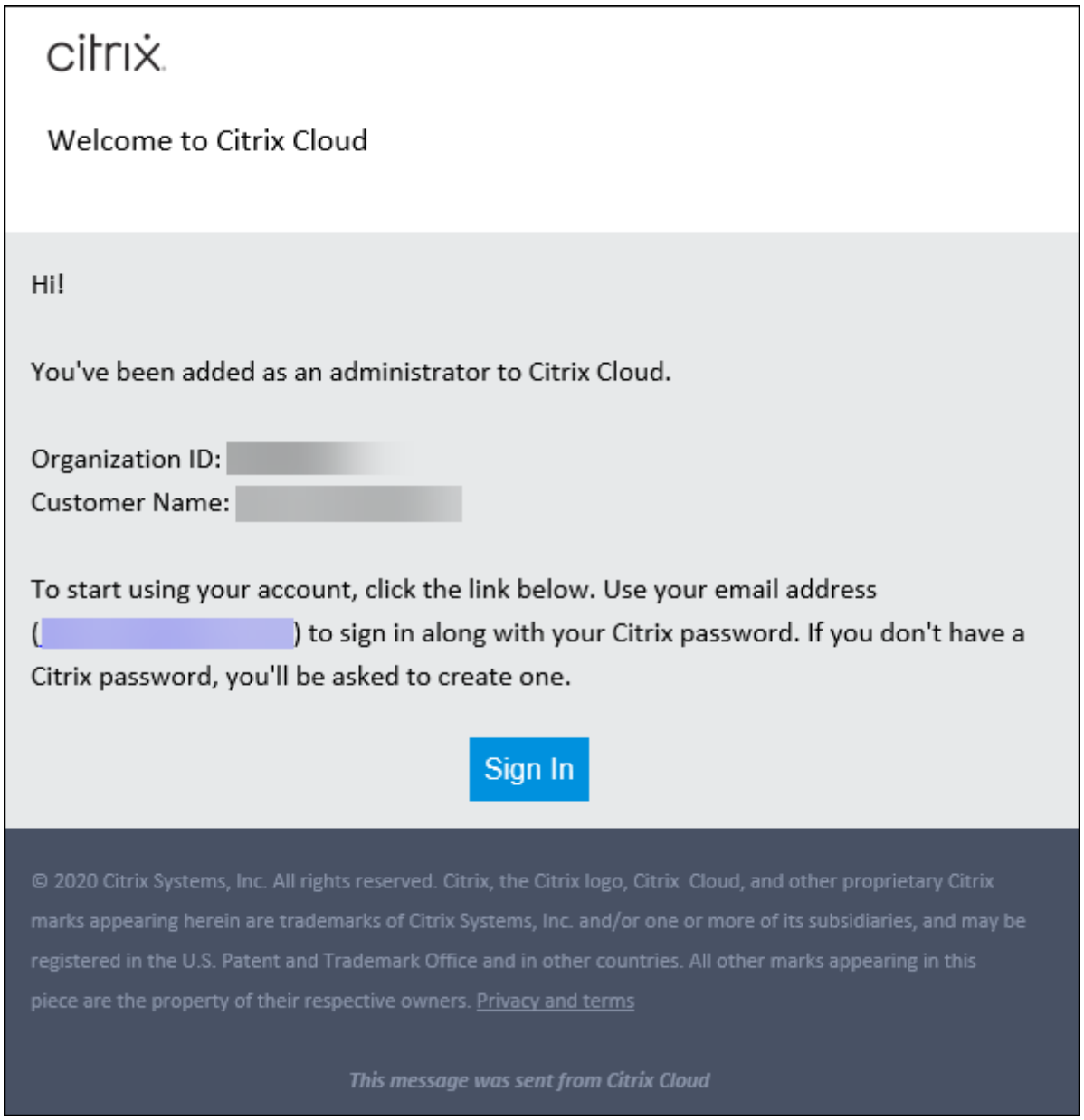
> **Conseil :**
>
> La propriété du locataire est attribuée au niveau de l'étendue. Les catalogues de machines, les groupes de mise à disposition, les applications et les connexions héritent de la propriété du locataire de l'étendue applicable.

Lorsque vous utilisez une étendue de locataire, tenez compte des points suivants :

- La propriété du locataire est attribuée dans l'ordre suivant : **Hébergement > Catalogues de machines > Groupes de mise à disposition > Applications**. Les objets de niveau inférieur dépendent d'objets de niveau supérieur pour hériter de la propriété du locataire. Par exemple, lorsque vous sélectionnez un groupe de mise à disposition, vous devez sélectionner l'hébergement et le catalogue de machines associés. Sinon, le groupe de mise à disposition ne peut pas hériter de la propriété du locataire.
- Après avoir créé une étendue de locataire, vous pouvez modifier les attributions de locataires en modifiant les objets. Lorsqu'une attribution de locataire est modifiée, elle est toujours soumise à la contrainte selon laquelle elle doit être attribuée aux mêmes locataires ou à un sous-ensemble de ces locataires. Toutefois, les objets de niveau inférieur ne sont pas réévalués lorsque les attributions de locataires changent. Assurez-vous que la restriction des

objets est correctement appliquée lorsque vous modifiez les attributions de locataires. Par exemple, si un catalogue de machines est disponible pour `TenantA` et `TenantB`, vous pouvez créer un groupe de mise à disposition pour `TenantA` et un pour `TenantB`. (`TenantA` et `TenantB` sont tous deux associés à ce catalogue de machines.) Vous pouvez ensuite modifier le catalogue de machines pour qu'il soit associé uniquement à `TenantA`. Par conséquent, le groupe de mise à disposition associé à `TenantB` devient non valide.

Configurer un accès personnalisé pour les administrateurs Après avoir créé des étendues de locataires, configurez un accès personnalisé pour les administrateurs respectifs. Pour plus d'informations, consultez Configurer un accès personnalisé pour un administrateur. Citrix Cloud envoie une invitation aux administrateurs clients que vous avez spécifiés et les ajoute à la liste. Lorsqu'ils reçoivent l'e-mail, ils cliquent sur **Se connecter** pour accepter l'invitation. Lorsqu'ils ouvrent une session sur l'interface de gestion **Configuration complète**, ils voient les ressources associées aux paires rôle/étendue attribuées.



Les administrateurs ayant accès à un locataire peuvent gérer uniquement les objets (par exemple, catalogue de machines, groupe de mise à disposition) associés au locataire.

Configurer un accès personnalisé pour un administrateur

Cette fonctionnalité vous permet de configurer les autorisations d'accès des administrateurs existants ou des administrateurs que vous invitez en fonction de leur rôle dans votre organisation.

Les modifications apportées aux autorisations d'accès prennent effet au bout de 5 minutes. Si vous vous déconnectez de l'interface de gestion Configuration complète puis que vous vous y reconnectez, les modifications prennent effet immédiatement. Dans les scénarios où les administrateurs continu-

ent d'utiliser l'interface de gestion après que les modifications ont pris effet sans s'y reconnecter, un avertissement s'affiche lorsqu'ils tentent d'accéder aux éléments pour lesquels ils ne disposent plus d'autorisations.

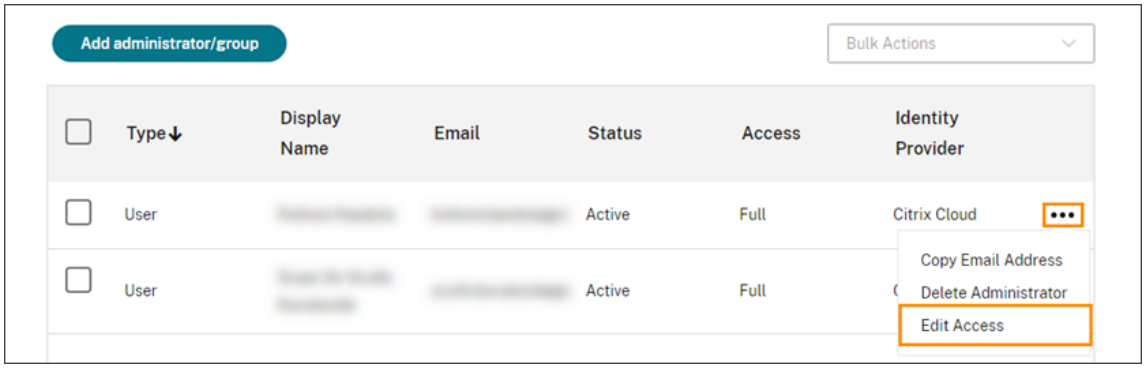
Par défaut, lorsque vous invitez des administrateurs, ils disposent d'un accès complet. L'accès complet permet à l'administrateur de gérer tous les services souscrits et toutes les opérations Citrix Cloud (comme l'invitation d'administrateurs supplémentaires). Un déploiement Citrix Cloud nécessite au moins un administrateur avec un accès complet.

Vous pouvez également accorder un accès personnalisé lorsque vous invitez un administrateur. L'accès personnalisé permet à l'administrateur de gérer uniquement les services et les opérations que vous spécifiez.

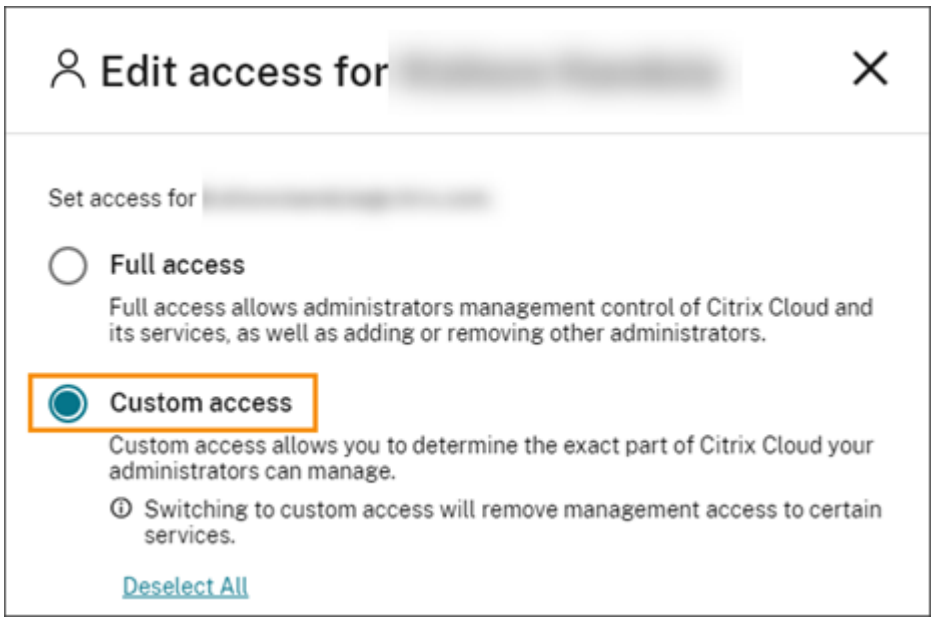
Lorsque vous créez un rôle ou une étendue dans Citrix DaaS, il/elle apparaît dans la liste d'accès personnalisés et peut être sélectionné(e). Lorsque vous sélectionnez un rôle pour un administrateur, vous pouvez modifier les étendues selon vos besoins pour refléter le rôle de l'administrateur au sein de votre organisation.

Pour configurer un accès personnalisé pour un administrateur :

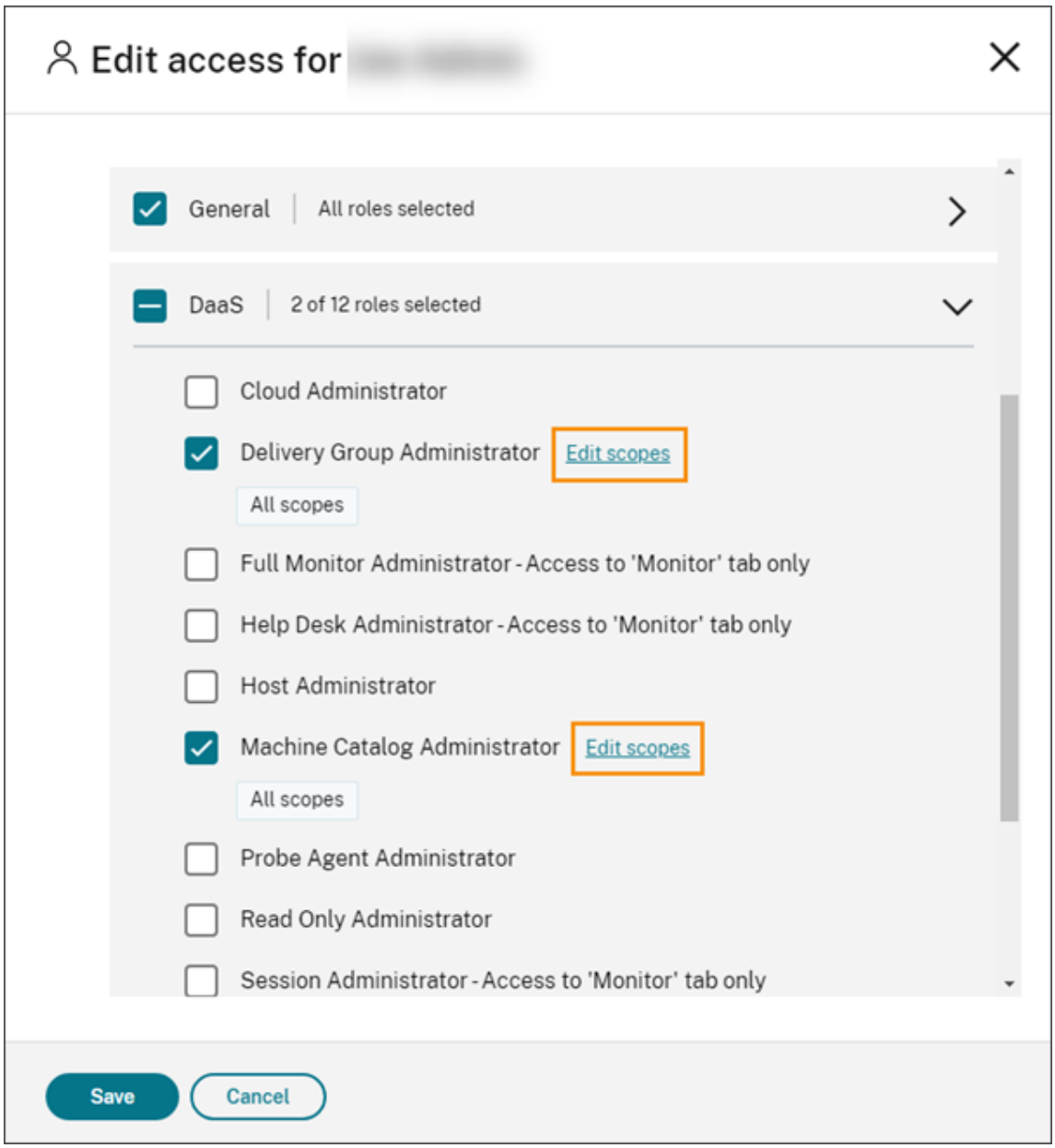
1. Connectez-vous à Citrix Cloud. Sélectionnez **Gestion des identités et des accès** > **Administrateurs** dans le menu en haut à gauche.
2. Recherchez l'administrateur que vous souhaitez gérer, cliquez sur le menu d'ellipse et sélectionnez **Modifier l'accès**.



3. Sélectionnez **Accès personnalisé**.

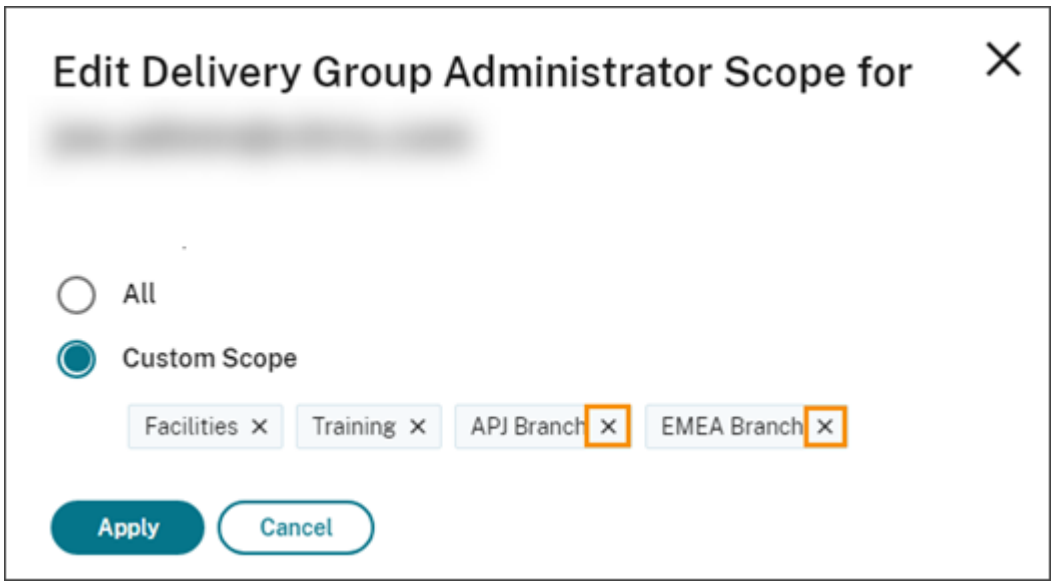


4. Sous **DaaS**, cochez ou décochez les cases à côté d'un ou de plusieurs rôles. Pour modifier les étendues associées à un rôle attribué, sélectionnez **Modifier les étendues**.

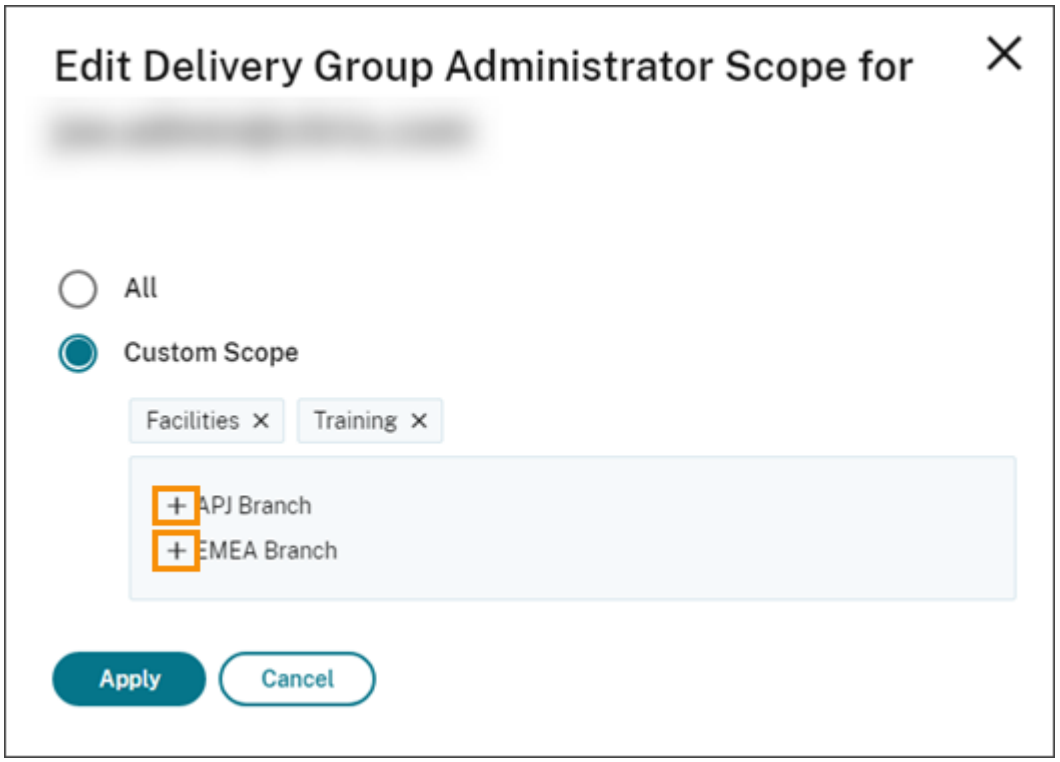


Par défaut, toutes les étendues sont sélectionnées pour chaque rôle sélectionné, comme indiqué par le libellé **Toutes les étendues**.

5. Pour spécifier les étendues d'un rôle sélectionné, sélectionnez **Étendue personnalisée**, puis ajoutez ou supprimez les étendues appropriées. Par défaut, toutes les étendues personnalisées sont ajoutées à un rôle. Pour supprimer une étendue, cliquez sur l'icône X sur l'étendue.



Les étendues qui ont été supprimées et qui peuvent être ajoutées au rôle apparaissent dans une liste en dessous des étendues déjà ajoutées. Pour ajouter une étendue au rôle, sélectionnez l'icône + correspondant à l'étendue.



6. Lorsque vous avez fini de sélectionner les étendues, sélectionnez **Appliquer**.
7. Sélectionnez **Enregistrer** pour enregistrer les rôles sélectionnés pour l'administrateur.

Différences par rapport à Citrix Virtual Apps and Desktops sur site

Si vous connaissez l'administration déléguée dans Citrix Virtual Apps and Desktops sur site, la version de Citrix DaaS présente plusieurs différences.

Dans Citrix Cloud :

- Les administrateurs sont identifiés par leur connexion Citrix Cloud, plutôt que par leur compte Active Directory. Vous pouvez créer des paires rôle/étendue pour des individus Active Directory, mais pas pour des groupes.
- Les administrateurs sont créés, configurés et supprimés dans la console Citrix Cloud, plutôt que dans Citrix DaaS.
- Les paires rôle/étendue sont attribuées aux administrateurs dans la console Citrix Cloud, plutôt que dans Citrix DaaS.
- Les rapports ne sont pas disponibles. Vous pouvez afficher les informations d'administrateur, de rôle et d'étendue dans l'interface **Gérer > Configuration complète** du service.
- L'accès personnalisé Administrateur Cloud est similaire à un administrateur complet dans la version locale. Les deux disposent d'autorisations complètes de gestion et de surveillance pour la version Citrix Virtual Apps and Desktops utilisée.

  Toutefois, dans Citrix DaaS, il n'existe aucun rôle d'administrateur complet nommé. N'associez pas « accès complet » dans Citrix Cloud à « administrateur complet » dans Citrix Virtual Apps and Desktops sur site. L'accès complet dans Citrix Cloud s'étend aux domaines, à la bibliothèque, aux notifications et aux emplacements de ressources de la plate-forme, ainsi qu'à tous les services auxquels vous êtes abonné.

Différences par rapport aux versions de Citrix DaaS antérieures

Avant la publication de la fonctionnalité d'accès personnalisé étendue (septembre 2018), il y avait deux rôles d'administrateur avec accès personnalisé : Administrateur complet et Administrateur du centre d'assistance. Lorsque l'administration déléguée est activée dans votre déploiement (ce qui correspond à un paramètre de plate-forme), ces rôles sont automatiquement mappés.

- Un administrateur qui était auparavant configuré en tant que **Virtual Apps and Desktops (ou XenApp and XenDesktop) : Administrateur complet** avec accès personnalisé est maintenant un **Administrateur Cloud** avec accès personnalisé.
- Un administrateur qui était auparavant configuré en tant que **Virtual Apps and Desktops (ou XenApp and XenDesktop) : Administrateur du centre d'assistance** avec accès personnalisé est maintenant un **Administrateur du centre d'assistance** avec accès personnalisé.

Informations supplémentaires

Pour plus d'informations sur les administrateurs, les rôles et les étendues utilisés dans la console **Surveiller** du service, reportez-vous à la section Administration déléguée et surveillance.

Page d'accueil de l'interface Configuration complète

November 2, 2023

Fournit une vue d'ensemble de votre déploiement et de vos charges de travail Citrix DaaS, ainsi que des informations qui vous aident à tirer le meilleur parti de votre abonnement. La page comprend les parties suivantes :

- Aperçu du service
- Alertes sur l'état du service
- Recommandations
- Nouveautés
- Fonctionnalités préliminaires
- Mise en route

Pour accéder à la page d'accueil, procédez comme suit :

1. Connectez-vous à Citrix Cloud.
2. Dans la vignette **DaaS**, cliquez sur **Gérer**.
3. Sélectionnez **Gérer > Configuration complète**. La page d'accueil s'affiche.

Aperçu du service

Fournit une vue d'ensemble de votre déploiement et de vos charges de travail Citrix DaaS :

- **Ressources**. Affiche le nombre de ressources déployées et leur nombre par catégorie.

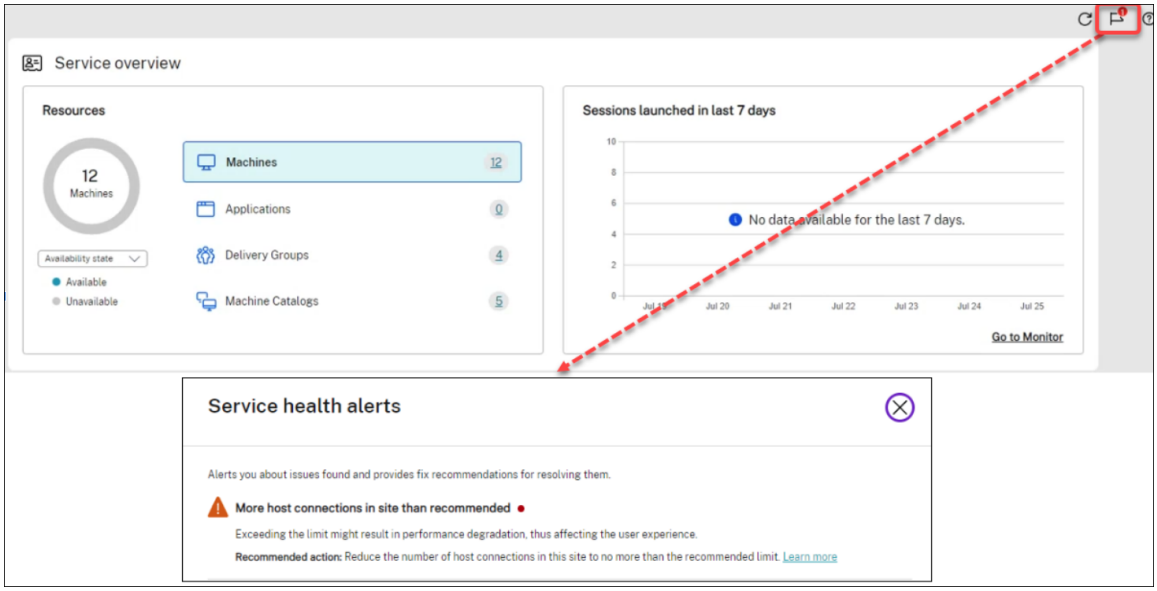
Ressource	Pour afficher les comptes par catégorie
Machines	Cliquez sur **Machines**, sélectionnez un état, puis survolez le graphique en anneau pour plus de détails. Options disponibles : **État de disponibilité** (Disponible, En cours d'utilisation, Désactivé ou Non disponible), **État d'enregistrement** (Enregistré ou Non enregistré) et **État de maintenance** (En maintenance ou Pas en mode en maintenance). Lorsque vous consultez le nombre de machines par état de disponibilité, vous pouvez cliquer sur un état pour afficher les détails de la machine correspondante.
Applications	Cliquez sur **Applications** et survolez le graphique en anneau pour plus de détails.
Groupes de mise à disposition	Cliquez sur **Groupes de mise à disposition** et survolez le graphique en anneau pour plus de détails.
Catalogues de machines	Cliquez sur **Catalogues de machines** et survolez le graphique en anneau pour plus de détails.

- **Sessions lancées au cours des 7 derniers jours**. Affiche le nombre de sessions de bureau et d'application lancées chaque jour au cours des sept derniers jours. Pour obtenir plus de détails, cliquez sur **Aller à Monitoring**.

Alertes sur l'état du service

Vous avertit des problèmes détectés et fournit des recommandations pour les résoudre. Les alertes apparaissent avec des symboles d'avertissement et d'erreur.

> **Remarque :**
>
> Les diagnostics sont mis à jour toutes les heures.
>
> Exemple d'alerte :



Recommandations

Recommande les fonctionnalités disponibles avec votre abonnement, telles que Workspace Environment Management et Autoscale. Pour communiquer avec nous, vous pouvez aimer ou ne pas aimer une recommandation et laisser vos commentaires.

> **Remarque :**
>
> Si vous n'aimez pas une recommandation, celle-ci disparaît. Si vous n'aimez pas toutes les recommandations ou le widget de recommandation, le widget de recommandation disparaît.

Nouveautés

Affiche une liste des dernières fonctionnalités Citrix DaaS les plus utiles pour votre entreprise. L'utilisation de ces fonctionnalités vous permet de tirer le maximum de votre abonnement. Pour une liste complète des nouvelles fonctionnalités, consultez la section Nouveautés.

Fonctionnalités préliminaires

Affiche les fonctionnalités actuellement en version préliminaire. En tant qu'administrateur Citrix Cloud disposant d'un accès complet, vous pouvez activer ou désactiver les fonctionnalités en version préliminaire sans contacter Citrix. Les modifications prennent jusqu'à 15 minutes pour prendre effet.

Il est recommandé d'utiliser les fonctionnalités préliminaires dans des environnements de non production. Les problèmes identifiés avec les fonctionnalités préliminaires ne sont pas pris en charge

par le support technique Citrix.

Mise en route

Affiche les étapes qui vous guident tout au long de la configuration initiale des applications et des bureaux.

Les étapes de configuration sont les suivantes :

1. Créer des emplacements de ressources

   Les emplacements de ressources font référence aux emplacements qui contiennent les applications et les bureaux que vous souhaitez mettre à la disposition de vos utilisateurs. Cette étape vous permet d'ajouter vos emplacements de ressources à DaaS et d'y installer des Cloud Connector. Les Cloud Connector servent de canaux qui authentifient et chiffrent toutes les communications entre Citrix Cloud et vos ressources.

2. Créer une connexion hôte

   Les hôtes sont des hyperviseurs ou des services cloud utilisés dans vos emplacements de ressources. Cette étape vous permet de spécifier les informations que DaaS utilise pour communiquer avec les machines virtuelles d'un hôte. Les informations détaillées incluent l'emplacement des ressources, le type d'hôte, les informations d'identification d'accès, la méthode de stockage à utiliser et les réseaux que les machines virtuelles de l'hôte peuvent utiliser.

3. Préparer une image principale

   Une image principale inclut le système d'exploitation, toutes les applications requises et le Virtual Delivery Agent (VDA). Les VDA établissent et maintiennent des connexions entre les machines virtuelles et les machines utilisateur.

4. Créer un catalogue de machines

   Un catalogue de machines est un ensemble de machines virtuelles avec OS mono-session ou multi-session identiques que vous attribuez aux utilisateurs. Cette étape vous permet de créer un catalogue de machines en spécifiant la technologie de provisioning, l'image principale et la taille de la machine virtuelle.

5. Attribuer des utilisateurs

   Un groupe de mise à disposition est une collection de machines sélectionnées à partir d'un ou de plusieurs catalogues de machines. Cette étape vous permet de créer des groupes de mise à disposition afin de spécifier les équipes, les services ou les types d'utilisateurs autorisés à utiliser des machines spécifiques.

6. Configurer Workspace

   Partagez l'URL de l'espace de travail depuis **Configuration de l'espace de travail > Accès** avec vos utilisateurs.

Licences

April 27, 2022

Cet article couvre les tâches et les ressources concernant les licences Microsoft et Citrix.

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

Ces informations s'appliquent lorsque vous mettez à disposition des charges de travail Windows Server.

Ce service 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 2019. 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 Microsoft :

1. Installez un serveur de licences Services Bureau à distance (RDS) sur une VM disponible. La VM doit toujours être disponible. Les charges de travail du service 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 modèle 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.

utilisation des licences Citrix

Pour plus d'informations sur l'utilisation des licences Citrix, consultez :

- Surveiller les licences et l'utilisation active des services cloud
- Surveiller les licences et l'utilisation active de Citrix DaaS

Licences multitypes

August 18, 2023

La fonction Licences multitypes prend en charge la consommation de différents droits de licence dans un seul déploiement de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Cet article s'applique à vous si vous disposez de plusieurs droits de licence Citrix. Un droit Citrix est une combinaison des éléments suivants :

- Produit qui, dans le contexte actuel de DaaS est toujours Citrix DaaS
- Édition du service (par exemple : Advanced, Advanced Plus, Premium ou Premium Plus)
- Modèle de licence (par exemple : utilisateur/appareil ou simultanée)

Règles relatives à la combinaison de droits

Les règles pour combiner les éditions de service sont les suivantes :

- Seule la combinaison de DaaS Advanced et Advanced Plus est autorisée
- Seule la combinaison de DaaS Premium et Premium Plus est autorisée
- DaaS Standard ne peut être combiné à aucune autre édition

Vous pouvez combiner les modèles de licences lorsque les règles d'édition de service spécifiques ci-dessus sont respectées.

Droit au niveau du site et du groupe de mise à disposition

Vous pouvez configurer et utiliser les droits de licence aux deux niveaux suivants :

- Site (votre déploiement du produit Citrix DaaS)
- Groupe de mise à disposition

Si vous n'avez pas encore configuré de droits de site ou de groupe de mise à disposition, prenez en compte le comportement par défaut suivant :

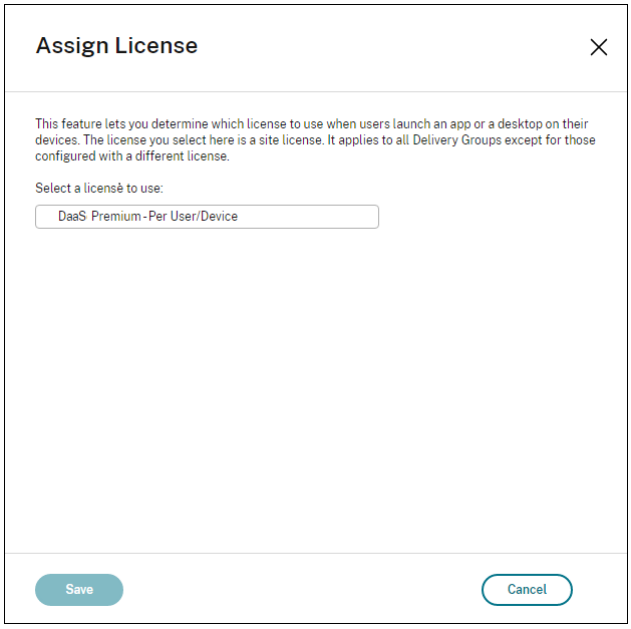
- Si vous disposez de plusieurs droits, le plus performant des droits disponibles est sélectionné comme droit applicable à l'ensemble du site, à condition qu'ils aient été commandés en même temps. Sinon, le premier droit est appliqué par défaut à l'échelle du site, sauf modification explicite ultérieure.
- Le droit de site est utilisé sauf si un droit de groupe de mise à disposition est configuré.

> **Remarque :**
>
> La configuration des droits de site ou de groupe de mise à disposition affecte la façon dont la consommation de licences est comptabilisée dans les écrans d'utilisation des licences dans Citrix Cloud.

Afficher et mettre à jour les droits au niveau du site

Pour spécifier le droit de licence à utiliser sur l'ensemble du site, accédez à **Configuration complète > Paramètres > Attribuer une licence** et cliquez sur **Modifier**. Le panneau **Attribuer une licence** s'affiche. Pour plus d'informations sur la façon d'accéder à la page **Configuration complète**, consultez la documentation Citrix DaaS.

Dans le panneau **Attribuer une licence**, sélectionnez la licence que vous souhaitez que le site utilise. La licence sélectionnée s'applique à tous les groupes de mise à disposition du site, à l'exception de ceux configurés avec une licence différente.



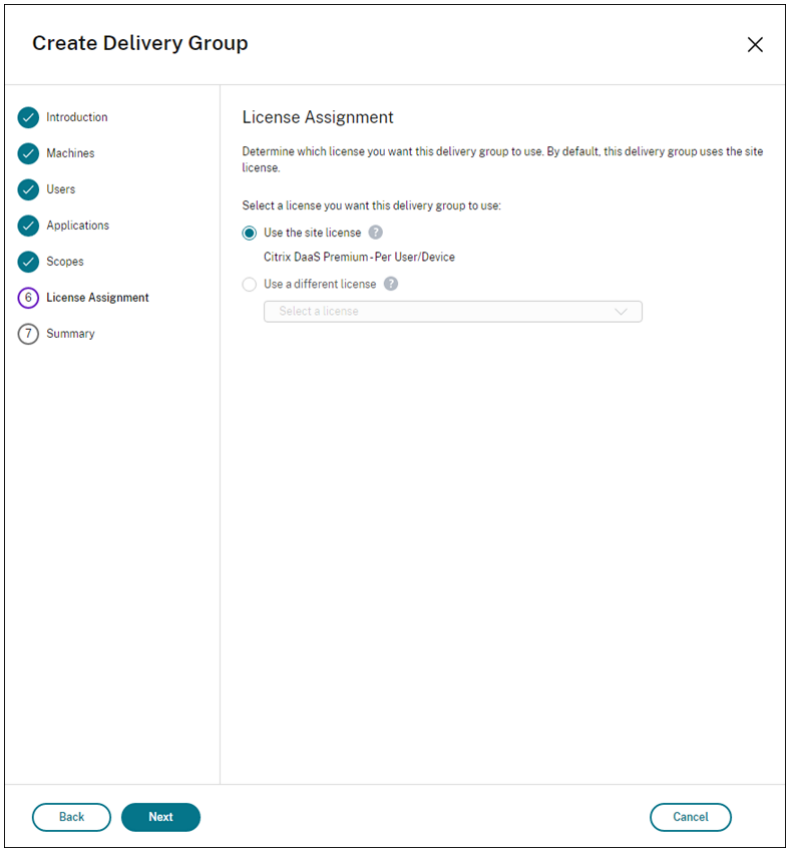
Les licences que vous pouvez sélectionner sont les suivantes :

- Citrix DaaS Premium –Licences par utilisateur/appareil
- Citrix DaaS Premium –Licences simultanées
- Citrix DaaS Premium pour Google Cloud –Licences par utilisateur/appareil
- Citrix DaaS Premium pour Google Cloud —Licences simultanées
- Citrix DaaS Advanced –Licences par utilisateur/appareil
- Citrix DaaS Advanced –Licences simultanées
- Citrix DaaS Advanced Plus –Licences par utilisateur/appareil
- Citrix DaaS Advanced Plus –Licences simultanées
- Citrix DaaS Standard pour Azure –Licences par utilisateur/appareil
- Citrix DaaS Standard pour Azure –Licences simultanées
- Citrix DaaS Standard pour Google Cloud –Licences par utilisateur/appareil
- Citrix DaaS Standard pour Google Cloud —Licences simultanées

Si vous avez une licence qui a expiré, contactez votre représentant commercial Citrix pour la renouveler ou pour acheter de nouvelles licences.

Afficher et mettre à jour un droit au niveau du groupe de mise à disposition

Vous pouvez spécifier quelle licence vous souhaitez qu'un groupe de mise à disposition utilise lors de la création ou de la modification d'un groupe de mise à disposition. Sur la page **Attribution de licences**, sélectionnez une option.



Options :

- **Utiliser la licence de site**. Une licence de site s'applique à tous les groupes de mise à disposition, à l'exception de ceux configurés avec une licence différente. La licence qui apparaît sous cette option est la licence de site en cours d'utilisation. Pour configurer la licence du site, accédez à **Gérer > Configuration complète**, sélectionnez le nœud **Paramètres**, puis modifiez **Attribuer une licence**.
- **Utiliser une licence différente**. Cette option vous permet de configurer ce groupe de mise à disposition pour utiliser une licence différente de la licence de site. N'oubliez pas qu'un droit de licence est une combinaison de code produit, d'édition et de modèle de licence. Le groupe de mise à disposition doit utiliser la même édition de licence (Standard, Premium ou Advanced) que le site. Si elle est configurée, le groupe de mise à disposition consomme uniquement la licence sélectionnée. Même si la licence sélectionnée est entièrement consommée ou est devenue invalide, le groupe de mise à disposition ne revient pas à la licence de site.

Par défaut, le groupe de mise à disposition utilise la licence de site.

Lorsqu'une licence de groupe de mise à disposition expire et n'est plus valide, utilisez une autre licence.

> **Remarque :**
>
> Si vous configurez ultérieurement un groupe de mise à disposition pour utiliser une licence différente, les utilisateurs connectés qui consomment la licence actuelle risquent de perdre temporairement l'accès à leurs bureaux et applications.

Exemple de combinaison de droits

Par exemple, considérez que le client A a initialement acheté l'édition Advanced et a ensuite acheté l'édition Advanced Plus. Dans ce cas, le client A dispose toujours d'une licence pour l'ensemble du site uniquement pour l'édition Advanced. Citrix ne modifie pas le paramètre initialement défini au niveau du site par le client A. Il est de la responsabilité du client A de modifier l'édition de licence vers Advanced Plus au niveau du site.

De même, le client A peut également mettre à jour l'édition de la licence vers Advanced Plus dans le groupe de mise à disposition. Si ce paramètre n'est pas configuré, le groupe de mise à disposition hérite de l'édition de licence définie au niveau du site.

L'administrateur du client A peut mettre à jour l'édition de la licence de la manière suivante :

- Mettre à jour l'édition de la licence au niveau du site : accéder à **Gérer > Configuration complète**, sélectionner le nœud **Paramètres**, puis modifier **Attribuer une licence**
- Mettre à jour l'édition de la licence au niveau du groupe de mise à disposition : accéder à **Gérer > Configuration complète**, puis sélectionner le nœud **Groupes de mise à disposition** Modifier le groupe de mise à disposition cible pour apporter des modifications

Mettre à jour le groupe de mise disposition à l'aide de la commande PowerShell

La commande PowerShell pour mettre à jour le groupe de mise à disposition est la suivante :

```
1 Set-BrokerDesktopGroup -Name <DGName> -ProductCode <Name of the product
      code> -LicenseModel <The type of license model>
2 <!--NeedCopy-->
```

Mettez à jour la commande précédente en fonction de vos informations.

Par exemple, comme ce qui suit :

- `Set-BrokerDesktopGroup -Name DG1 -ProductCode VADS -LicenseModel CONCURRENT`
- `Set-BrokerDesktopGroup -Name DG1 -ProductCode $null -LicenseModel $null` (Définissez la configuration au niveau du groupe de mise à disposition sur celle du site)
- `Set-BrokerSite -CloudSiteLicense VADS:ADVANCED:USERDEVICE`

Notez que le modèle de licence et le code produit ne sont pas définis au niveau du groupe de mise à disposition. Dans ce scénario, ces deux propriétés définies au niveau du site sont utilisées pour le groupe de mise à disposition.

Pour plus d'informations sur le SDK Remote PowerShell Citrix DaaS, consultez la documentation sur les SDK et les API.

Informations supplémentaires

- Licences
- Créer des groupes de mise à disposition
- Gérer des groupes de mise à disposition

Équilibrer la charge des machines

December 4, 2023

> **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 12, 2024

> **Conseil :**
>
> Dans **Configuration complète > Accueil**, la fonction d'alertes d'état du service vous envoie des alertes proactives pour vous assurer que votre cache d'hôte local et vos zones sont correctement configurés. Ainsi, en cas de panne, le cache d'hôte local fonctionne et vos utilisateurs ne sont pas affectés. Les alertes se répartissent en deux niveaux : les alertes à l'échelle du site affichées dans la page d'accueil (icône représentant un drapeau) et les alertes relatives aux zones affichées dans l'onglet Dépannage de chaque zone. Pour plus d'informations, consultez la section Zones.

Le mode de cache d'hôte local (LHC) permet de poursuivre les opérations de négociation de connexion dans un déploiement Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) lorsqu'un composant Cloud Connector ne peut pas communiquer avec Citrix Cloud. Le cache d'hôte local est activé lorsque la connexion réseau est perdue pendant 60 secondes.

Grâce au cache d'hôte local, les utilisateurs qui sont connectés lorsqu'une panne se produit peuvent continuer à travailler sans interruption. Les délais des nouvelles connexions et des reconnexions sont réduits.

> **Important :**
>
> Si vous utilisez un déploiement StoreFront sur site, vous devez ajouter tous les Cloud Connector avec lesquels sont (ou peuvent être) enregistrés des VDA à StoreFront en tant que Delivery Controller. Un Cloud Connector qui n'est pas ajouté à StoreFront ne peut pas passer en mode panne, ce qui peut entraîner des échecs de lancement de l'utilisateur.
>
> Pour les déploiements sans instance StoreFront locale, utilisez la fonctionnalité de continuité de la plate-forme Citrix Workspace pour permettre aux utilisateurs de se connecter aux ressources pendant les pannes. Pour plus d'informations, consultez Continuité du service.

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 de l'application Citrix Workspace 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 :

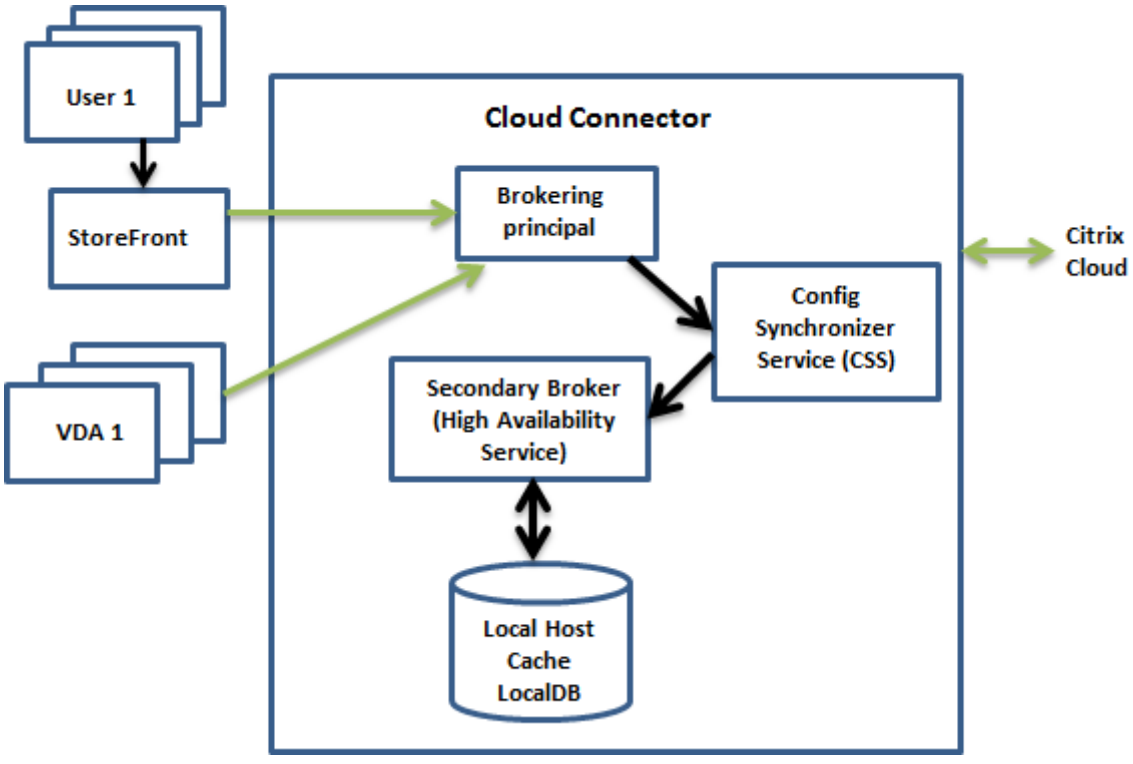
- Résultats de toute analyse de point de terminaison de machine client réalisée par l'application Citrix Workspace.
- Identités des machines d'infrastructure (telles que les serveurs Citrix Gateway et StoreFront) impliquées dans le site.
- Dates, heures et types d'activités récentes des utilisateurs.

Fonctionnement

Découvrez comment le cache d'hôte local interagit avec Citrix Cloud.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

En mode de fonctionnement normal



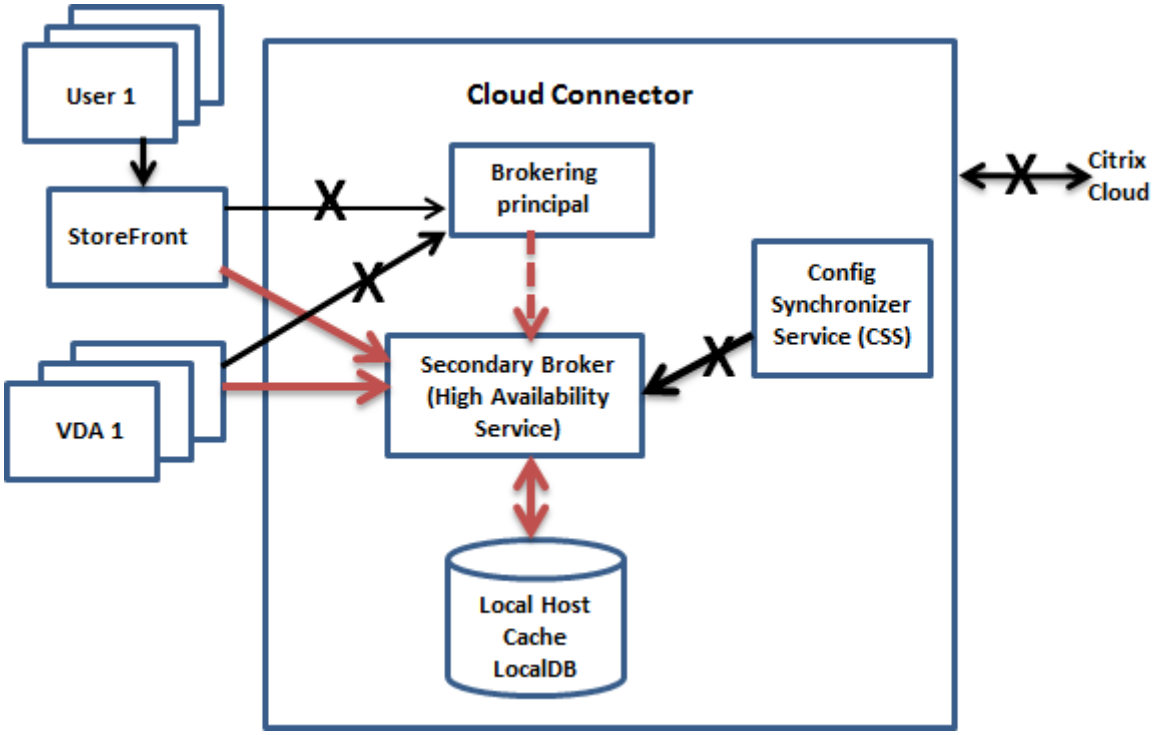
- Le broker principal (Citrix Remote Broker Provider Service) sur un Cloud Connector accepte des requêtes de connexion provenant de StoreFront. Le broker principal communique avec Citrix Cloud pour connecter les utilisateurs aux VDA qui sont enregistrés auprès du Cloud Connector.

- Citrix Config Synchronizer Service (CSS) interroge le broker dans Citrix Cloud environ toutes les 5 minutes pour savoir si des modifications ont été apportées à la configuration. 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 Cloud Connector. (Le broker secondaire est également connu sous le nom de service de haute disponibilité, ou HA Broker, comme indiqué dans la figure précédente.)

  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 Cloud Connector. 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 dans Citrix Cloud. 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 Cloud Connector. La base de données du cache d'hôte local ne peut pas être partagée sur des Cloud Connector. 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, les données de configuration ne sont pas copiées.

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 à Citrix Cloud. 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 Citrix Cloud.

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 consigne les synchronisations et les pannes.

Aucun délai n'est imposé pour le fonctionnement en mode panne.

Vous pouvez également déclencher intentionnellement une panne. Voir Forcer une panne pour savoir quand cela peut être nécessaire et comment procéder.

Emplacements de ressources avec plusieurs Cloud Connector

Parmi ses différentes tâches, le service CSS fournit régulièrement au broker secondaire des informations sur tous les Cloud Connector dans l'emplacement de ressources. Ces informations permettent à chaque broker secondaire de connaître tous les brokers secondaires homologues qui s'exécutent sur d'autres Cloud Connector dans l'emplacement des ressources.

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 se ré-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.

> **Important :**
>
> Les connecteurs d'un emplacement des ressources doivent être en mesure de communiquer entre eux à l'adresse `http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection`. S'ils ne peuvent pas communiquer à cette adresse, plusieurs brokers peuvent être sélectionnés et des échecs de lancement intermittents peuvent survenir lors d'un événement de cache d'hôte local.

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 Cloud Connector est redémarré :

- Si ce Cloud Connector n'est pas le broker sélectionné, le redémarrage n'a aucun impact.
- Si ce Cloud Connector est le broker sélectionné, un autre Cloud Connector est sélectionné, et par conséquent les VDA s'enregistrent. Une fois que le Cloud Connector redémarré est sous tension, il reprend automatiquement la négociation des connexions, et les VDA s'enregistrent à nouveau. Dans ce scénario, les performances peuvent être affectées lors des enregistrements.

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, si la défaillance est due à la perte de la connectivité à Citrix Cloud à partir de leur emplacement de ressources, Citrix recom-

mande de restaurer la connectivité à partir de l'emplacement de ressources le plus rapidement possible.

Durant une panne :

- Lors d'un événement de mise en cache de l'hôte local, l'interface Configuration complète peut être temporairement inaccessible. Si l'interface Configuration complète est accessible, les VDA situés dans des emplacements de ressources fonctionnant en mode haute disponibilité s'affichent comme étant non enregistrés dans l'interface Configuration complète. Ces VDA restent accessibles via le cache d'hôte local.
- Vous avez un accès limité au SDK Remote 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`
    * Définissez l'authentification du SDK sur `OnPrem` de sorte que le proxy du SDK n'essaie pas de rediriger les appels de l'applet de commande : `$XDSDKAuth="OnPrem"`
    * Utiliser le port 89 : `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ContollerDNSName, DesktopGroupName, RegistrationState`
  - Après avoir exécuté ces commandes, vous pouvez accéder à :
    * Toutes les applets de commande `Get-Broker*`.
- Les données de surveillance ne sont pas envoyées à Citrix Cloud pendant une panne. Par conséquent, les fonctions de **surveillance** n'affichent pas l'activité lors d'une défaillance.
- 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.

- Lors d'un événement de mise en cache de l'hôte local, chaque zone agit indépendamment. Les lancements entre zones (depuis un broker dans une zone vers un VDA situé dans une autre zone) ne sont pas pris en charge durant une panne. Utilisez la fonctionnalité de vérification de l'intégrité avancée de StoreFront pour acheminer les requêtes de lancement vers la zone appropriée lors d'un événement LHC.
- 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. Ce scénario 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.
- Lesrestrictions de balises dans lesquelles des balises sont utilisées pour désigner des emplacements de ressources 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.

Exigences de StoreFront

Si vous utilisez un déploiement StoreFront sur site, vous devez ajouter tous les Cloud Connector avec lesquels sont (ou peuvent être) enregistrés des VDA à StoreFront en tant que Delivery Controller. Un Cloud Connector qui n'est pas ajouté à StoreFront ne peut pas passer en mode panne, ce qui peut entraîner des échecs de lancement de l'utilisateur.

Disponibilité des ressources

Pour garantir la disponibilité des ressources (applications et bureaux) lors d'une panne, vous pouvez procéder de deux manières :

- Publiez les ressources dans chaque emplacement de ressources de votre déploiement.
- Si vous utilisez StoreFront 1912 CU4 ou version ultérieure, publiez les ressources sur au moins un emplacement de ressources et activez la vérification de l'état avancée sur tous les serveurs StoreFront. Pour les versions antérieures à StoreFront 2308, la vérification de l'état avancée est désactivée par défaut et doit être activée par un administrateur. Pour StoreFront version 2308 et versions ultérieures, cette fonctionnalité est activée par défaut. Pour plus d'informations et des instructions sur l'activation de la vérification de l'état avancée, consultez la section Vérification de l'état avancée.

Prise en charge des applications et des bureaux

Le mode LHC prend en charge les types de VDA et les modèles de mise à disposition suivants :

Type de VDA	Modèle de mise à disposition	Disponibilité du VDA pendant les événements LHC
OS multi-session	Applications et bureaux	Toujours disponible.
Système d'exploitation monosession statique (attribué)	Bureaux	Toujours disponible.
Système d'exploitation mono-session à alimentation gérée aléatoire (regroupé)	Bureaux	Non disponible par défaut. Toutes les tentatives de lancement de session sur des VDA à alimentation gérée appartenant à des groupes de

> **Remarque :**
>
> L'activation de l'accès à des VDA de bureau à alimentation gérée dans des groupes de mise à disposition mis en pool n'affecte pas le fonctionnement de la propriété `ShutdownDesktopsAfterUse` configurée pendant les opérations normales. Lorsque l'accès à ces bureaux pendant un événement LHC est activé, 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. Un redémarrage du VDA peut se produire lorsqu'un utilisateur ferme sa session pendant des opérations autres que le LHC ou lorsque les administrateurs redémarrent le VDA.

Important : l'activation de l'accès à des machines mono-session regroupées à alimentation gérée peut entraîner la présence de machines disponibles pour de nouvelles connexions pendant les événements LHC, selon le groupe de mise à disposition. Ces machines peuvent contenir des modifications issues des sessions utilisateur précédentes dans les sessions suivantes.

Activer le mode LHC pour les VDA à OS mono-session et alimentation gérée mis en pool à l'aide de l'interface Configuration complète

À l'aide de l'interface Configuration complète, vous pouvez rendre ces machines disponibles pour de nouvelles connexions pendant les événements LHC, selon le groupe de mise à disposition.

- Pour activer cette fonctionnalité lors de la création de groupes de mise à disposition, consultez Créer des groupes de mise à disposition.
- Pour activer cette fonctionnalité pour un groupe de mise à disposition existant, consultez Gérer les groupes de mise à disposition

> **Remarque :**
>
> Ce paramètre n'est disponible dans l'interface Configuration complète que pour les groupes de mise à disposition de bureaux mis en pool qui fournissent des VDA à alimentation gérée.

Activer le mode LHC pour les VDA à OS mono-session et alimentation gérée mis en pool à l'aide de PowerShell

Pour activer le mode LHC pour des VDA appartenant à un groupe de mise à disposition spécifique, procédez comme suit :

1. Activez cette fonctionnalité au niveau du site en exécutant cette commande :

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. Activez le mode LHC pour un groupe de mise à disposition en exécutant cette commande avec le nom du groupe de mise à disposition spécifié comme suit :

   ```
   Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
    $true
   ```

Pour modifier la disponibilité par défaut du mode LHC pour les groupes de mise à disposition mis en pool récemment créés avec des VDA à alimentation gérée, exécutez la commande suivante :

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

Vérifier que le cache d'hôte local fonctionne

Découvrez comment vérifier que le cache d'hôte local est correctement configuré.

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Pour vérifier que le cache d'hôte local est configuré et fonctionne correctement :

- Si vous utilisez StoreFront, vérifiez que le déploiement local de StoreFront pointe vers tous les Cloud Connector de cet emplacement de ressources.
- Assurez-vous que les importations de synchronisation se déroulent correctement. Vérifiez les journaux d'événements.
- Assurez-vous que la base de données Cache hôte local a été créée sur chaque Cloud Connector. Cela confirme que le High Availability Service peut prendre le relais, si nécessaire.
  - Sur le serveur Cloud Connector, accédez à `c:\Windows\ServiceProfiles\NetworkService`.
  - Vérifiez que `HaDatabaseName.mdf` et `HaDatabaseName_log.ldf` sont créés.

- Forcez une interruption sur tous les Cloud Connector dans l'emplacement de ressources. Après avoir vérifié que le cache d'hôte local fonctionne, n'oubliez pas de remettre tous les Cloud Connector 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*.

Service de synchronisation de la configuration

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 se produit chaque fois qu'une configuration mise à jour est reçue depuis Citrix Cloud. Il 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.

Service de haute disponibilité

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.

Remote Broker Provider

Ce service fait office de proxy entre Citrix Cloud, vos VDA et vos machines Cloud Connector.

- 3001 : vérifie si les machines Cloud Connector doivent passer en mode haute disponibilité. Cet événement se produit après un seul échec de machine Cloud Connector à la vérification de l'intégrité. Si une machine Cloud Connector échoue à la prochaine vérification de l'intégrité au bout de 60 secondes, elle passe en mode haute disponibilité.
- 3002 : indique que la machine Cloud Connector ne peut pas passer en mode haute disponibilité. La raison pour laquelle le passage en mode haute disponibilité échoue est fournie dans les informations sur l'événement.
- 3003 : indique que la machine Cloud Connector passe par différents états du mode haute disponibilité. Ce diagramme décrit les états d'entrée et de sortie du mode haute disponibilité. L'événement fournit les informations suivantes :
  - L'état à partir duquel la machine Cloud Connector est en cours de transition.
  - L'état vers lequel la machine Cloud Connector est en cours de transition.
  - La durée de l'état précédent.

> **Remarque :**
>
> Des événements 3001 peuvent se produire fréquemment sur vos machines Cloud Connector. Ces événements peuvent être dus à des interruptions du réseau et ne constituent pas une source de

> préoccupation.

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.

Bien qu'un Cloud Connector puisse être mis à jour pendant une interruption forcée, des problèmes imprévus peuvent survenir. Nous vous recommandons de définir un calendrier pour les mises à jour de Cloud Connector afin d'éviter les intervalles de mode d'interruption forcée.

Pour forcer une interruption, modifiez le registre de chaque serveur Cloud Connector. Dans `HKLM\Software\Citrix\DesktopServer\LHC`, créez et définissez `OutageModeForced` comme `REG_DWORD` sur `1`. Ce réglage demande au broker Cache d'hôte local d'entrer en mode d'interruption, quel que soit l'état de la connexion à Citrix Cloud. 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\HighAavailabilityService`.

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, peuvent 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
```

Commandes PowerShell du cache d'hôte local

Vous pouvez gérer le cache d'hôte local sur vos Cloud Connector à l'aide des commandes PowerShell.

Le module PowerShell se trouve à l'emplacement suivant sur les Cloud Connector :

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **Important :**
>
> Exécutez ce module uniquement sur les Cloud Connector.

Importer le module PowerShell Pour importer le module, exécutez la commande suivante sur votre Cloud Connector :

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

Commandes PowerShell pour gérer le cache d'hôte local (LHC) Les applets de commande suivantes vous aident à activer et à gérer le mode LHC sur les Cloud Connectors.

Applets de commande	Fonction
`Enable-LhcForcedOutageMode`	Permet de placer le broker en mode LHC. Les fichiers de base de données du cache d'hôte local 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 Cloud Connector sur lequel il a été exécuté. Pour que le LHC soit actif, cette applet de commande doit être exécutée sur tous les Cloud Connector de l'emplacement des ressources.
`Disable-LhcForcedOutageMode`	Permet de faire sortir le broker du mode LHC. Cette applet de commande désactive uniquement le mode LHC sur le Cloud Connector sur lequel elle était exécutée. `Disable-LhcForcedOutageMode` doit être exécuté sur tous les Cloud Connector de l'emplacement des ressources.
`Set-LhcConfigSyncIntervalOverride`	Permet de définir l'intervalle auquel Citrix Config Synchronizer Service (CSS) vérifie les modifications de configuration sur le site Citrix DaaS. L'intervalle de temps peut aller de 60 secondes (une minute) à 3 600 secondes (une heure). Ce paramètre s'applique uniquement au Cloud Connector sur lequel il a été exécuté. Pour des raisons de cohérence entre les Cloud Connector, pensez à exécuter cette applet de commande sur chaque Cloud Connector. Pa exemple : `Set-LhcConfigSyncIntervalOverride -Seconds 1200`

Applets de commande	Fonction
`Clear-LhcConfigSyncIntervalOverride`	Permet de définir l'intervalle auquel Citrix Config Synchronizer Service (CSS) vérifie les modifications de configuration sur le site Citrix DaaS, à la valeur par défaut de 300 secondes (cinq minutes). Ce paramètre s'applique uniquement au Cloud Connector sur lequel il a été exécuté. Pour des raisons de cohérence entre les Cloud Connector, pensez à exécuter cette applet de commande sur chaque Cloud Connector.
`Enable-LhcHighAvailabilitySDK`	Permet d'accéder à toutes les applets de commande `Get-Broker*` du Cloud Connector sur lequel elles étaient exécutées
`Disable-LhcHighAvailabilitySDK`	Désactive l'accès aux commandes Broker PowerShell dans le Cloud Connector sur lequel elles étaient exécutées.

> **Remarque :**
>
> - Utilisez le port 89 lorsque vous exécutez les applets de commande `Get-Broker*` sur le Cloud Connector. Par exemple :
>
>   ```
>   - Get-BrokerMachine -AdminAddress localhost:89
>   ```
>
> - Lorsqu'il n'est pas en mode LHC, le broker LHC du Cloud Connector ne contient que les informations de configuration.
> - En mode LHC, le broker LHC du Cloud Connector sélectionné contient les informations suivantes :
>   - États des ressources
>   - Détails de la session
>   - Enregistrements de VDA
>   - Informations de configuration

Informations supplémentaires

Voir Considérations sur le dimensionnement et la scalabilité du cache d'hôte local pour plus d'informations sur :

- Méthodes d'essai et résultats

- Considérations sur la taille de la RAM
- Considérations sur la configuration des sockets et des cœurs d'UC
- Considérations sur le stockage

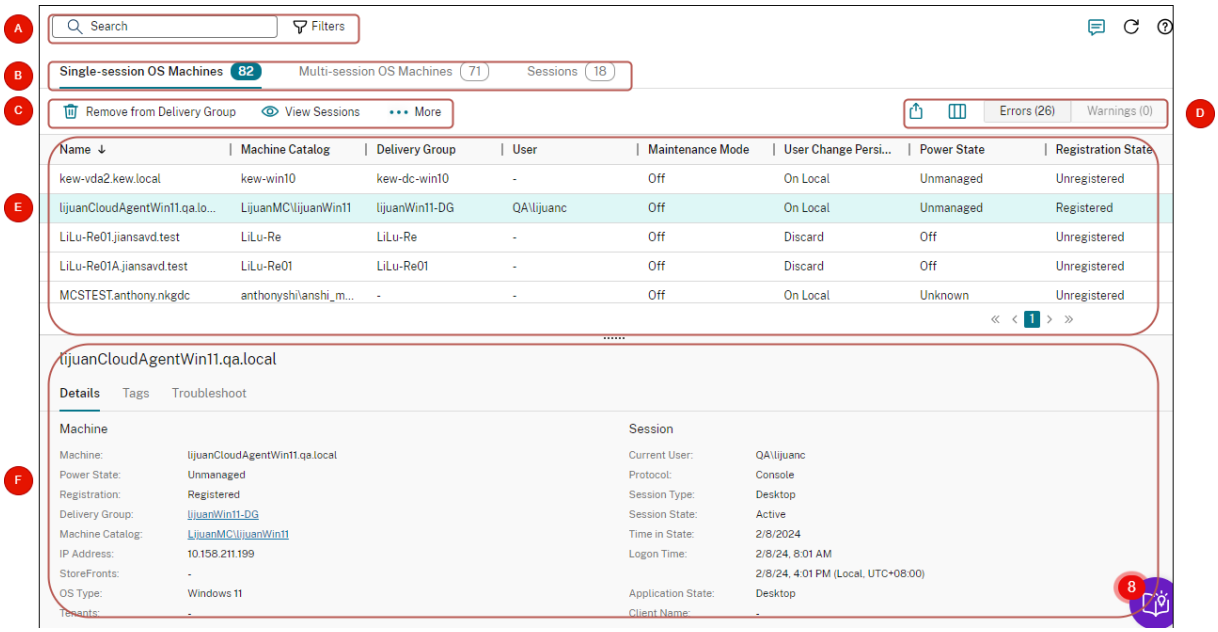
Surveiller et gérer les machines et les sessions à l'aide de la fonction de recherche

June 12, 2024

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.
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 -Icône **Exporter** : permet d'exporter la liste des instances affichées dans la vue principale vers un fichier CSV. -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. 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**. Étiquette **Avertissements** : activez cette étiquette pour afficher uniquement les machines non enregistrées

Légende	Zone	Description
F	Volet de détails	Affiche les informations suivantes Détails de l'instance sélectionnée (machine ou session) Balises appliquées à la machine sélectionnée 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

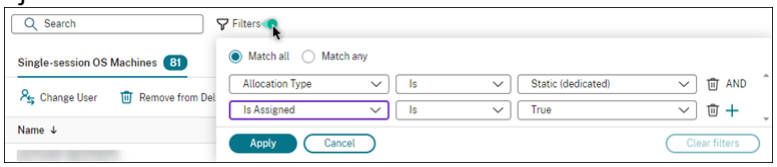
Utilisez la fonction de recherche pour localiser des machines et des sessions spécifiques :

- 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

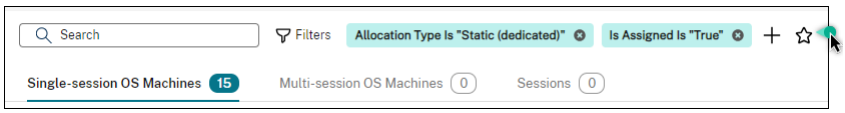
Par exemple, pour localiser toutes les machines avec OS mono-session qui sont *statiques* et *attribuées à des utilisateurs*, procédez comme suit :

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.

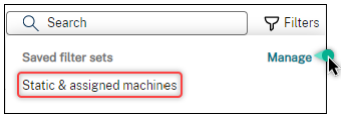


Enregistrer le jeu de filtres actuel pour une recherche rapide

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.

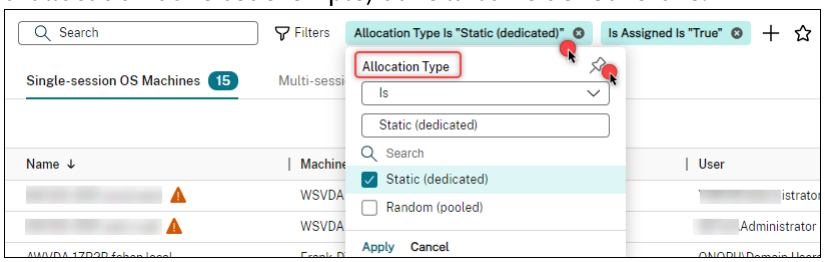


> **Remarque :**
>
> Les jeux de filtres sont enregistrés pour chaque compte utilisateur. Pour gérer les ensembles de filtres enregistrés, sélectionnez **Gérer**.

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 12, 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
Exécuter vérification de l'état	Disponible uniquement pour les VDA Windows enregistrés, version 2019 ou versions ultérieures. Exécutez une vérification de l'intégrité sur une machine. Pour plus d'informations sur le contenu des contrôles, consultez la section À propos des vérifications de l'intégrité.	Mono-session et multi-session
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
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. 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

Action	Description	S'applique à
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
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, DaaS stocke le contenu de la mémoire de la machine dans un fichier, puis arrête celle-ci.	Machines avec OS mono-session
Reprendre	Reprenez une machine suspendue. Lorsque vous reprenez une machine suspendue, DaaS la démarre et la restaure 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

Colonne	Description	S'applique à
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
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

Colonne	Description	S'applique à
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
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. `True` indique que la machine est physique, ce qui signifie que son alimentation n'est pas gérée par DaaS. `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 de redémarrage et non disponible	Mono-session et multi-session

Colonne	Description	S'applique à
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. États possibles : Désactivé, Non enregistré, Disponible, Déconnecté, En cours d'utilisation et Préparation.	Mono-session et multi-session
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. 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

Colonne	Description	S'applique à
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. **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
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

Colonne	Description	S'applique à
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

Colonne	Description	S'applique à
Persistance des modifications de l'utilisateur	Indique le mode de gestion des modifications apportées par les utilisateurs, notamment si les modifications sont persistantes	Mono-session et multi-session
Action d'alimentation en attente	Indique s'il y a des actions d'alimentation en attente pour la machine.	Mono-session et multi-session
État d'alimentation	État d'alimentation de la machine. Valeurs possibles : Non géré, Indisponible, Suspendu, Désactivation en cours, Suspension et Reprise.	Mono-session et multi-session
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. **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 12, 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 devient déconnectée, 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.

Colonne	Description
Nom d'utilisateur de broker	Nom de l'utilisateur du broker.
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. `True` indique que la machine est physique, ce qui signifie que son alimentation n'est pas gérée par DaaS. `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 Local : persistant. Les modifications apportées par les utilisateurs sont enregistrées localement. 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. **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 Manuel : non provisionné à l'aide de PVS ou MCS. PVS : provisionné par PVS (machines physiques, lames et machines virtuelles). 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

April 17, 2023

> **Remarque :**
>
> - 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.

Cette fonctionnalité vous permet d'autoriser uniquement les machines StoreFront et Citrix Gateway approuvées à communiquer avec des Citrix 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. Affichez les paramètres des clés de sécurité dans l'interface Configuration complète. (Utilisez le SDK Remote PowerShell)
2. Configurez les paramètres de votre déploiement. (Utilisez l'interface Configuration complète ou Remote PowerShell SDK).
3. Configurez les paramètres dans StoreFront. (Utilisez PowerShell).
4. Configurez les paramètres dans Citrix ADC.

Afficher les paramètres des clés de sécurité dans l'interface Configuration complète

Par défaut, les paramètres des clés de sécurité sont masqués dans l'interface Configuration complète. Pour les afficher dans cette interface, utilisez le SDK Remote PowerShell. Pour plus d'informations sur le SDK Remote PowerShell, reportez-vous à la section SDK et API.

Les étapes détaillées sont les suivantes :

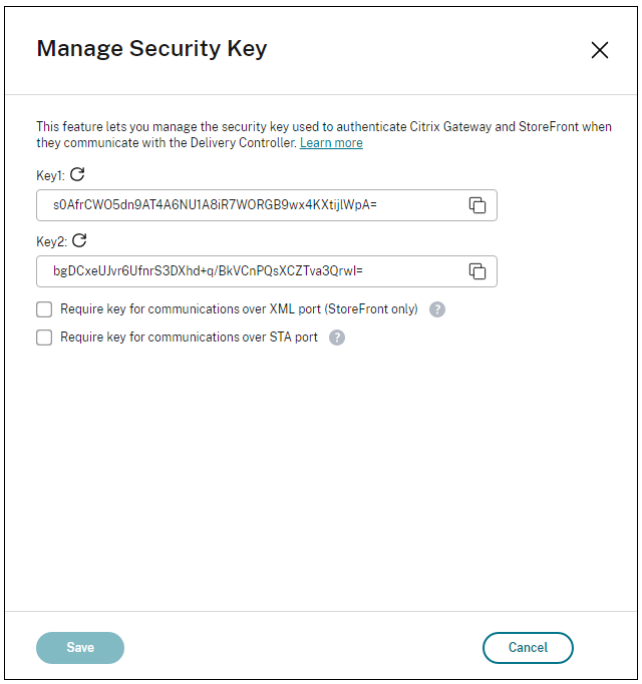
1. Exécutez le SDK Remote PowerShell.
2. Dans une fenêtre de commandes, exécutez les commandes suivantes :
    - `Add-PSSnapIn Citrix*`. Cette commande ajoute les composants logiciels enfichables Citrix.
    - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

Configurer les paramètres de votre déploiement

Vous pouvez configurer les paramètres de votre déploiement à l'aide de Configuration complète ou de PowerShell.

Utiliser l'interface Configuration complète

Après avoir activé la fonctionnalité, accédez à **Configuration complète > Paramètres > Gérer la clé de sécurité**, puis cliquez sur **Modifier**. Le panneau **Gérer la clé de sécurité** s'affiche. Cliquez sur **Enregistrer** pour appliquer vos modifications et quitter le panneau.



> **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.

Cliquez sur l'icône d'actualisation pour générer de nouvelles clés.

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.

Après avoir appliqué vos modifications, cliquez sur **Fermer** pour quitter le panneau **Gérer la clé de sécurité**.

Utiliser le SDK Remote PowerShell

Voici les étapes PowerShell équivalentes aux opérations effectuées dans l'interface Configuration complète.

1. Exécutez le SDK 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 défini les paramètres de votre déploiement, 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 des communications via le port XML, utilisez les commandes `Get-STFStoreServie` et `Set-STFStoreService`. Par exemple :
  - `PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80 -TransportType HTTP -Servers <domain name1, domain name2> -XMLValidationEnabled $true -XMLValidationSecret <the key you generated in Studio>`

- Pour configurer la clé des communications via le port STA, utilisez la commande `New-STFSecureTicketAuthority`. Par exemple :

  - `PS C:\> $sta = New-STFSecureTicketAuthority –StaUrl <STA URL > -StaValidationEnabled $true -StavalidationSecret <the key you generated in Studio>`

Consultez l'aide de la commande PowerShell pour plus d'informations et la syntaxe.

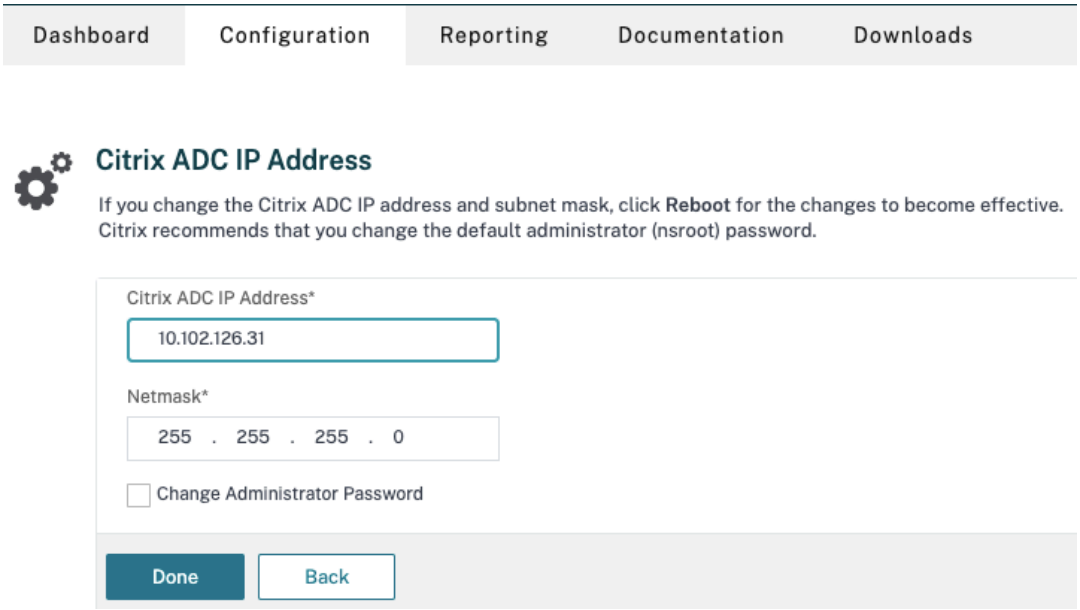
Configurer les paramètres dans Citrix ADC

> **Remarque :**
>
> La configuration de cette fonctionnalité dans Citrix ADC n'est pas requise sauf si vous utilisez Citrix ADC comme passerelle. If you use Citrix ADC, follow the steps below.

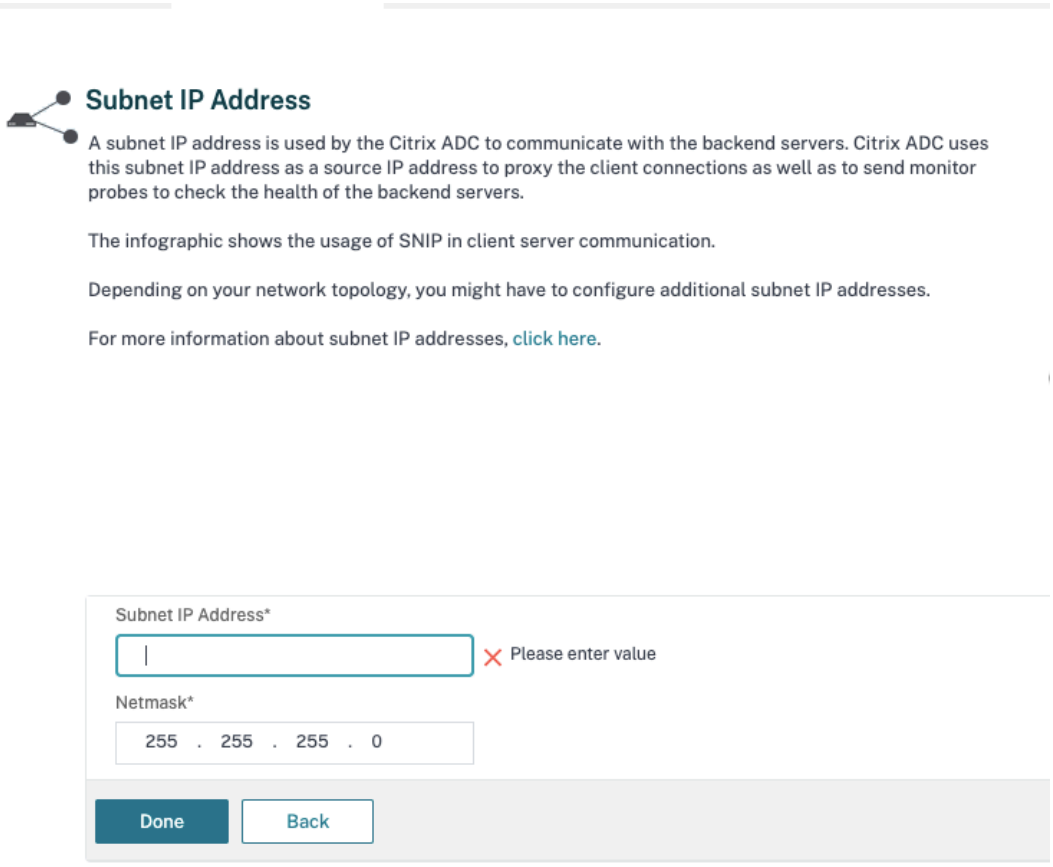
1. Assurez-vous que la configuration préalable suivante est déjà en place :

   - Les adresses IP associées à Citrix ADC suivantes sont configurées.

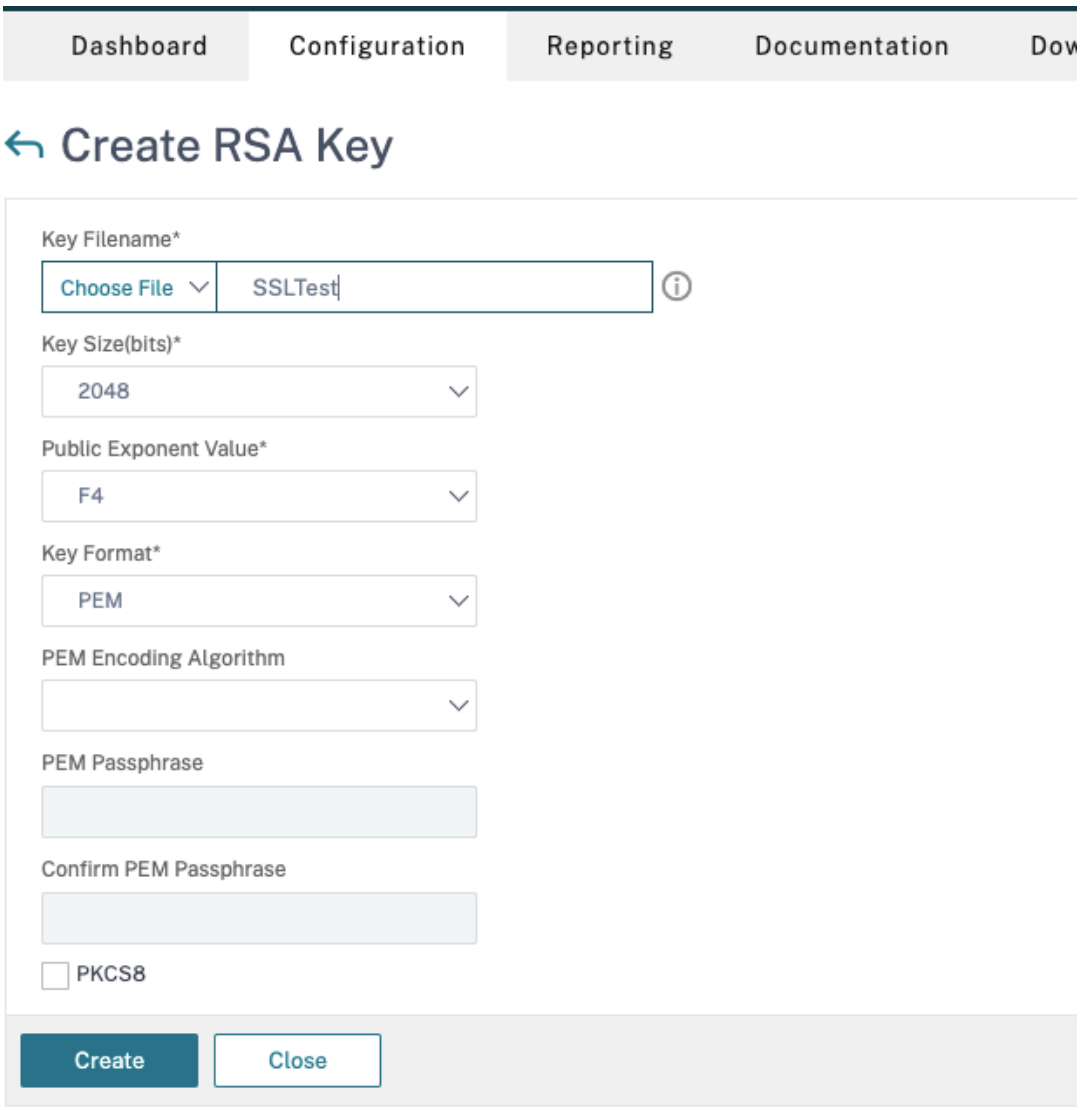
     – Adresse IP Citrix ADC Management (NSIP) permettant d'accéder à la console Citrix ADC. Pour plus d'informations, consultez la section Configuration de l'adresse NSIP.



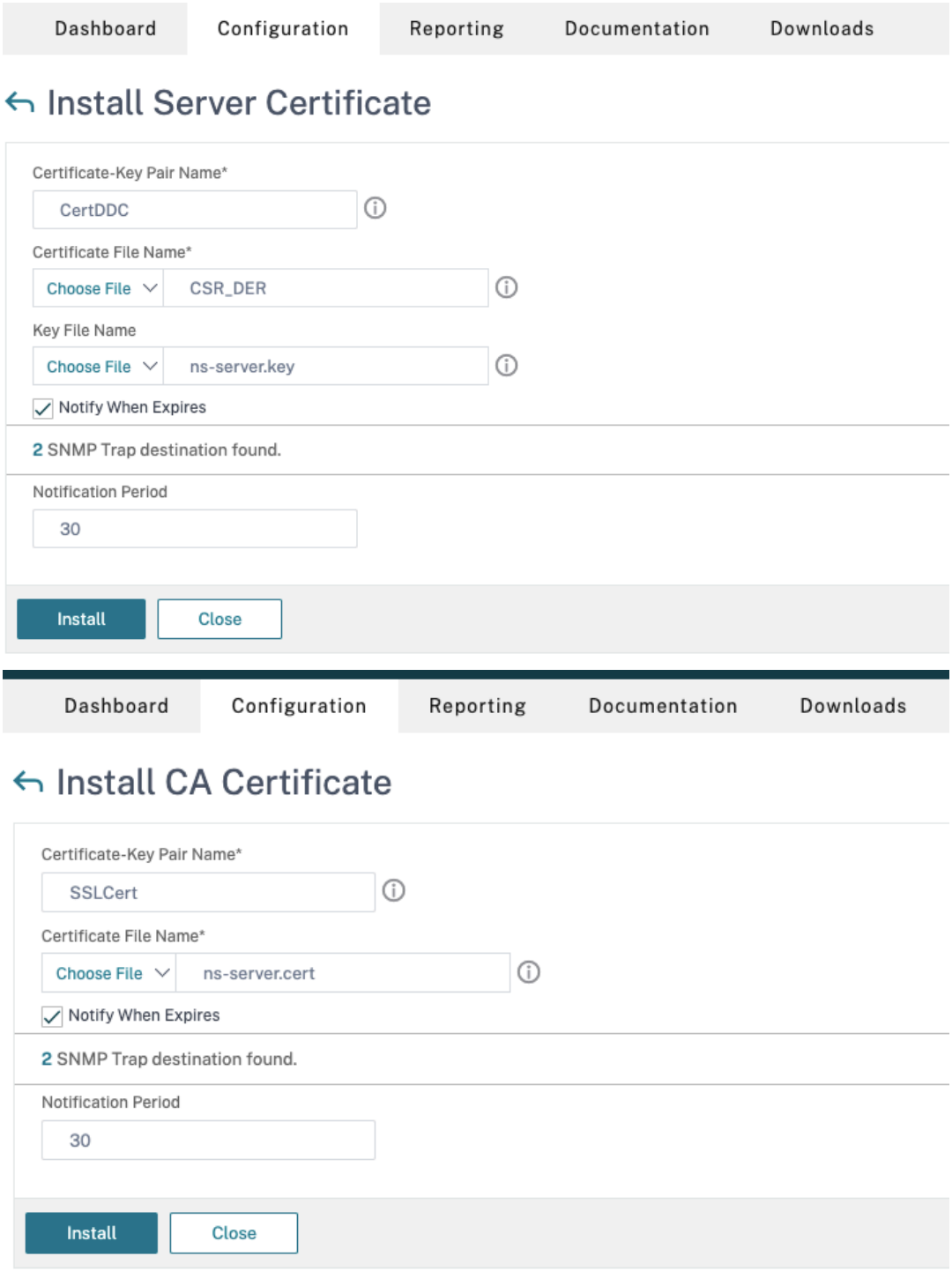
     – Adresse IP de sous-réseau (SNIP) permettant la communication entre l'appliance Citrix ADC et les serveurs principaux. Pour plus d'informations, consultez la section Configuration des adresses IP de sous-réseau.
     – Adresse IP virtuelle Citrix Gateway et adresse IP virtuelle de l'équilibreur de charge pour se connecter à l'appliance ADC pour le lancement de session. Pour plus d'informations, consultez la section Créer un serveur virtuel.



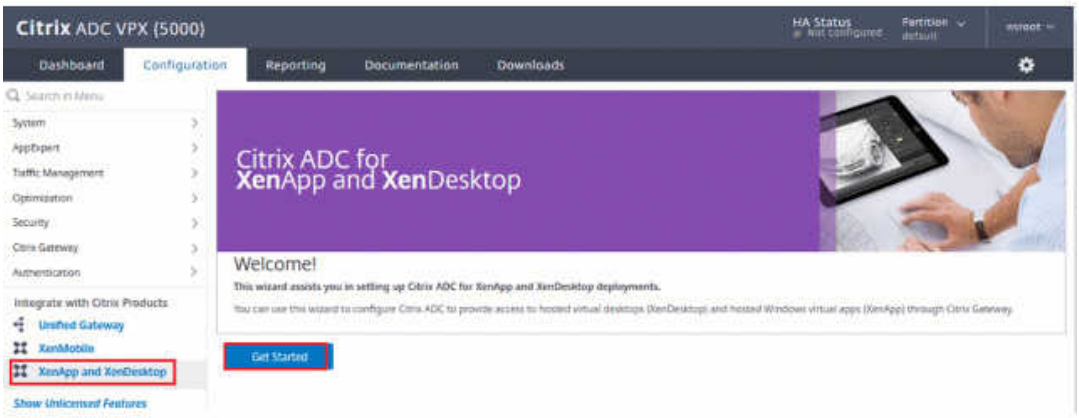
- Les modes et fonctionnalités requis dans l'appliance Citrix ADC sont activés.
  - Pour activer les modes, dans l'interface graphique Citrix ADC, accédez à **System > Settings > Configure Mode**.
  - Pour activer les fonctionnalités, dans l'interface graphique Citrix ADC, accédez à **System > Settings > Configure Basic Features**.
- 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.

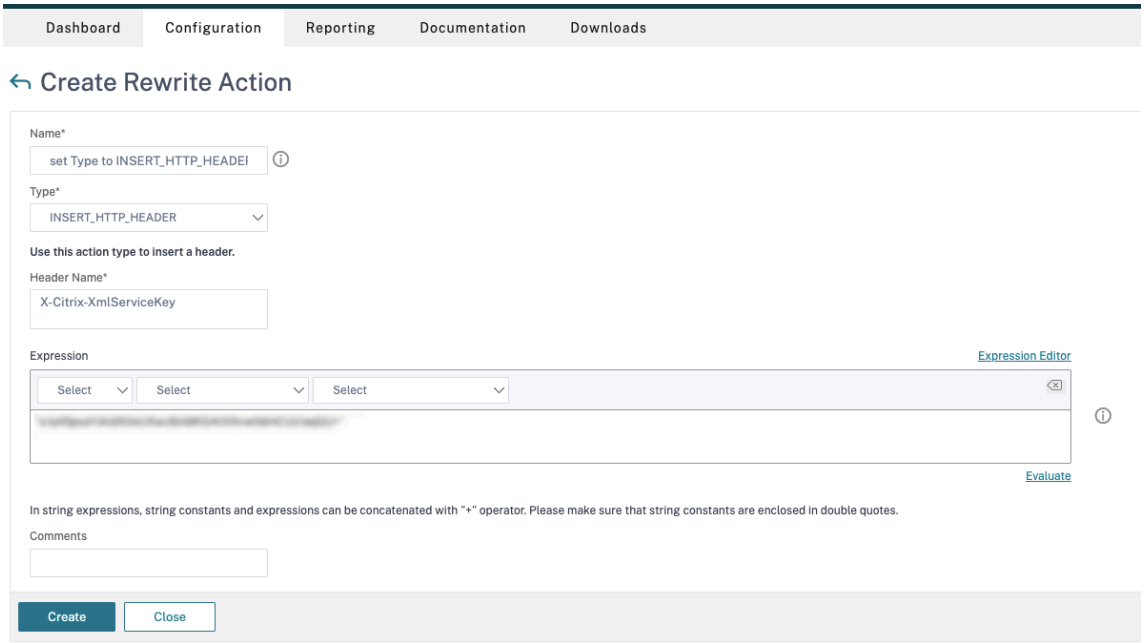


- Un composant Citrix Gateway a été créé pour Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Testez la connectivité en cliquant sur le bouton **Tester STA** pour vérifier que les serveurs virtuels sont en ligne. Pour plus d'informations, consultez la section Configuration de Citrix ADC pour Citrix Virtual Apps and Desktops.



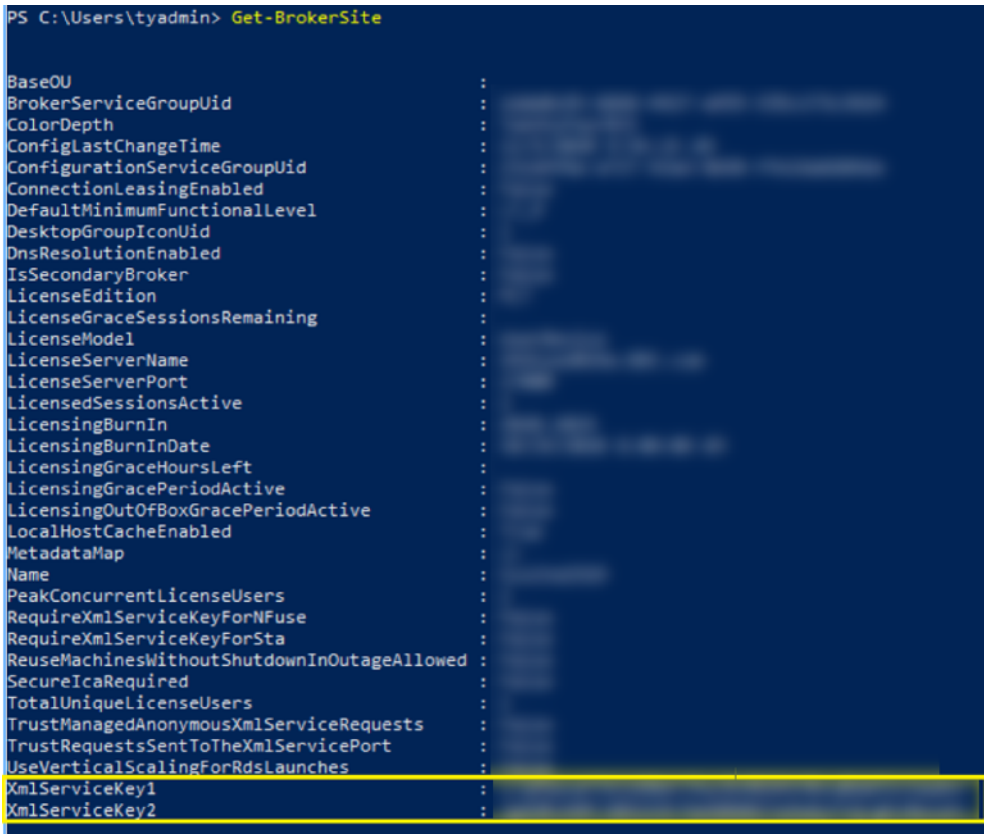
2. Ajoutez une action de réécriture. Pour plus d'informations, consultez la section Configuration d'une action de réécriture.

   a) Accédez à **AppExpert > Rewrite > 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-

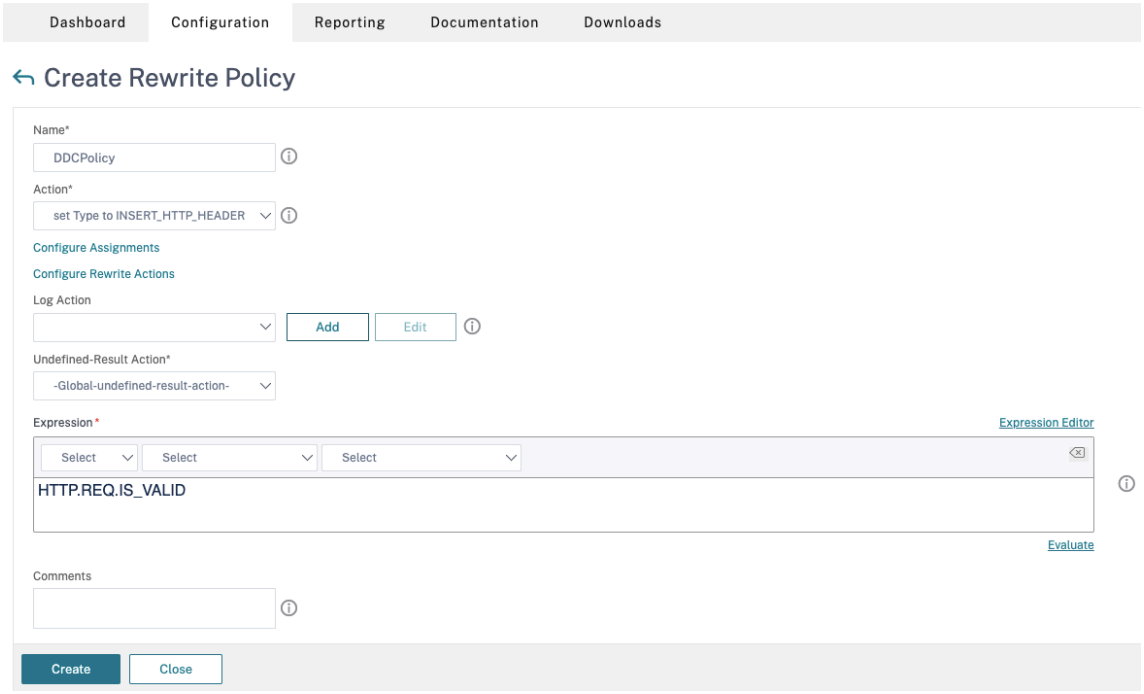
vez copier la valeur XmlServiceKey1 à partir de votre configuration Desktop Delivery Controller.



3. Ajoutez une stratégie de réécriture. Pour plus d'informations, consultez la section Configuration d'une stratégie de réécriture.

   a) Accédez à **AppExpert > Rewrite > Policies**.

   b) Cliquez sur **Add** pour ajouter une nouvelle stratégie.



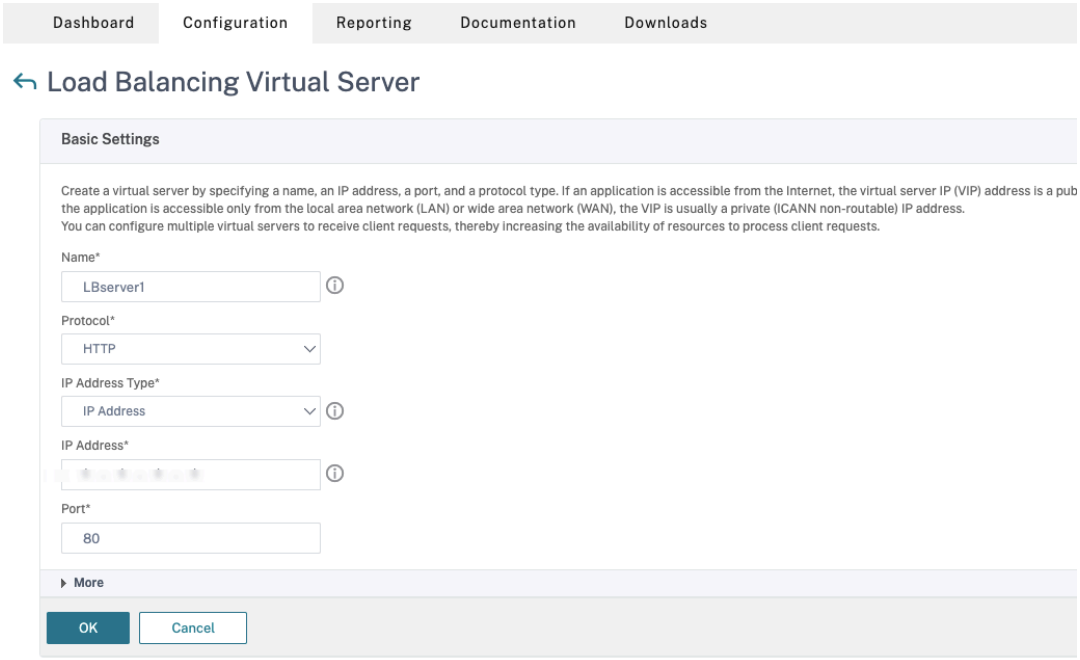
a) Dans **Action**, sélectionnez l'action créée à l'étape précédente.
b) Dans **Expression**, ajoutez HTTP.REQ.IS_VALID.
c) Cliquez sur **OK**.

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.

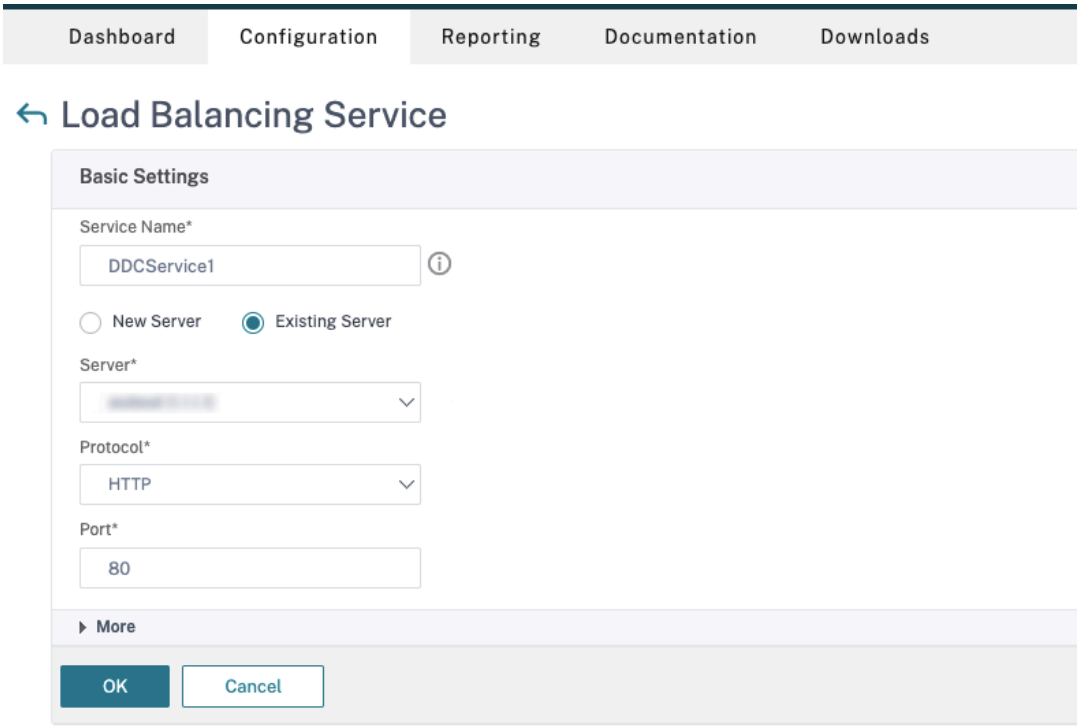
      - Accédez à **Traffic Management > Load Balancing > Servers**.
      - Dans la page **Virtual Servers**, cliquez sur **Add**.



- 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.

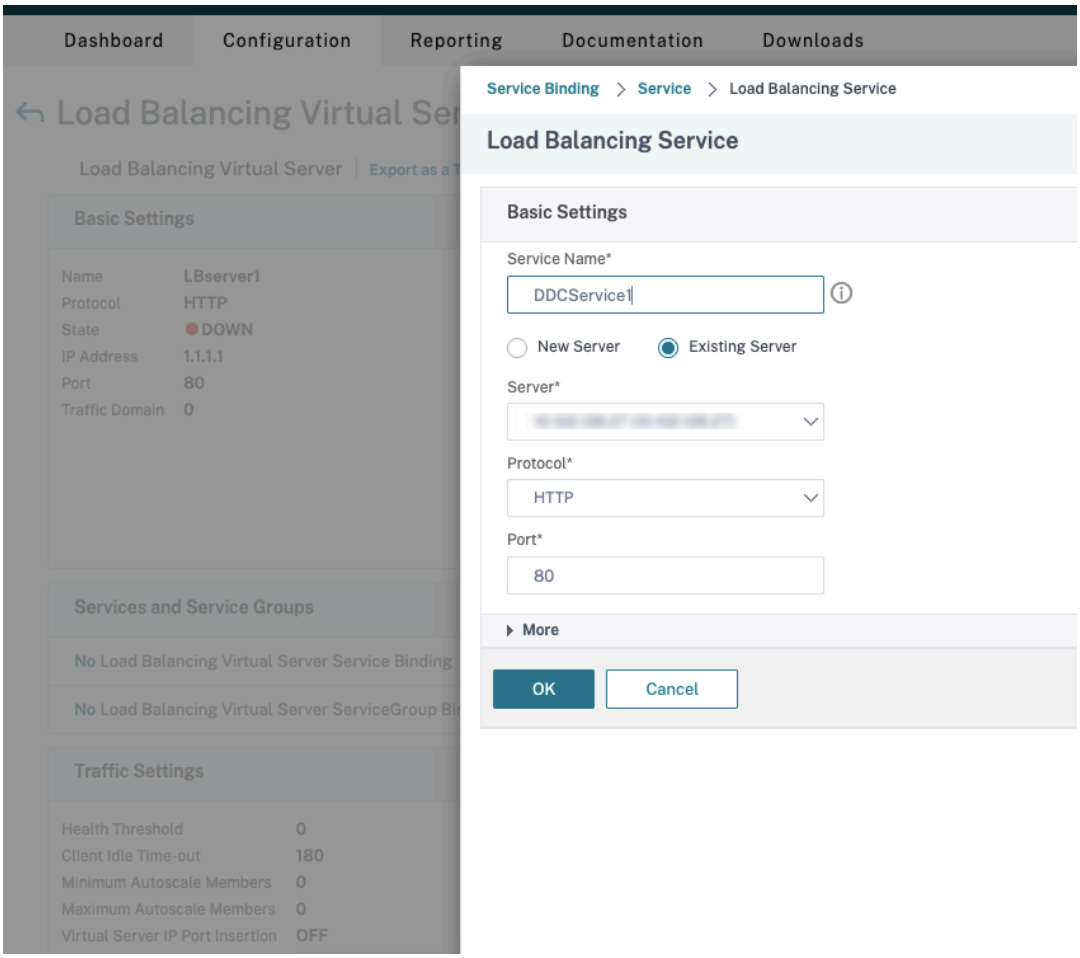
- Accédez à **Traffic Management > Load Balancing > Services**.



- 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.

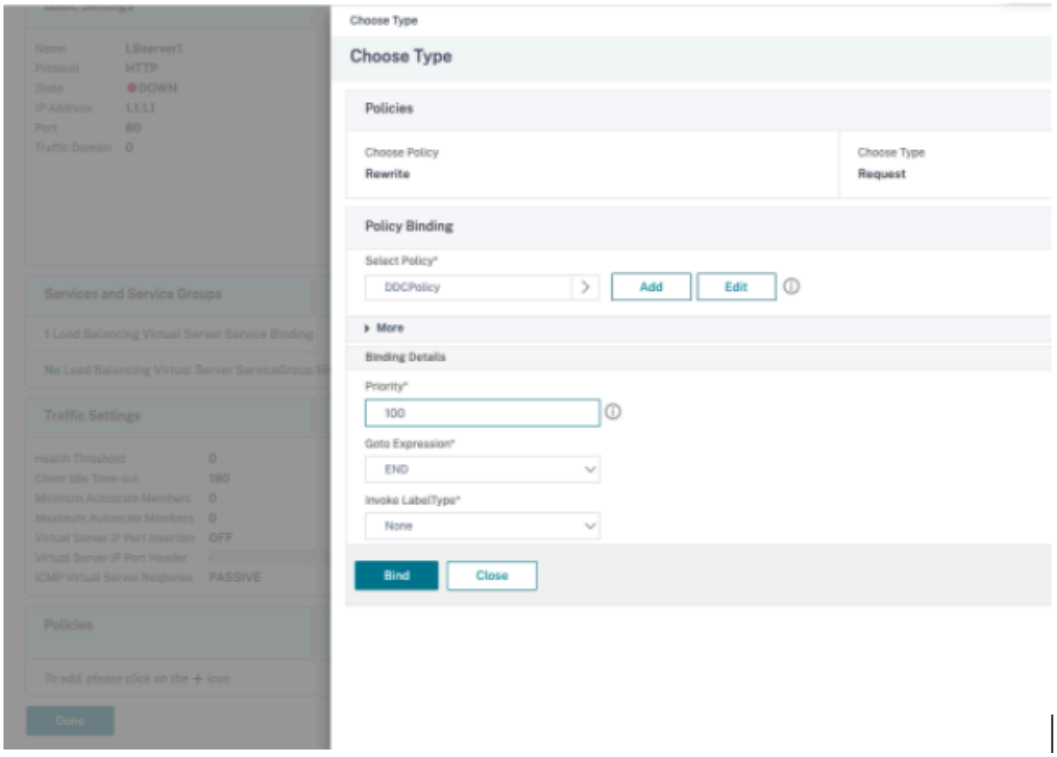
- Sélectionnez le serveur virtuel créé précédemment, puis cliquez sur **Edit**.
- Dans **Services and Service Groups**, cliquez sur **No Load Balancing Virtual Server Service Binding**.



- Dans **Service Binding**, sélectionnez l'instance Citrix DaaS créée précédemment.
- Cliquez sur **Bind**.

d) Liez la stratégie de réécriture créée précédemment au serveur virtuel.

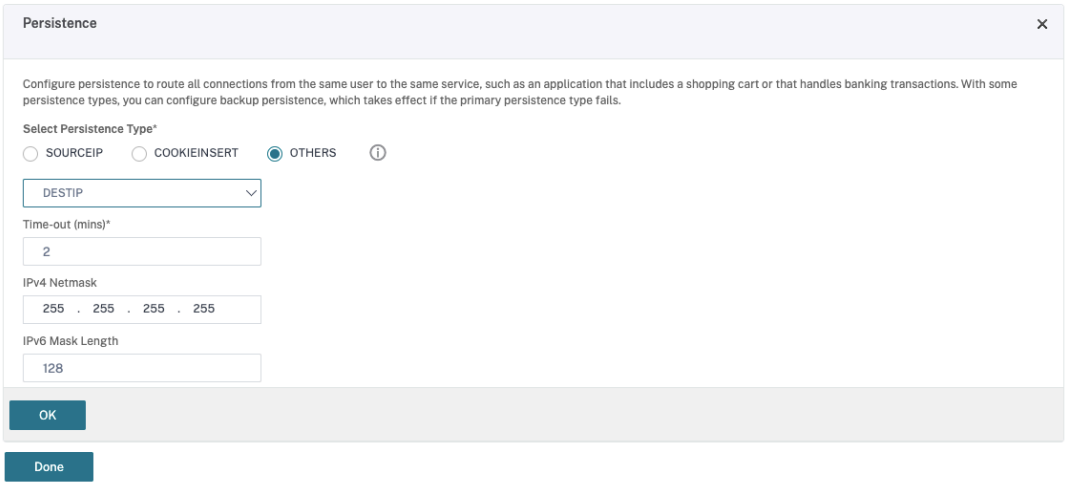
- Sélectionnez le serveur virtuel créé précédemment, puis cliquez sur **Edit**.
- Dans **Advanced Settings**, cliquez sur **Policies**, puis dans la section **Policies**, cliquez sur **+**.



- 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**.

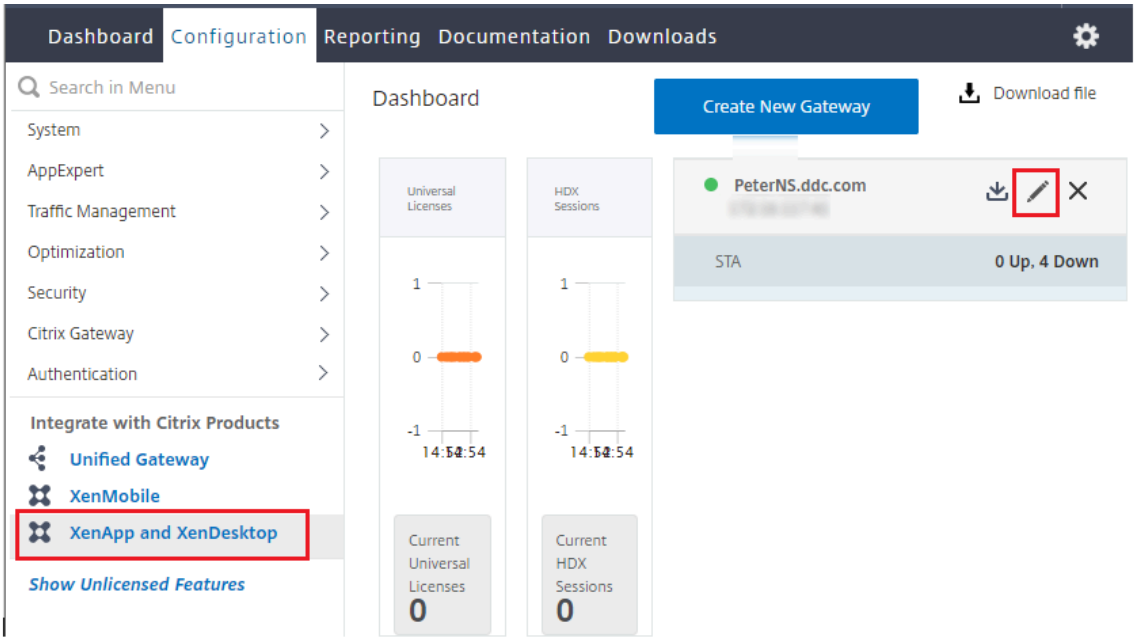
f) Répétez également ces étapes pour l'autre serveur virtuel.

Modification de la configuration si l'appliance Citrix ADC est déjà configurée avec Citrix DaaS

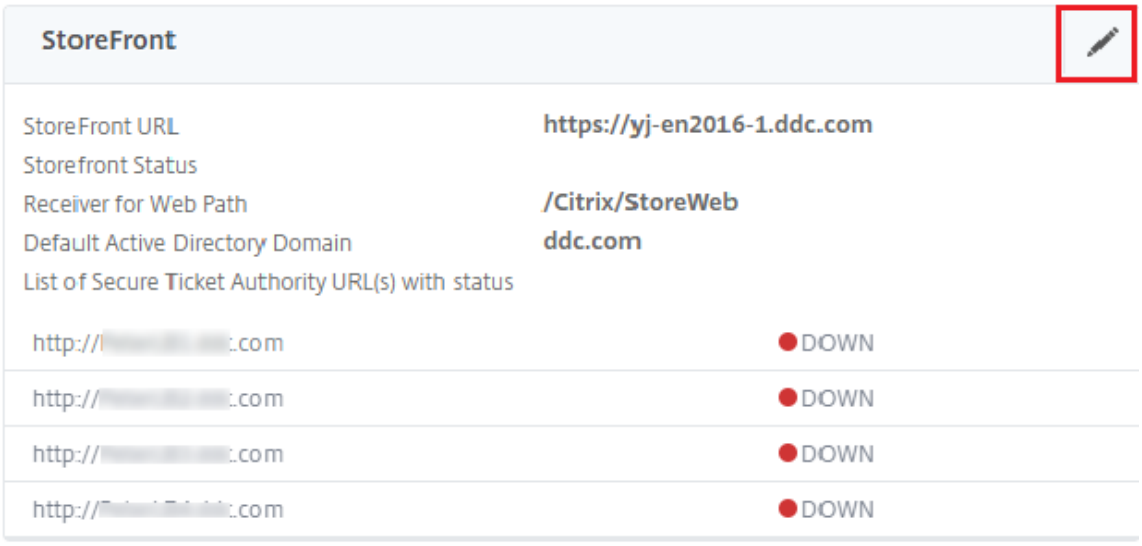
Si vous avez déjà configuré l'appliance Citrix ADC avec Citrix DaaS, pour utiliser la fonctionnalité Secure XML, vous devez apporter les modifications de configuration suivantes.

- 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 DaaS, le paramètre `TrustRequestsSentToTheXmlServicePort` est défini sur True.

1. Dans l'interface graphique Citrix ADC, accédez à **Configuration > Integrate with Citrix Products**, puis cliquez sur **XenApp and XenDesktop**.
2. Sélectionnez l'instance de passerelle et cliquez sur l'icône de modification.

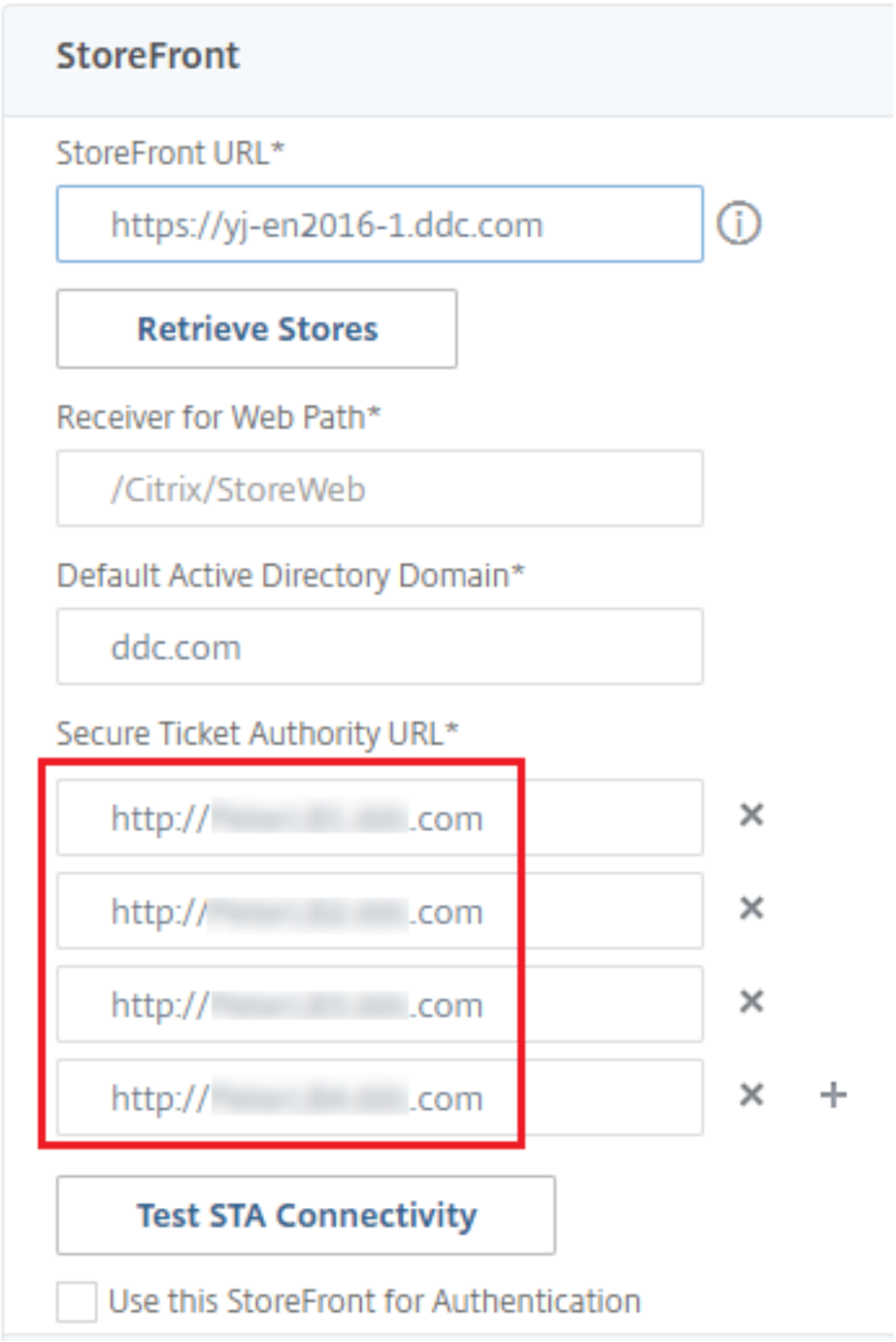


3. Dans le volet StoreFront, cliquez sur l'icône de modification.



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

March 30, 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. La possibilité de se déplacer entre plusieurs stations de travail rapidement, d'accéder aux mêmes applications chaque fois qu'ils ouvrent une session, est une priorité pour la plupart des travailleurs mobiles, tels que le personnel médical d'un hôpital.

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 par conséquent ne pas demander à l'utilisateur de devoir s'authentifier à nouveau. Si vous augmentez la durée pour laquelle une session est gardée ouverte, les risques

d'accès non autorisé sont accrus : un utilisateur distrait peut s'éloigner de sa machine cliente et 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.
- Si vous ne souhaitez pas autoriser les utilisateurs à se reconnecter aux sessions interrompues sans authentification, utilisez la fonction de 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 durée 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 durée, modifiez le registre sur la machine utilisateur :

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

où `seconds` est le nombre de secondes après lesquelles plus aucune tentative n'est faite pour reconnecter la session.

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 application Citrix Workspace après l'interruption d'une connexion.

- **Authentification de la reconnexion automatique des clients :** active ou désactive l'authentification utilisateur après 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 serveur 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.

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 sur un site, le serveur crypte ses informations d'identification, les stocke en mémoire, puis 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 de 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. Lorsqu'elle est activée, si le serveur ne détecte plus aucune activité (par exemple, aucun changement de l'horloge, aucun mouvement de la souris, aucune mise à jour de l'écran), cette fonctionnalité empêche les services Bureau à distance de se déconnecter de cette session. 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 Microsoft 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 utilisateur 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 pour les utilisateurs qui accèdent aux bureaux et aux applications via une connexion Citrix StoreFront ou via l'application Citrix Workspace. Par défaut, le contrôle de l'espace de travail est désactivé pour les sessions de bureau virtuel, mais il est 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, si l'employé d'un centre hospitalier ferme la session qu'il a ouverte sur une machine cliente dans la salle des urgences et en ouvre une autre sur une machine dans le service de radiologie, les stratégies, les mappages d'imprimante et de lecteur client correspondant à la machine cliente du service de radiologie sont appliqués à l'ouverture de session sur cette machine.

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 aussi utiliser l'interface de gestion Configuration complète. 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 en même temps. Vous pouvez afficher les applications sur plusieurs appareils. 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 l'image principale, déployez la nouvelle image dans le catalogue. Pour plus d'informations, veuillez consulter la section Modifier l'image principale.

Ce paramètre s'applique uniquement aux machines virtuelles dotées de VDA de bureau mono-session (poste de travail). Microsoft contrôle le délai de connexion sur les machines dotées de VDA de serveur multi-session.

Balises

November 24, 2023

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.

- Personnalisez les résultats de la recherche dans l'interface de gestion Configuration complète.

  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 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.

  Les détails et les exemples d'utilisation d'une restriction de balise sont décrits plus loin dans cet article.

- 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 des 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 stations de travail les plus puissantes, 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
- 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 l'interface de gestion Configuration complète :

- 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

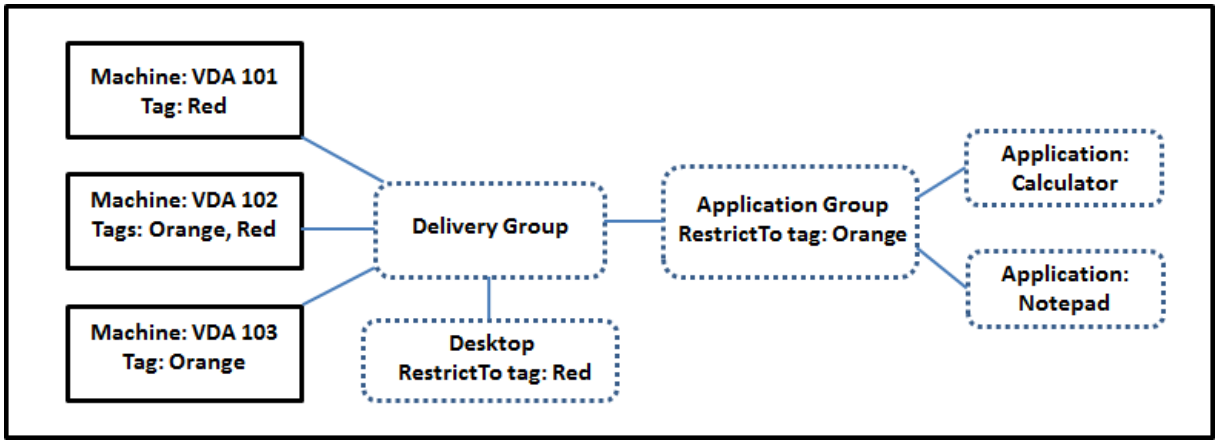
Une restriction de balise implique plusieurs étapes :

- 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 Controller. Le Controller 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 Controller 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.



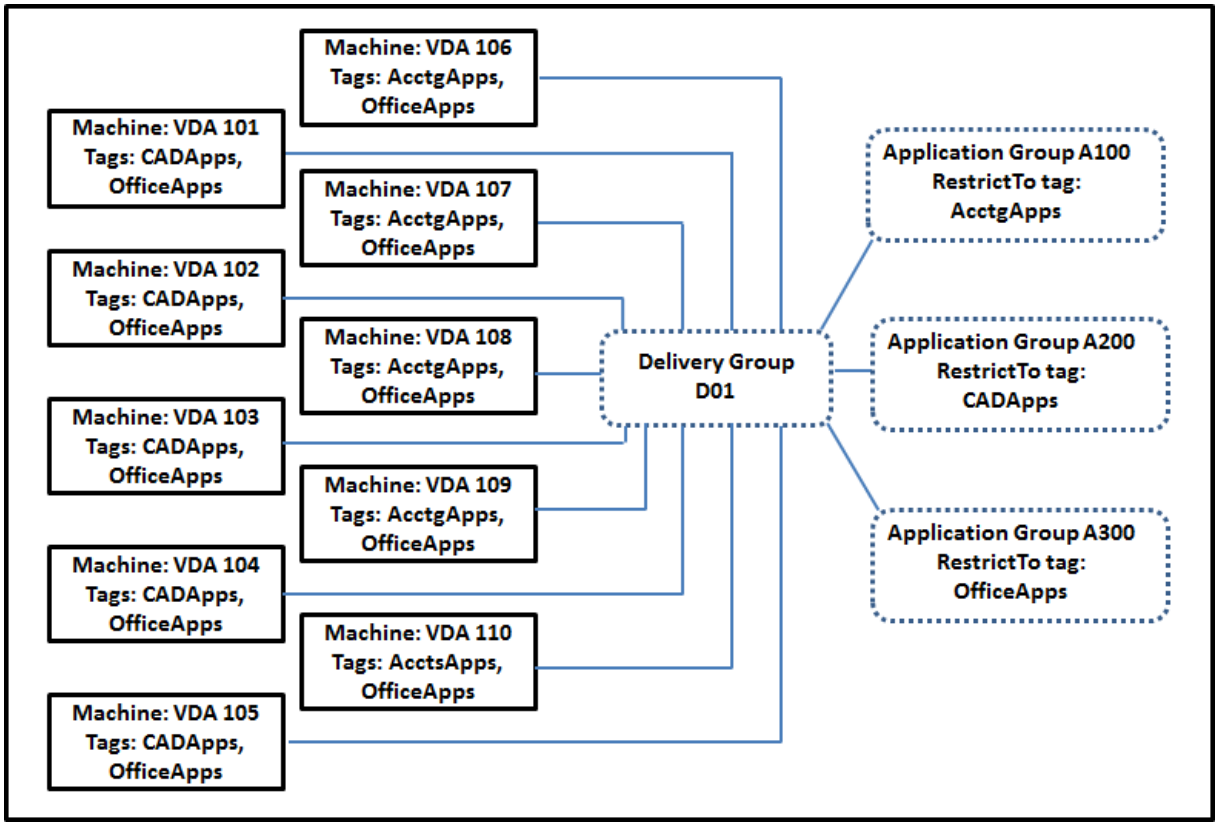
- Des balises ont été ajoutées à chacune des trois machines (VDA 101-103).
- Le bureau du groupe de mise à disposition a été créé avec une restriction de balise nommée `Red`. Ainsi, ce bureau ne peut être lancé que sur les machines de ce groupe de mise à disposition qui ont la balise `Red` : VDA 101 et 102.
- Le groupe d'applications a été créé avec la restriction de balise `Orange`. Ainsi, chacune de ses applications (`Calculator` et `Notepad`) ne peut être lancée que 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 (`Red` et `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 101-110), 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 l'interface de gestion Configuration complète.

(Exception : les balises utilisées pour les attributions de stratégie sont créées, modifiées et supprimées

via l'action **Gérer les balises**. Cependant, vous appliquez (attribuez) des balises 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.

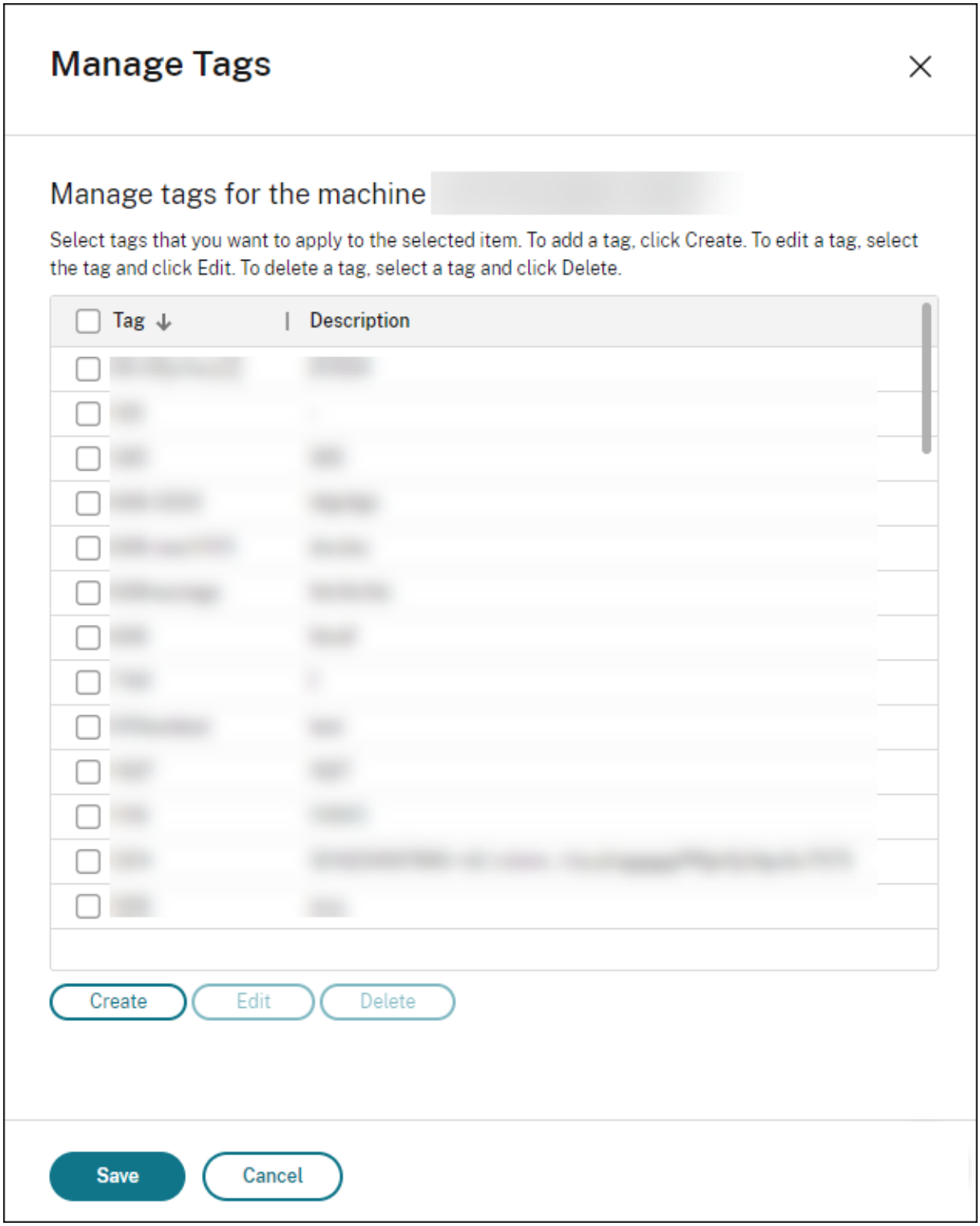
Utiliser la fonctionnalité Gérer les balises

Dans **Gérer > Configuration complète**, sélectionnez les éléments auxquels vous souhaitez appliquer une balise. Les éléments comprennent :

- Une ou plusieurs machines
- Une ou plusieurs applications
- Un bureau, un groupe de mise à disposition ou un groupe d'applications
- Un catalogue de machines

Sélectionnez ensuite **Gérer les balises** dans la barre d'actions. La boîte de dialogue **Gérer les balises** répertorie toutes les balises existantes, et pas seulement pour les éléments sélectionnés.

- Une case à cocher activée indique que la balise a déjà été ajoutée aux éléments sélectionnés. (Dans la capture d'écran ci-dessous, une balise appelée « Tag1 » est appliquée à la machine sélectionnée.)
- Si vous sélectionnez 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**. Consultez les précautions lors de l'utilisation de balises.

- **Pour créer une balise :**

Sélectionnez **Créer**. Entrez un nom et une description. Les noms de balise doivent être uniques et ne sont pas sensibles à la casse. Sélectionnez ensuite **Enregistrer**.

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. Une case à cocher contenant un trait indique que la balise est déjà appliquée sur certains éléments sélectionnés, mais pas tous. Lorsque vous sélectionnez plusieurs éléments et que la case à cocher d'une balise comporte un trait d'union, la modification par une coche affecte toutes les machines sélectionnées.

  Si vous tentez d'ajouter une balise à des machines et que cette balise est utilisée comme restriction dans un groupe d'applications, vous êtes averti que l'action peut rendre 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. Une case à cocher contenant un trait indique que la balise est déjà appliquée sur certains éléments sélectionnés, mais pas tous. Lorsque vous sélectionnez plusieurs éléments et que la case à cocher d'une balise comporte un trait d'union, désélectionner la case à cocher supprime la balise de toutes les machines sélectionnées.

  Si vous essayez de supprimer une restriction de balise d'une machine, vous êtes averti que l'action peut affecter les machines envisagées pour le démarrage. Si c'est votre intention, continuez.

- **Pour modifier une balise :**

  Sélectionnez une balise, puis sélectionnez **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 sélectionnez **Supprimer**. La boîte de dialogue **Supprimer les balises** indique le nombre d'éléments qui utilisent actuellement les balises sélectionnées (par exemple « 2 machines »). Sélectionnez un élément pour afficher plus d'informations (par exemple, les noms des deux machines sur lesquelles la balise est appliquée). Confirmez que vous souhaitez supprimer les balises.

  Vous ne pouvez pas 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.

Sélectionnez **Enregistrer** lorsque vous avez terminé dans la boîte de dialogue **Gérer les balises**.

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, puis sélectionnez **Afficher les machines** dans la barre d'actions. Sélectionnez une machine, 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 que la restriction de balise affectera, à l'aide des actions **Gérer les balises**.

- **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. Sélectionnez **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**, sélectionnez **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 être utilisée à des fins différentes. N'oubliez pas que l'ajout, le retrait et la suppression d'une balise peuvent avoir des effets inattendus. Vous pouvez utiliser une

balise pour trier les affichages des machines lorsque vous utilisez la recherche dans l'interface de gestion Configuration complète. 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.

Si vous ajoutez une balise à des machines après que cette balise est configurée en tant que restriction de balise de groupe de bureaux et d'applications, vous êtes averti que les machines peuvent être disponibles pour le lancement 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, vous voyez 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, vous êtes averti 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, 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

Lorsqu'une application a été ajoutée à	Ces machines dans les groupes de mise à disposition sélectionnés sont prises en compte pour le démarrage
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 précédent.

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 **Gérer > Configuration complète**, sélectionnez **Groupes de mise à disposition** dans le volet gauche. 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**, sélectionnez **Créer**. Créez une balise nommée `CADApps`. Sélectionnez **OK**.
4. Sélectionnez à nouveau **Créer** et créez une balise nommée `OfficeApps`. Sélectionnez **OK**.
5. 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`). Fermez ensuite 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**, sélectionnez **Créer**. Créez une balise nommée `AcctgApps`. Sélectionnez **OK**.
9. Appliquez la balise `AcctgApps` qui vient d'être créée et la balise `OfficeApps` aux machines sélectionnées en sélectionnant les cases à cocher en regard de chaque nom de balise. Fermez ensuite la boîte de dialogue.

Créez les groupes d'applications avec des restrictions de balise.

1. Dans **Gérer > Configuration complète**, sélectionnez **Applications** dans le volet gauche.
2. Sélectionnez **Créer groupe d'applications** dans la barre d'actions. L'assistant démarre.
3. Sur la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition `D01`. Sélectionnez **Restreindre les lancements aux machines dotées de balises** puis sélectionnez la balise `AcctgApps` dans la liste.
4. 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`.
5. 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.
6. 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 applications appropriés.

Appliquer des balises aux catalogues de machines

Vous pouvez utiliser **Gérer > Configuration complète** ou PowerShell pour appliquer des balises aux catalogues de machines.

- L'utilisation de l'interface de gestion est décrite à la section Gérer le balises. Les affichages du catalogue n'indiquent pas si les balises sont appliquées.
- Pour utiliser PowerShell, reportez-vous à la rubrique Utiliser PowerShell pour appliquer des balises aux catalogues.

Voici un exemple d'utilisation de balises avec des catalogues :

- Un groupe de mise à disposition contient 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.

Utiliser PowerShell pour appliquer des balises aux catalogues

Les applets de commande PowerShell suivantes sont disponibles :

- 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 précédemment créée nommée `fy2018` au catalogue nommé `acctg` :`Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`.

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 DaaS, 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
   ```

   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
   ```

3. 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).

Configuration du fuseau horaire

March 7, 2024

Personnalisez le format de la date et de l'heure dans la console de gestion en fonction de vos préférences.

> **Remarque :**
>
> Ce paramètre est spécifique à chaque compte utilisateur.

1. Accédez à **Configuration complète > Paramètres > Date et heure**.
2. Cliquez sur **Modifier** pour configurer les paramètres suivants :
   - **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).

       > **Remarque :**
       >
       > Sélectionnez l'option **Identique à l'heure locale** si vous souhaitez que le format corresponde au fuseau horaire de votre navigateur.

   - **Format de la date :**
     - Configurez le format de date en fonction de vos préférences, comme AAAA/MM/JJ.

       > **Remarque :**
       >
       > Sélectionnez l'option **Identique à l'heure locale** si vous souhaitez que le format corresponde au fuseau horaire de votre navigateur.

   - **Fuseau horaire :**
     - **UTC :** affiche la date et l'heure en UTC sur toute l'interface utilisateur. Les survols de la souris affichent la date et l'heure correspondant à votre fuseau horaire.
     - **Fuseau horaire local :** affichez la date et l'heure selon votre fuseau horaire local sur toute l'interface utilisateur. Les survols de la souris affichent la date et l'heure en UTC.

Dépanner les problèmes d'enregistrement et de lancement de session VDA

March 30, 2022

Nous proposons une fonctionnalité de vérification de l'état qui vous permet d'évaluer l'intégrité des VDA. Cette fonctionnalité vous permet d'identifier les causes possibles des problèmes courants d'enregistrement de VDA et de lancement de session via l'interface de gestion Configuration complète.

À la différence de Vérification de l'état du cloud, un outil autonome permettant d'évaluer l'état et la disponibilité du site et de ses autres composants, cette fonctionnalité est disponible en tant qu'action **Exécuter vérification de l'état** dans l'interface de gestion Configuration complète.

L'action **Exécuter vérification de l'état** peut exécuter les mêmes vérifications que Vérification de l'état du cloud, sauf les suivantes :

- Pour l'enregistrement d'un VDA :
  - Disponibilité du port de communication VDA
- Pour le lancement de session sur les VDA :
  - Disponibilité du port de communication de lancement de session
  - Chemin de lancement de l'application VDA

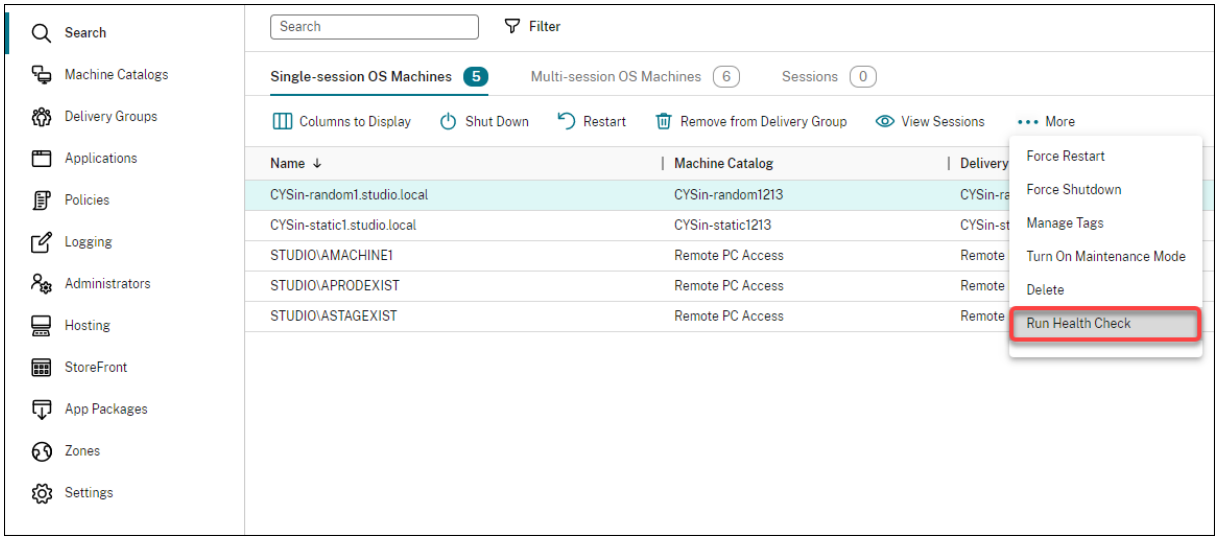
Conditions préalables

Avant d'utiliser la fonctionnalité, vérifiez que vous remplissez les conditions préalables suivantes :

- VDA Windows
- VDA version 2109 ou ultérieure
- Les VDA sont enregistrés

Effectuer des vérifications de l'état pour les VDA

1. Dans l'interface de gestion Configuration complète, accédez au nœud **Rechercher**.
2. Sélectionnez une ou plusieurs machines, puis **Exécuter vérification de l'état** dans la barre d'actions.



> **Remarque :**
>
> Actuellement, vous ne pouvez exécuter des vérifications de l'état que pour les VDA enregistrés. L'action **Exécuter vérification de l'état** n'est pas disponible pour les VDA non enregistrés.

Une fois que vous avez sélectionné **Exécuter vérification de l'état**, une fenêtre s'affiche, affichant la progression des vérifications. Attendez que les vérifications de l'état soient terminées ou cliquez sur **Annuler** pour les annuler. Si nécessaire, vous pouvez déplacer la fenêtre.

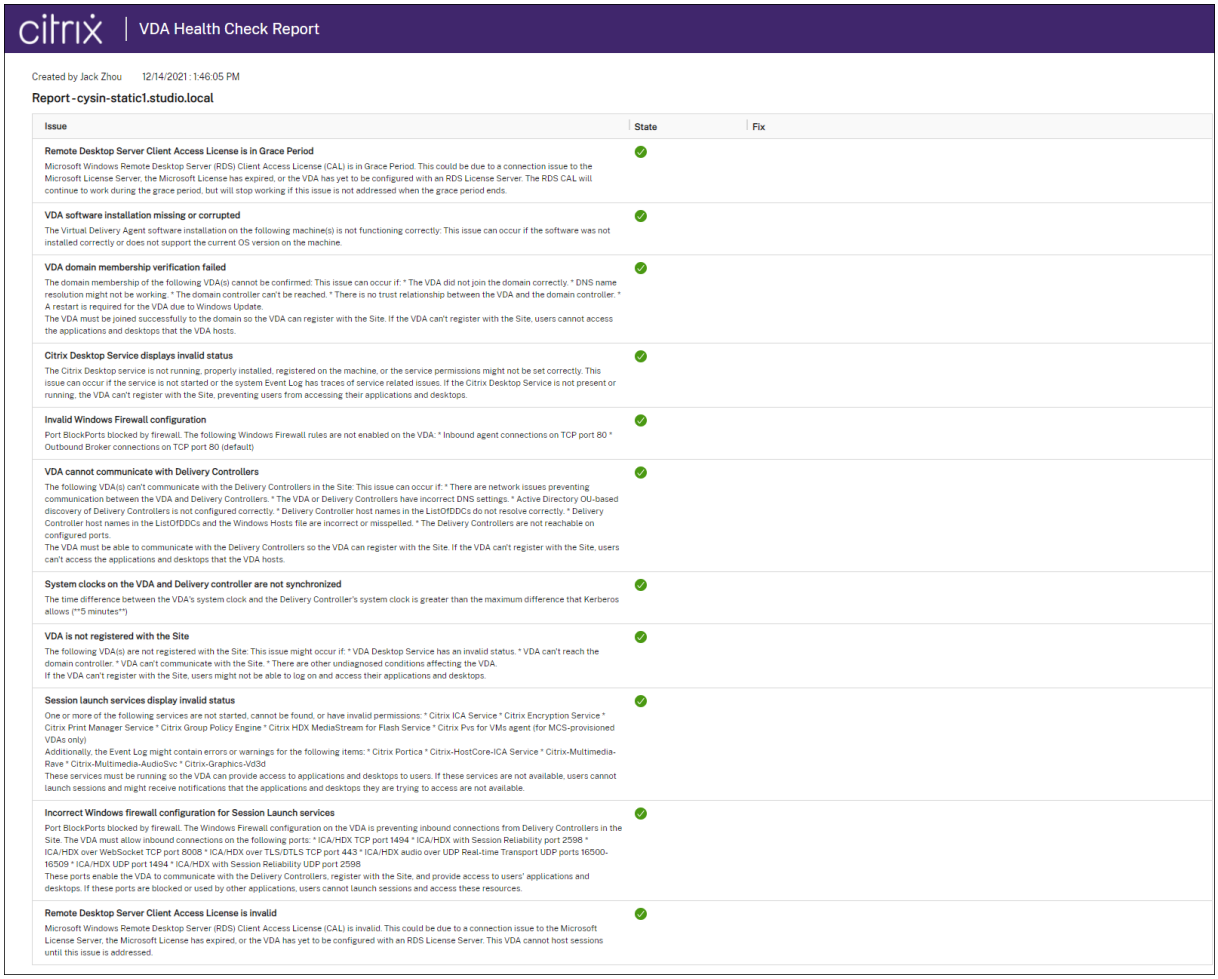
> **Remarque :**
>
> Dans les scénarios où une fenêtre « Vérification de l'état en cours » existe déjà, vous ne pouvez pas exécuter de vérifications supplémentaires tant que les vérifications existantes ne sont pas terminées.

Une fois les vérifications terminées, les deux boutons suivants apparaissent : **Afficher le rapport** et **Fermer**. Pour afficher les résultats des vérifications, cliquez sur **Afficher le rapport**.

Le rapport de vérification s'ouvre dans un nouvel onglet du navigateur. Le rapport contient les éléments suivants :

- Heure et date à laquelle le rapport de résultats a été généré

- La personne qui a effectué les vérifications de l'état
- Les vérifications sont exécutées sur les machines cibles
- Problèmes détectés, et recommandations de corrections



citrix | VDA Health Check Report

Created by Jack Zhou 12/14/2021 1:46:05 PM

Report - cysin-static1.studio.local

Issue	State	Fix
Remote Desktop Server Client Access License is in Grace Period Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is in Grace Period. This could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. The RDS CAL will continue to work during the grace period, but will stop working if this issue is not addressed when the grace period ends.		
VDA software installation missing or corrupted The Virtual Delivery Agent software installation on the following machine(s) is not functioning correctly: This issue can occur if the software was not installed correctly or does not support the current OS version on the machine.		
VDA domain membership verification failed The domain membership of the following VDA(s) cannot be confirmed: This issue can occur if: * The VDA did not join the domain correctly. * DNS name resolution might not be working. * The domain controller can't be reached. * There is no trust relationship between the VDA and the domain controller. * A restart is required for the VDA due to Windows Update. The VDA must be joined successfully to the domain so the VDA can register with the Site. If the VDA can't register with the Site, users cannot access the applications and desktops that the VDA hosts.		
Citrix Desktop Service displays invalid status The Citrix Desktop service is not running, properly installed, registered on the machine, or the service permissions might not be set correctly. This issue can occur if the service is not started or the system Event Log has traces of service related issues. If the Citrix Desktop Service is not present or running, the VDA can't register with the Site, preventing users from accessing their applications and desktops.		
Invalid Windows Firewall configuration Port BlockPorts blocked by firewall. The following Windows Firewall rules are not enabled on the VDA: * Inbound agent connections on TCP port 80 * Outbound Broker connections on TCP port 80 (default)		
VDA cannot communicate with Delivery Controllers The following VDA(s) can't communicate with the Delivery Controllers in the Site: This issue can occur if: * There are network issues preventing communication between the VDA and Delivery Controllers. * The VDA or Delivery Controllers have incorrect DNS settings. * Active Directory OU-based discovery of Delivery Controllers is not configured correctly. * Delivery Controller host names in the ListOfDDCs do not resolve correctly. * Delivery Controller host names in the ListOfDDCs and the Windows Hosts file are incorrect or misspelled. * The Delivery Controllers are not reachable on configured ports. The VDA must be able to communicate with the Delivery Controllers so the VDA can register with the Site. If the VDA can't register with the Site, users can't access the applications and desktops that the VDA hosts.		
System clocks on the VDA and Delivery controller are not synchronized The time difference between the VDA's system clock and the Delivery Controller's system clock is greater than the maximum difference that Kerberos allows (**5 minutes**)		
VDA is not registered with the Site The following VDA(s) are not registered with the Site: This issue might occur if: * VDA Desktop Service has an invalid status. * VDA can't reach the domain controller. * VDA can't communicate with the Site. * There are other undiagnosed conditions affecting the VDA. If the VDA can't register with the Site, users might not be able to log on and access their applications and desktops.		
Session launch services display invalid status One or more of the following services are not started, cannot be found, or have invalid permissions: * Citrix ICA Service * Citrix Encryption Service * Citrix Print Manager Service * Citrix Group Policy Engine * Citrix HDX MediaStream for Flash Service * Citrix Pvs for VMs agent (for MCS-provisioned VDAs only) Additionally, the Event Log might contain errors or warnings for the following items: * Citrix Portica * Citrix-HostCore-ICA Service * Citrix-Multimedia-Rave * Citrix-Multimedia-AudioSvc * Citrix-Graphics-Vd3d These services must be running so the VDA can provide access to applications and desktops to users. If these services are not available, users cannot launch sessions and might receive notifications that the applications and desktops they are trying to access are not available.		
Incorrect Windows firewall configuration for Session Launch services Port BlockPorts blocked by firewall. The Windows Firewall configuration on the VDA is preventing inbound connections from Delivery Controllers in the Site. The VDA must allow inbound connections on the following ports: * ICA/HDX TCP port 1494 * ICA/HDX with Session Reliability port 2598 * ICA/HDX over WebSocket TCP port 8008 * ICA/HDX over TLS/DTLS TCP port 443 * ICA/HDX audio over UDP Real-time Transport UDP ports 16500-16509 * ICA/HDX UDP port 1494 * ICA/HDX with Session Reliability UDP port 2598 These ports enable the VDA to communicate with the Delivery Controllers, register with the Site, and provide access to users' applications and desktops. If these ports are blocked or used by other applications, users cannot launch sessions and access these resources.		
Remote Desktop Server Client Access License is invalid Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is invalid. This could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. This VDA cannot host sessions until this issue is addressed.		

Vous pouvez effectuer des vérifications individuellement et par lots.

> **Remarque :**
>
> Lorsque vous exécutez des vérifications par lots, ne sélectionnez pas plus de 10 machines. Sinon, l'action **Exécuter vérification de l'état** n'est pas disponible.

Accès des utilisateurs

April 20, 2023

Deux composants principaux fournissent l'accès aux applications et aux bureaux dans un déploiement Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) :

- **Plate-forme Citrix Workspace** : la plate-forme Citrix Workspace est une solution numérique complète qui vous permet de fournir un accès sécurisé aux informations, applications et autres contenus pertinents pour le rôle d'une personne dans votre organisation. Les utilisateurs s'abonnent aux services que vous mettez à disposition et peuvent y accéder depuis n'importe où, sur n'importe quel appareil. La plate-forme Citrix Workspace vous aide à organiser et à automatiser les détails les plus importants dont vos utilisateurs ont besoin pour collaborer, prendre de meilleures décisions et se concentrer pleinement sur leur travail.

  Le déploiement de Citrix Workspace ne demande aucun effort et il est tenu à jour par Citrix. La plate-forme Citrix Workspace est recommandée pour les nouveaux clients, les clients existants, les évaluations et les preuves de concept.

- **StoreFront local :** les clients peuvent également utiliser un StoreFront existant pour regrouper les applications et les bureaux dans Citrix Cloud. Ce cas d'utilisation offre une plus grande sécurité, y compris la prise en charge de l'authentification à deux facteurs, et empêche les utilisateurs d'entrer leur mot de passe dans le service de cloud. Elle permet également aux clients de personnaliser leurs noms de domaine et leurs URL. Ce type de déploiement est recommandé pour les clients Citrix Virtual Apps and Desktops qui disposent déjà d'un déploiement StoreFront.

  Consultez également Cache d'hôte local et StoreFront.

Lorsque les utilisateurs se connectent en dehors du pare-feu d'entreprise, Citrix Cloud peut utiliser la technologie Citrix Gateway (anciennement NetScaler Gateway) pour sécuriser les connexions avec le protocole SSL. L'appliance virtuelle Citrix Gateway ou Citrix 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.

Utilisation de Citrix Workspace

L'accès aux espaces de travail se fait via `https://<customername>.cloud.com`. Si nécessaire, vous pouvez personnaliser la partie `<customername>` de l'URL de l'espace de travail. Vous pouvez ensuite configurer la connectivité pour chaque emplacement de ressources que vous souhaitez utiliser afin que les utilisateurs puissent accéder aux ressources de leur espace de travail. Les utilisateurs accèdent à leur espace de travail à l'aide de la dernière version de l'application Citrix Workspace.

Pour plus d'informations sur l'utilisation de Citrix Workspace, consultez :

- Configurer les espaces de travail : pour configurer l'accès et les personnalisations.
- Espaces de travail sécurisés : pour configurer l'authentification.
- Gérer votre expérience d'espace de travail : pour comprendre comment les utilisateurs accèdent à leur espace de travail et comment il apparaît.

Pour fournir un accès distant aux utilisateurs via Citrix Workspace, vous pouvez utiliser le service Citrix Gateway ou votre propre Citrix Gateway.

- Pour utiliser le service Citrix Gateway :

  1. Dans **Citrix Cloud > Emplacements de ressources**, sélectionnez **Passerelle** pour l'emplacement de ressources que vous souhaitez utiliser.
  2. Sélectionnez **Gateway Service**, puis cliquez sur **Enregistrer**.
  3. Dans **Citrix Cloud > Configuration de l'espace de travail > Intégrations de services**, recherchez le Gateway Service et sélectionnez **Activer** dans le menu des points de suspension.

- Pour utiliser votre propre Citrix Gateway :

  1. Configurez Citrix Gateway en tant que proxy ICA (aucune stratégie d'authentification ou de session n'est nécessaire).
  2. Configurer un emplacement de ressources pour utiliser Citrix Gateway :

     a) Dans **Citrix Cloud > Emplacements de ressources**, sélectionnez **Passerelle** pour l'emplacement de ressources que vous souhaitez utiliser.
     b) Sélectionnez **Gateway traditionnel** et entrez le nom de domaine complet externe. N'ajoutez pas de protocole. Les ports sont facultatifs. Une combinaison d'accès à distance et d'accès interne n'est pas prise en charge dans Citrix Workspace.

  3. Liez les connecteurs Citrix Cloud Connector en tant que serveurs STA avec Citrix Gateway. Pour plus de détails, consultez l'article CTX232640.

     > **Remarque :**
     >
     > Seules les machines Citrix Cloud Connector sont prises en charge pour une utilisation en tant que serveurs STA avec Citrix Gateway. L'utilisation d'autres connecteurs en tant que serveurs STA, tels que Connector Appliance, n'est pas prise en charge.

Pour plus d'informations sur le service Citrix Gateway et Citrix Gateway, reportez-vous à la section Citrix Gateway.

Utilisation d'un StoreFront local

Pour plus de détails sur la configuration d'un magasin StoreFront local, consultez la documentation StoreFront.

L'un des avantages de l'utilisation d'une instance StoreFront existante est que Citrix Cloud Connector fournit un cryptage des mots de passe des utilisateurs. Le Cloud Connector crypte les informations d'identification avec AES-256, à l'aide d'une clé unique générée de manière aléatoire. Cette clé est

renvoyée directement à l'application Citrix Workspace et n'est jamais envoyée au cloud. L'application Citrix Workspace la fournit ensuite au VDA lors du lancement de session afin de décrypter les informations d'identification et de fournir une expérience de connexion unique à Windows.

- Pour le transport, sélectionnez HTTP et le port 80. La machine StoreFront doit pouvoir accéder directement au Cloud Connector via le nom de domaine complet (FQDN) fourni. Le Cloud Connector doit pouvoir atteindre l'URL Cloud NFuse/STA sur (`https://<customername\>.xendesktop.net/Scripts/wpnbr.dll` et `ctxsta.dll`).
- Ajoutez des connecteurs cloud en tant que Delivery Controller pour une haute disponibilité.

Utilisez la version la plus récente de StoreFront.

Accès externe

Pour fournir un accès externe via Citrix Gateway et un magasin StoreFront local, procédez comme suit :

- Configurez Citrix Gateway comme lors d'un déploiement habituel avec des stratégies d'authentification et de session. Pour plus d'informations, consultez la documentation relative à Citrix Gateway.
- Pointez les Delivery Controller de votre magasin StoreFront local vers les connecteurs Citrix Cloud Connector. Liez les Cloud Connector en tant que serveurs STA à Citrix Gateway.
- Citrix Gateway doit utiliser les mêmes URL STA que StoreFront. Si la passerelle n'est pas déjà configurée pour utiliser l'autorité STA d'un environnement Citrix Virtual Apps and Desktops, les Citrix Cloud Connector peuvent être utilisés comme STA.

Accès interne

Pour fournir un accès interne via un StoreFront local, pointez les Delivery Controller du magasin StoreFront local vers les Citrix Cloud Connector.

Accès externe et interne

Pour fournir un accès externe et interne via Citrix Gateway et un magasin StoreFront local, procédez comme suit :

- Configurez Citrix Gateway comme lors d'un déploiement habituel avec des stratégies d'authentification et de session. Pour plus d'informations, consultez la documentation relative à Citrix Gateway.
- Liez les Cloud Connector en tant que serveurs STA à Citrix Gateway.

- Pointez les Delivery Controller de votre magasin StoreFront local vers les connecteurs Cloud Connector.

Cache hôte local et StoreFront

Le cache d'hôte local permet de poursuivre les opérations de négociation de connexion dans un déploiement Citrix DaaS lorsqu'un Cloud Connector ne peut pas communiquer avec Citrix Cloud.

La fonctionnalité Cache d'hôte local fonctionne uniquement dans les emplacements de ressources contenant un StoreFront local déployé par le client. Le cache d'hôte local n'est pas pris en charge pour une utilisation avec Citrix Workspace.

Un StoreFront local doit être déployé par le client sur chaque emplacement de ressources. Vérifiez que l'emplacement de ressources contient un StoreFront local qui pointe vers tous les Cloud Connector dans cet emplacement de ressources.

Pour plus d'informations, veuillez consulter la section Cache d'hôte local.

IP virtuelle et boucle virtuelle

March 30, 2022

> **Important :**
>
> Le multi-session Windows 10 Enterprise ne prend pas en charge Virtualisation IP des services Bureau à distance (Virtual IP) et nous ne prenons pas en charge Virtual IP ni Virtual Loopback sur un multi-session Windows 10 Enterprise.

Les fonctionnalités d'adresses IP virtuelles et de bouclage virtuel sont prises en charge sur les machines Windows Server 2016. Elles ne s'appliquent pas aux machines avec OS de bureau Windows.

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 (127.0.0.1 par défaut) pour utiliser une adresse de bouclage virtuel 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 des sessions à 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 échoueront car le port est déjà utilisé.

Pour assurer un fonctionnement correct de ces applications dans l'environnement Citrix Virtual Apps, chaque machine nécessite une adresse IP unique.

Les adresses IP virtuelles et le bouclage virtuel sont des fonctionnalités indépendantes. Vous pouvez sélectionnez ces deux options ou l'une ou l'autre.

Résumé des actions de l'administrateur :

- Pour utiliser l'adresse IP virtuelle Microsoft, activez 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.

IP virtuelle

Lorsque l'adresse IP virtuelle 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 une adresse IP virtuelle dans les 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 IP virtuelles :

1. Obtenez l'outil TCP View auprès de Microsoft. Cet outil répertorie toutes les applications liées à des adresses IP et ports spécifiques.
2. Désactivez la fonction Résoudre les adresses IP afin de visualiser les adresses au lieu des noms d'hôtes.
3. Lancez l'application et utilisez l'outil 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. Consultez la documentation Microsoft pour obtenir des instructions.

- Lorsque cette fonctionnalité est activée, au démarrage de la session, le serveur demande des adresses IP attribuées dynamiquement auprès du serveur DHCP.
- La fonctionnalité de virtualisation IP des services Bureau à distance attribue les adresses IP aux connexions 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 ensuite que l'adresse IP qu'elle doit 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 demandée, la fonctionnalité d'adresse IP virtuelle intercepte l'adresse IP retournée et la remplace par l'adresse IP virtuelle de la session. Les applications qui tentent d'obtenir l'adresse IP du serveur local à travers ce type de fonctions de nom n'obtiennent que l'adresse IP virtuelle 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 IP virtuelle recherche également 0.0.0.0 dans ces types d'appels et modifie l'appel en écoute sur l'adresse IP virtuelle spécifique, ce qui permet à plusieurs applications d'écouter sur le même port sur le même ordinateur, car ils effectuent l'écoute sur des adresses différentes. Cette écoute est uniquement modifiée si une session ICA et la fonction d'adresse IP virtuelle sont activées. Par exemple, si deux instances d'une application exécutée dans des sessions différentes tentent toutes deux de se lier à toutes les interfaces (0.0.0.0) et à un port spécifique (comme 9000), elles sont liées à VIPAddress1:9000 et VIPAddress2:9000, sans aucun conflit.

Bouclage virtuel

L'activation des paramètres de stratégie d'adresse IP virtuelle 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 ; cela 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 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.

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

May 17, 2024

Introduction

Les déploiements Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) répartis sur différents emplacements géographiques et connectés à un réseau étendu peuvent rencontrer des problèmes de latence réseau et de fiabilité. L'utilisation 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. Dans l'environnement Citrix DaaS, chaque emplacement de ressources est considéré comme une zone.

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, ce qui améliore les performances. Les zones 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.

Dans cet article, le terme « local » fait référence à la zone dont il est question. Par exemple, « Un VDA s'enregistre auprès d'un Cloud Connector local » signifie qu'un VDA s'enregistre auprès d'un Cloud Connector dans la zone dans laquelle le VDA est situé.

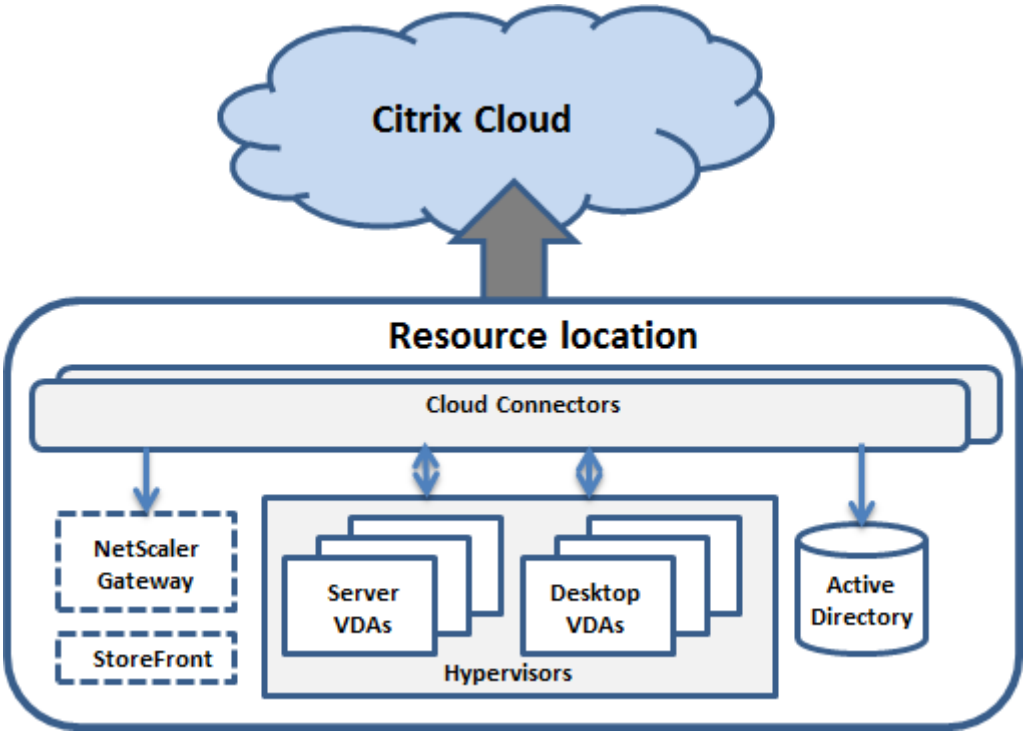
Différences par rapport aux zones des environnements Citrix Virtual Apps and Desktops locaux

Les zones d'un environnement Citrix DaaS sont similaires, mais pas identiques à celles d'un déploiement local de Citrix Virtual Apps and Desktops.

- Dans Citrix DaaS, les zones sont créées automatiquement lorsque vous créez un emplacement de ressources et que vous y ajoutez un Cloud Connector. Contrairement à un déploiement local, un environnement Citrix DaaS ne classe pas les zones en tant que zones primaires ou satellites.
- Dans XenApp version 6.5 et versions antérieures, les zones incluaient des collecteurs de données. Citrix DaaS n'utilise pas de collecteurs de données pour les zones. En outre, les zones de basculement et les zones préférées fonctionnent différemment.

Que contient une zone ?

Une zone équivaut à un emplacement de ressources. Lorsque vous créez un emplacement de ressources et installez un Cloud Connector, une zone est automatiquement créée pour vous. Chaque zone peut contenir différents types de ressources, en fonction de vos besoins et de votre environnement.



Au moins un Cloud Connector doit être installé sur chaque zone, de préférence deux ou plus, afin d'assurer la redondance.

Vous pouvez placer des catalogues de machines, hyperviseurs, connexions hôtes, utilisateurs et applications dans une zone. Une zone peut également contenir des serveurs Citrix Gateway et StoreFront. Pour utiliser la fonctionnalité de cache d'hôte local, une zone doit disposer d'un serveur StoreFront.

Les zones sont prises en charge par Citrix Workspace et le service Citrix Gateway.

Le placement d'éléments dans une zone affecte la façon dont Citrix DaaS interagit avec ces derniers et avec d'autres objets qui leur sont liés.

- Lorsqu'une connexion d'hyperviseur est placée dans une zone, il est supposé que tous les hyperviseurs gérés via cette connexion résident également dans cette zone.
- Lorsqu'un catalogue de machines est placé dans une zone, il est supposé que tous les VDA de ce catalogue se trouvent dans la zone.
- Des instances de Citrix Gateway peuvent être ajoutées aux zones. Lorsque vous créez un emplacement de ressources, vous avez la possibilité d'ajouter un Citrix Gateway. Lorsqu'une

passerelle Citrix Gateway est associée à une zone, elle est utilisée de préférence lorsque des connexions à des VDA dans cette zone sont utilisées.
- Dans l'idéal, Citrix Gateway situé dans une zone est utilisé pour les connexions utilisateur entrant dans cette zone depuis d'autres zones ou des emplacements externes. Vous pouvez également l'utiliser pour les connexions au sein de la zone.
- Après avoir créé des emplacements de ressources supplémentaires et y avoir installé des Cloud Connector (ce qui crée automatiquement des zones supplémentaires), vous pouvez déplacer des ressources entre les zones. La contrepartie de cette flexibilité est le risque de séparer des éléments qui fonctionnent mieux quand ils sont proches les uns des autres. 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. Par conséquent, 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.

Si la connexion entre une zone et Citrix Cloud échoue, la fonctionnalité Cache d'hôte local active un Cloud Connector dans la zone afin de continuer à établir des connexions avec les VDA de cette zone. (Un StoreFront doit être installé sur la zone) Ce scénario peut par exemple être efficace dans un bureau où les utilisateurs utilisent un site StoreFront local pour accéder à leurs ressources locales, même si la liaison WAN connectant leur bureau au réseau d'entreprise échoue. Pour plus d'informations, veuillez consulter la section Cache d'hôte local.

Où les VDA sont-ils enregistrés ?

Les VDA doivent être à la version minimale 7.7 pour utiliser ces fonctionnalités d'enregistrement de zone :

- Un VDA situé dans une zone s'enregistre auprès d'un Cloud Connector local.
  - Tant que ce Cloud Connector peut communiquer avec Citrix Cloud, les opérations normales se poursuivent.
  - Si ce Cloud Connector est opérationnel, mais qu'il ne peut pas communiquer avec Citrix Cloud (et que la zone est dotée d'un StoreFront local), il entre en mode panne Cache d'hôte local.
  - Si un Cloud Connector échoue, les VDA dans cette zone tentent de s'enregistrer auprès d'autres Cloud Connector locaux. Un VDA dans une zone ne tente jamais de s'enregistrer auprès d'un Cloud Connector dans une autre zone.
- Si vous ajoutez ou supprimez un Cloud Connector d'une zone (à l'aide de la console de gestion Citrix Cloud), et que la mise à jour automatique est activée, les VDA dans cette zone reçoivent des listes mises à jour des Cloud Connector qui sont disponibles ; cela leur permet de savoir auprès de quels Cloud Connector ils peuvent s'enregistrer et accepter des connexions.

- Si vous déplacez un catalogue de machines vers une autre zone (à l'aide de l'interface de gestion Configuration complète), les VDA de ce catalogue s'enregistrent auprès des Cloud Connector situés dans la zone dans laquelle vous avez déplacé le catalogue. Lorsque vous déplacez un catalogue, assurez-vous de déplacer également toute connexion hôte associée à la même zone.
- Lors d'une panne (lorsque les Cloud Connector d'une zone ne peuvent pas communiquer avec Citrix Cloud), seules les ressources associées aux machines enregistrées dans cette zone sont disponibles.

Préférence de zone

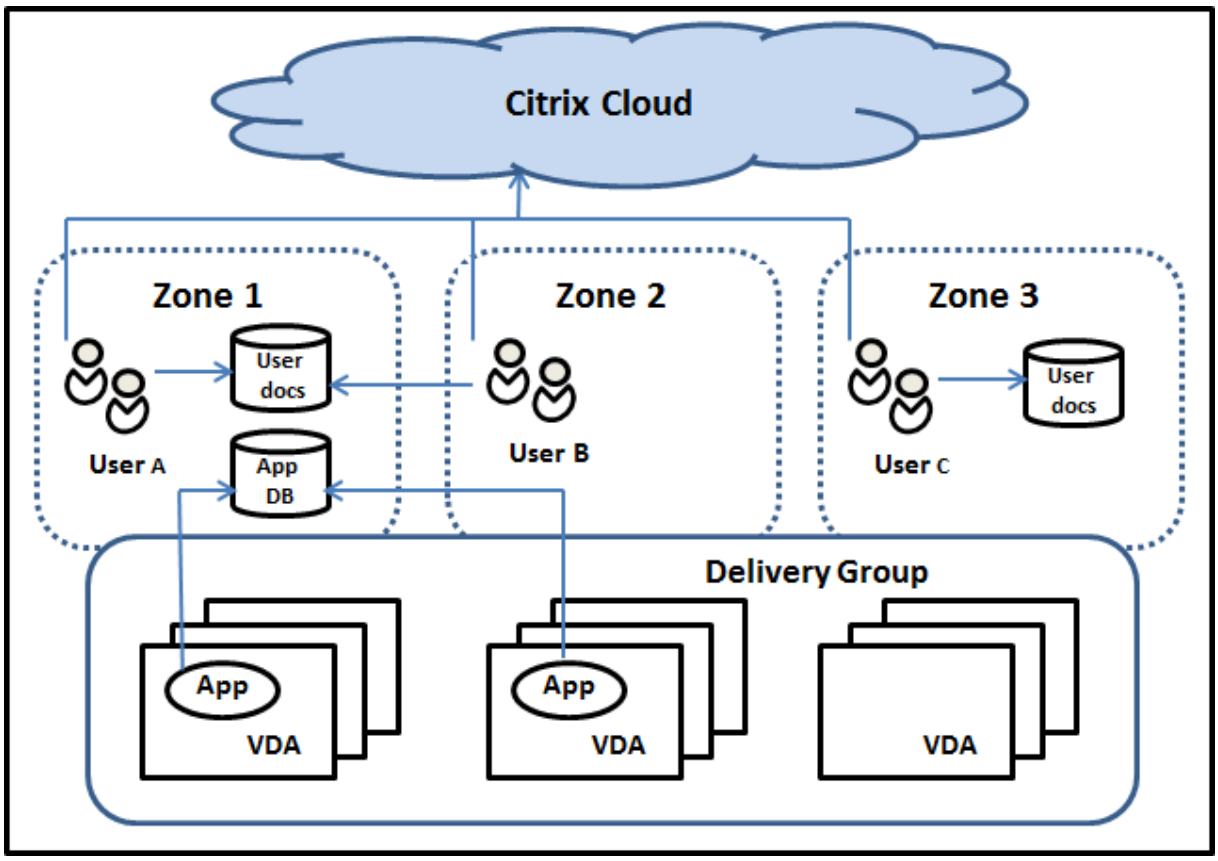
Dans un site multi-zone, la fonctionnalité de préférence de zone permet à l'administrateur de mieux contrôler les VDA utilisés pour lancer une application ou un bureau.

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. L'emplacement de l'utilisateur requiert StoreFront 3.7 et Citrix Gateway (anciennement NetScaler Gateway) 11.0-65.x au minimum.

Le graphique suivant illustre un exemple de configuration multi-zone.



Dans cet exemple, les VDA sont répartis entre trois zones, mais ils sont tous dans le même groupe de mise à disposition. Par conséquent, le broker Citrix DaaS peut choisir le VDA à utiliser pour une demande de lancement d'un utilisateur. Cet exemple montre que les utilisateurs peuvent exécuter leurs points de terminaison d'application Citrix Workspace à différents emplacements. L'utilisateur A utilise un périphérique avec l'application Citrix Workspace dans la zone 1. L'utilisateur B utilise un périphérique dans la zone 2. De même, les documents d'un utilisateur peuvent être stockés dans différents endroits. Les utilisateurs A et B utilisent un partage situé dans la zone 1. L'utilisateur C utilise un partage dans la zone 3. De plus, l'une des applications publiées utilise une base de données qui se trouve dans la zone 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 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. 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. 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 (ou n'est pas) utilisée.

- **Utilisation obligatoire de la zone d'accueil utilisateur :** dans un groupe de mise à disposition, vous pouvez spécifier « Lancer la session dans la zone d'accueil de l'utilisateur (si l'utilisateur dispose d'une zone d'accueil), sans basculement vers une autre zone si aucune ressource n'est disponible dans la zone d'accueil. » 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 « Lancer l'application uniquement dans cette zone, sans basculement vers une autre zone si aucune ressource n'est disponible 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 spécifier « Ne considérer aucune des zones utilisateur lors du lancement de cette application. » Par exemple, utilisez l'emplacement de l'utilisateur comme préférence de zone si vous voulez que les utilisateurs exécutent une application spécifique sur un VDA proche de leur machine, 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. Cette action 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 non préférée.
3. Démarrer une nouvelle session dans la zone préférée.
4. Se reconnecter à une session connectée existante dans une zone non préférée.
5. Démarrer une nouvelle session dans une zone non 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 doit être configuré pour associer des plages d'adresses IP à des zones particulières. L'identité de zone détectée doit être transmise via StoreFront à Citrix DaaS.

Bien que rédigé pour l'utilisation sur site des zones, le post de blog Zone Preference Internals contient des détails techniques pertinents.

Autorisations pour gérer les zones

Un administrateur complet peut effectuer toutes les tâches de gestion de zone prises en charge. 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 de machines d'une zone vers une autre, vous devez disposer d'une autorisation de modification pour ce catalogue.

Si vous utilisez Citrix Provisioning : étant donné que la console Citrix Provisioning ne peut pas identifier les zones, Citrix vous recommande d'utiliser l'interface **Gérer > Configuration complète** pour créer les catalogues de machines que vous souhaitez placer dans des zones spécifiques. Après avoir créé le catalogue, vous pouvez utiliser la console Citrix Provisioning pour provisionner des machines dans ce catalogue.

Création de zone

Lorsque vous créez un emplacement de ressources dans Citrix Cloud et que vous y ajoutez un Cloud Connector, Citrix DaaS crée et nomme automatiquement une zone. Vous pouvez éventuellement ajouter une description plus tard.

Une fois que vous avez créé plus d'un emplacement de ressources (et que des zones sont créées automatiquement), vous pouvez déplacer des ressources d'une zone à une autre.

Les zones et emplacements de ressources sont synchronisés périodiquement, généralement et environ toutes les cinq minutes. Par conséquent, si vous modifiez le nom d'un emplacement de ressources dans Citrix Cloud, cette modification est propagée à la zone associée dans les cinq minutes.

Ajouter ou modifier la description d'une zone

Bien que vous ne puissiez pas modifier le nom d'une zone, vous pouvez ajouter une description ou la modifier.

1. Dans **Gérer > Configuration complète**, sélectionnez **Zones** dans le volet gauche.
2. Sélectionnez une zone dans le volet central, puis sélectionnez **Modifier la zone** dans la barre d'actions.
3. Ajoutez une description ou modifiez la description de la zone.

4. Sélectionnez **OK** ou **Appliquer**.

Déplacer des ressources d'une zone à une autre

1. Dans **Gérer > Configuration complète**, sélectionnez **Zones** dans le volet gauche.
2. Sélectionnez une zone dans le volet central, puis sélectionnez un ou plusieurs éléments.
3. 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. (Bien que vous puissiez sélectionner des Cloud Connector, vous ne pouvez pas les déplacer vers une autre zone.)

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 de machines utilise une connexion hôte vers un hyperviseur ou un service de cloud, le catalogue et la connexion doivent se trouver dans la même zone. Sinon, les performances peuvent être affectées. Si vous déplacez un élément, déplacez l'autre.

Suppression de zone

Vous ne pouvez pas supprimer une zone. Toutefois, vous pouvez supprimer un emplacement de ressources (après suppression de ses Cloud Connector). La suppression de l'emplacement de ressources supprime automatiquement la zone.

- Si la zone ne contient pas d'éléments (tels que des catalogues, connexions, applications ou utilisateurs), elle est supprimée lors de la prochaine synchronisation entre les zones et les emplacements de ressources. La synchronisation se produit toutes les cinq minutes.
- Si la zone contient des éléments, elle est automatiquement supprimée après suppression de tous les éléments.

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. Dans **Gérer > Configuration complète**, sélectionnez **Zones** dans le volet gauche.
2. Sélectionnez une zone dans le volet central, puis sélectionnez **Ajouter des utilisateurs à la zone** dans la barre d'actions.
3. Dans la boîte de dialogue **Ajouter des utilisateurs à la zone**, sélectionnez **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.

4. Sélectionnez **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. Dans **Gérer > Configuration complète**, sélectionnez **Zones** dans le volet gauche.
2. Sélectionnez une zone dans le volet central, puis sélectionnez **Supprimer des utilisateurs de la zone** dans la barre d'actions.
3. Dans la boîte de dialogue **Supprimer des utilisateurs de la zone**, sélectionnez **Supprimer**, puis sélectionnez les utilisateurs et les groupes d'utilisateurs à supprimer de la zone. Cette action supprime uniquement les utilisateurs de la zone. Ces utilisateurs restent dans les groupes de mise à disposition auxquels ils appartiennent.
4. 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 ou de 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 **Zones** dans le volet gauche. Sélectionnez une application, puis sélectionnez **Propriétés** 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

Si vous disposez de plusieurs zones, vous pouvez spécifier une zone lorsque vous ajoutez une connexion hôte ou que vous créez un catalogue. Les zones sont répertoriées par ordre alphabétique dans les listes de sélection. Par défaut, le premier nom par ordre alphabétique est sélectionné.

Dépannage

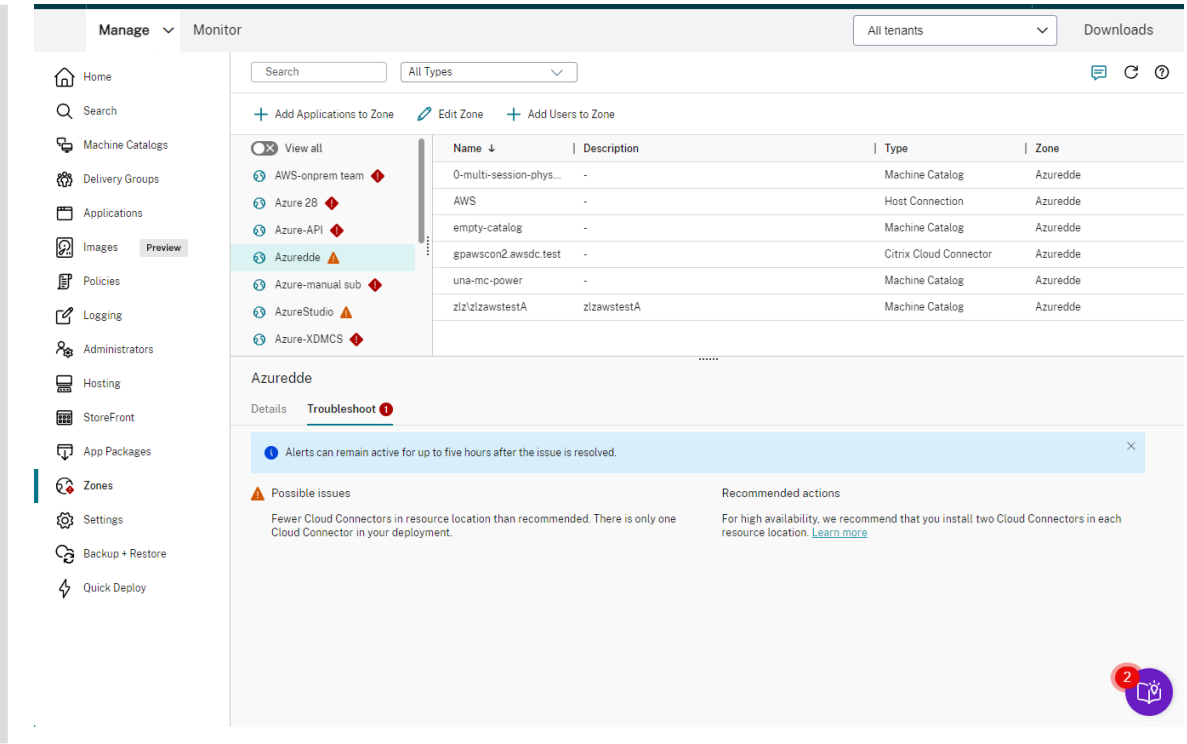
La configuration complète vous envoie des alertes proactives pour vous assurer que votre cache d'hôte local et vos zones sont correctement configurés afin que vous puissiez résoudre les problèmes à temps avant qu'une panne n'affecte vos utilisateurs. Cette fonctionnalité permet de maintenir l'accès continu des utilisateurs aux charges de travail critiques.

Un onglet **Dépannage** apparaît pour chaque zone présentant des problèmes.

Pour vérifier les problèmes liés à une zone, procédez comme suit :

1. Accédez à **Configuration complète > Zones** et cliquez sur la zone avec l'icône d'avertissement.
2. Accédez à l'onglet **Dépannage** dans le volet inférieur et lisez les informations qui s'y trouvent.

> **Remarque :**
>
> Les diagnostics sont mis à jour toutes les heures.
>
> Exemple d'informations de dépannage :



Le tableau suivant fournit une liste complète des avertissements et des erreurs liés aux zones :

Gravité	Problèmes possibles	Actions recommandées
Avertissement	L'emplacement des ressources contient plusieurs domaines. Lorsque plusieurs domaines se trouvent dans un même emplacement de ressources, si les relations d'approbation ne sont pas correctement configurées, l'enregistrement des VDA peut prendre plus de temps. En outre, les VDA peuvent ne pas s'enregistrer en mode haute disponibilité.	Assurez-vous que les relations de confiance entre les domaines de cet emplacement de ressources sont correctement configurées. Consultez Détails techniques sur Citrix Cloud Connector.

Gravité	Problèmes possibles	Actions recommandées
Avertissement	Il y a plus de connexions hôte dans l'emplacement de ressources que ce qui est recommandé. Le dépassement de la limite peut entraîner une dégradation des performances, ce qui affecte l'expérience utilisateur.	Réduisez le nombre de connexions hôtes dans cet emplacement de ressources pour ne pas dépasser la limite recommandée. Voir Limites.
Avertissement	Il y a moins d'unités centrales logiques que ce qui est recommandé. En mode haute disponibilité, cela peut entraîner une dégradation des performances.	Assurez-vous que chaque Cloud Connector répond aux exigences minimales en matière de processeur logique. Consultez la section Cache d'hôte local.
Avertissement	Il y a moins de Cloud Connector dans l'emplacement de ressources que ce qui est recommandé. Il n'y a qu'un seul Cloud Connector dans votre déploiement.	Nous recommandons d'installer deux composants Cloud Connector dans chaque emplacement de ressources pour garantir une haute disponibilité. Consultez Détails techniques sur Citrix Cloud Connector.
Avertissement	RAM inférieure à la quantité recommandée sur au moins une machine Cloud Connector. En mode haute disponibilité, cela peut entraîner une dégradation des performances.	Assurez-vous que chaque machine Cloud Connector répond aux exigences minimales en matière de RAM. Consultez Considérations sur le dimensionnement et la capacité à monter en charge des machines Cloud Connector.

Gravité	Problèmes possibles	Actions recommandées
Erreur	Il y a plus de VDA dans l'emplacement de ressources que ce qui est recommandé. En mode haute disponibilité, le cache d'hôte local n'autorise l'enregistrement que de 10 000 VDA. Les tentatives d'enregistrement effectuées par d'autres VDA échoueront	Réduisez le nombre de VDA dans cet emplacement de ressources pour ne pas dépasser la limite recommandée. Voir Limites.
Erreur	Les Cloud Connector de la zone sont inaccessibles. Aucun des Cloud Connector de la zone n'est accessible. Les VDA situés dans cet emplacement de ressources peuvent ne pas être disponibles à moins que le cache d'hôte local ou la continuité de service ne soient configurés pour votre déploiement.	Vérifiez la connectivité des Cloud Connector de la zone et consultez le registre pour vérifier si le mode LHC est forcé via le registre. Si le registre ne force pas le mode LHC, envisagez d'exécuter l'utilitaire de vérification de la connectivité Cloud Connector. Si le problème persiste, ouvrez un ticket d'assistance.

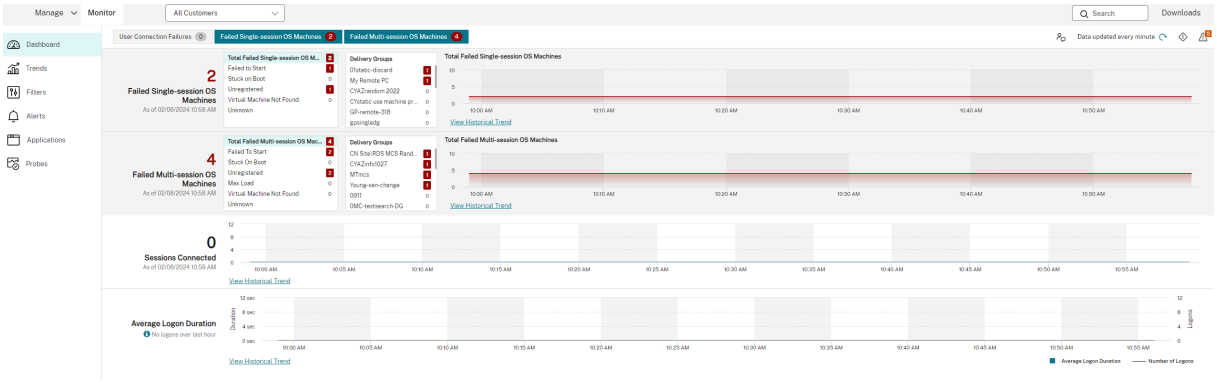
Surveiller

February 21, 2024

Les administrateurs et le support technique peuvent surveiller Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) à partir de l'onglet **Surveiller**, la console de surveillance et de dépannage. L'onglet **Surveiller** affiche un tableau de bord permettant de surveiller, de résoudre les problèmes et d'effectuer des tâches de support pour les abonnés.

> **Remarque :**
>
> La console Monitor est disponible en tant que console Director pour surveiller et résoudre les problèmes liés aux déploiements Current Release et LTSR de Citrix Virtual Apps and Desktops.

Pour accéder à **Surveiller**, connectez-vous à Citrix Cloud. Dans le menu supérieur gauche, sélectionnez **Mes services > DaaS**. Cliquez sur **Surveiller**.



> **Remarque :**
>
> La résolution d'écran optimale recommandée pour afficher Citrix Monitor est 1440 x 1024.

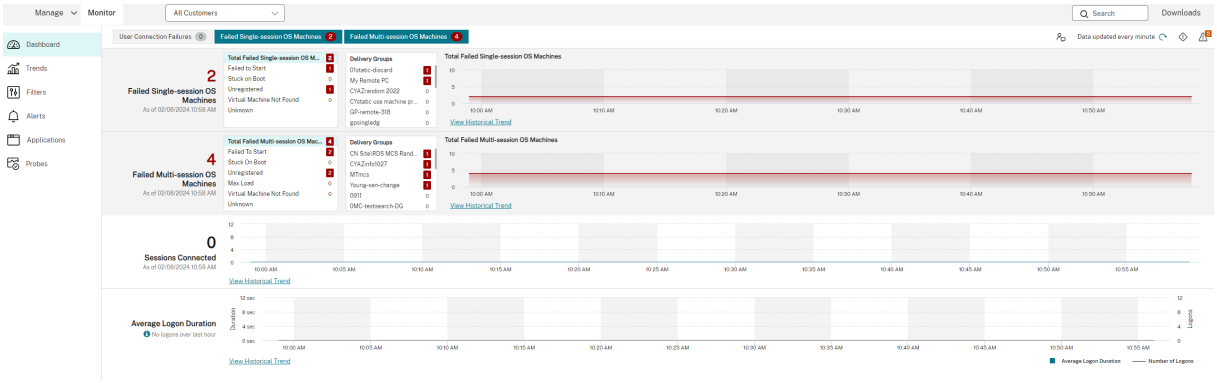
Les avantages du service de surveillance sont les suivants :

- Accès aux données en temps réel à partir de l'agent Broker à l'aide d'une console unifiée, intégrée à Analytics et Performance Manager.
- Analytics est une solution de gestion des performances permettant d'assurer l'intégrité et la capacité à monter en charge qui offre des tendances historiques pour identifier les goulots d'étranglement dans votre environnement Citrix DaaS.
- Accès aux données d'historiques stockées dans la base de données Monitor pour accéder à la base de données de journalisation de la configuration.
- Visibilité accrue au niveau de l'expérience des utilisateurs pour les applications et les bureaux virtuels, et les utilisateurs pour Citrix DaaS.
- Le service de surveillance utilise un tableau de bord de résolution des problèmes qui offre un contrôle d'intégrité en temps réel et historique de Citrix DaaS. 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.

Analyse de site

March 30, 2024

Le tableau de bord de l'onglet Surveiller 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.

Panneau	Description
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 le tableau adjacent, ce numéro est ensuite classé en fonction de chaque 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 survenus au cours des 60 dernières minutes, classés en fonction de chaque groupe 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.
Session(s) connectée(s)	Sessions connectées sur tous les groupes de mise à disposition pour les dernières 60 minutes.

Panneau	Description
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.

> **Remarque :**
>
> Lorsque le type d'hôte que vous utilisez ne prend pas en charge une mesure particulière, aucune icône n'apparaît pour celle-ci. 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 précédentes) :

- Contrôler l'alimentation de la machine utilisateur
- Empêcher les connexions aux machines

Contrôler des sessions

Si une session est déconnectée, elle est toujours active et ses applications continuent de fonctionner. Cependant, la machine utilisateur 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. Consultez également la liste de toutes les machines et 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.

Action	Description
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. Cliquez ensuite sur le grand nombre total pour ouvrir la vue Filtres. Vous pouvez afficher les données de session graphiques basées sur les groupes de mise à disposition sélectionnés et sur les plages et l'utilisation 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. Vous pouvez filtrer 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.
Afficher les données sur une période plus longue	Dans la vue **Tendances**, sélectionnez l'onglet **Sessions** pour accéder à des données d'utilisation plus spécifiques. Vous pouvez analyser les données des sessions connectées et déconnectées sur une période plus longue. Vous pouvez consulter le nombre total de sessions antérieures aux 60 dernières minutes. Pour afficher ces informations, cliquez sur **Afficher les tendances historiques**.

> **Remarque :**
>
> Supposons qu'une machine utilisateur s'exécute sur un VDA (Virtual Delivery Agent) d'ancienne génération, tel qu'un VDA antérieur à la version 7 ou un Linux VDA. Dans ce cas, Monitor 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 :

la console Gérer 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, l'onglet Surveiller 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 l'onglet Monitor.

Vous pouvez mapper le bureau attribué qui est affiché dans StoreFront au nom du groupe de mise à disposition affiché dans Monitor. Pour le mappage, 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-->
```

Exécutez la commande PowerShell précédente à l'aide du SDK Remote PowerShell, comme décrit dans ce blog.

Désactiver la visibilité des applications en cours d'exécution dans le Gestionnaire d'activités

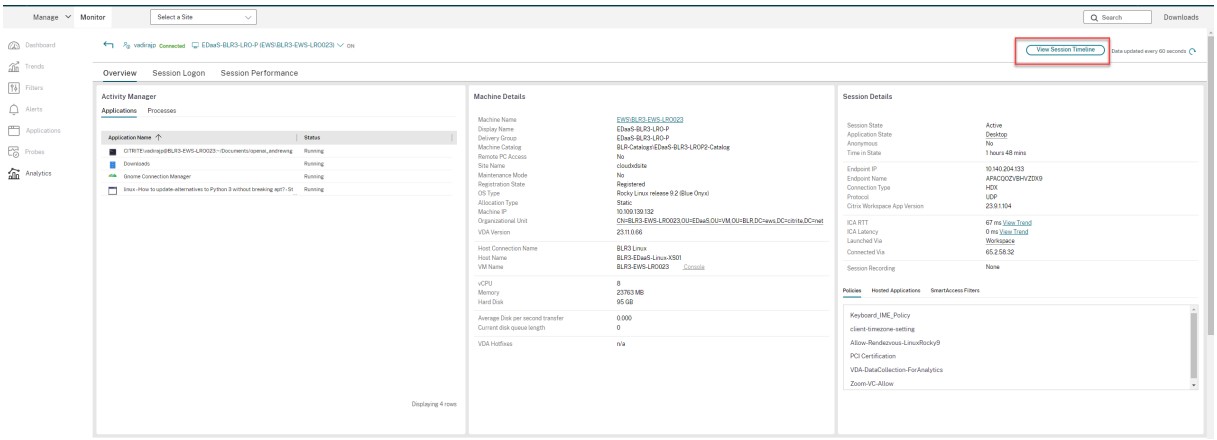
Par défaut, le Gestionnaire d'activités affiche une liste de toutes les applications en cours d'exécution pour la session d'un utilisateur. Tous les administrateurs disposant d'un accès à la fonctionnalité Gestionnaire d'activités peuvent consulter ces informations. Pour les rôles d'administrateur délégué, cela comprend l'administrateur complet, l'administrateur de groupe de mise à disposition et l'administrateur d'assistance.

Pour protéger la confidentialité des utilisateurs et les applications qu'ils exécutent, vous pouvez désactiver l'onglet **Applications** afin de ne plus répertorier les applications en cours d'exécution. Pour cela, sur le VDA, modifiez la clé de registre dans HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerData
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.

> **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.

Accès à Citrix Analytics for Performance - Détails de la session

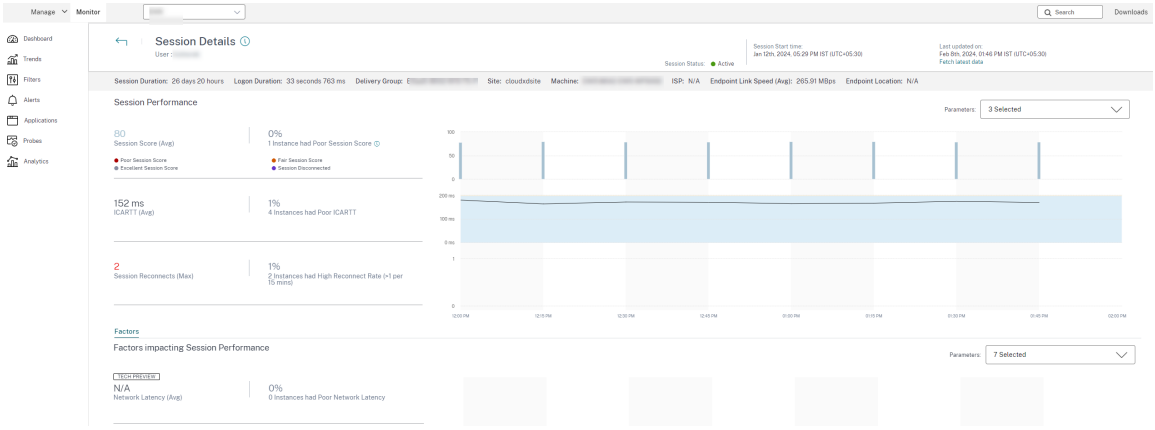
La page Détails de la session de Citrix Analytics for Performance est accessible dans Moniteur. Cliquez sur **Afficher chronologie de la session** dans la section **Détails de la session** du Gestionnaire d'activités pour ouvrir la page Détails de la session de Citrix Analytics for Performance dans Monitor.



Remarque :

Cette fonctionnalité nécessite que vous disposiez d'un droit Citrix Analytics for Performance valide.

Les détails des sessions sont disponibles pour les sessions classées dans la catégorie Excellente, Acceptable ou Médiocre de Citrix Analytics for Performance. Pour plus d'informations sur les raisons pour lesquelles une session peut ne pas être classée, consultez l'article Non classé.

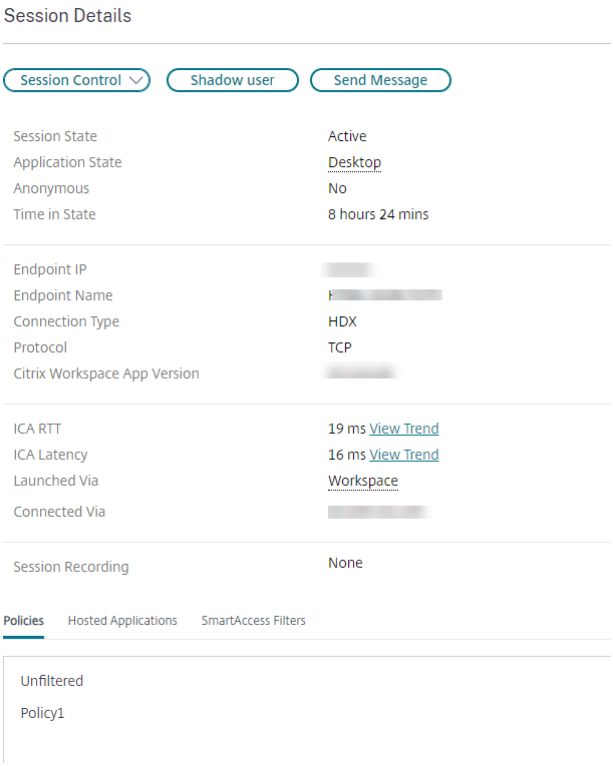


Vous pouvez voir une tendance pour l'expérience de session au cours des trois derniers jours au maximum. Cette vue des tendances inclut également les facteurs qui contribuent à l'expérience de session. Ces informations complètent les données en temps réel disponibles dans Moniteur, utilisées par l'administrateur du service d'assistance lors de la résolution des problèmes liés à l'expérience de session.

Pour plus d'informations sur la page Détails de la session, voir Détails de la session.

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.



Utilisez le menu déroulant **Contrôle de session** dans le volet **Détails de la session** pour fermer ou déconnecter une session.

- 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 incluent les tendances représentées sous la forme de graphiques et de tableaux. Les rapports au format CSV contiennent des données tabulaires que vous pouvez utiliser pour générer des vues ou utiliser à des fins d'archives.

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.

Le moniteur 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 associé au service de surveillance, 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.

Format de rapport	Nombre d'enregistrements pris en charge par défaut
PDF	500
Excel	100 000
CSV	100 000 (10 000 000 dans l'onglet **Sessions**)

Gestion des erreurs

Erreurs que vous pouvez rencontrer lors d'une opération d'exportation :

- **La session 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 Monitor Service.
- **La session de surveillance a expiré :** cette erreur peut se produire en raison de problèmes de réseau ou d'utilisation élevée des ressources par Monitor Service ou sur le serveur SQL Server.
- **Opérations d'exportation ou d'aperçu max. simultanées en cours :** une seule instance d'exportation ou d'aperçu peut être exécutée à un moment donné. Si vous recevez une erreur concernant les **opérations d'exportation ou d'aperçu simultanées maximales**, attendez avant d'effectuer la prochaine opération.

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 l'onglet Surveiller, 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 ou les machines 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 l'onglet Surveiller avec l'état « Échec du démarrage » et utilisez cette commande pour les redémarrer.

Commande	Fonction
Forcer le redémarrage	Redémarre la machine virtuelle sans d'abord effectuer de procédure d'arrêt. 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 d'abord effectuer une procédure d'arrêt. 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 de maintenance prend effet dès que les sessions de tous les utilisateurs sont fermées. Pour les utilisateurs dont les sessions ne sont pas fermées, envoyez un message les informant que les machines sont arrêtées à un moment donné. Vous pouvez utiliser les commandes d'alimentation pour forcer l'arrêt 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 de 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 mesures telles que les suivantes :

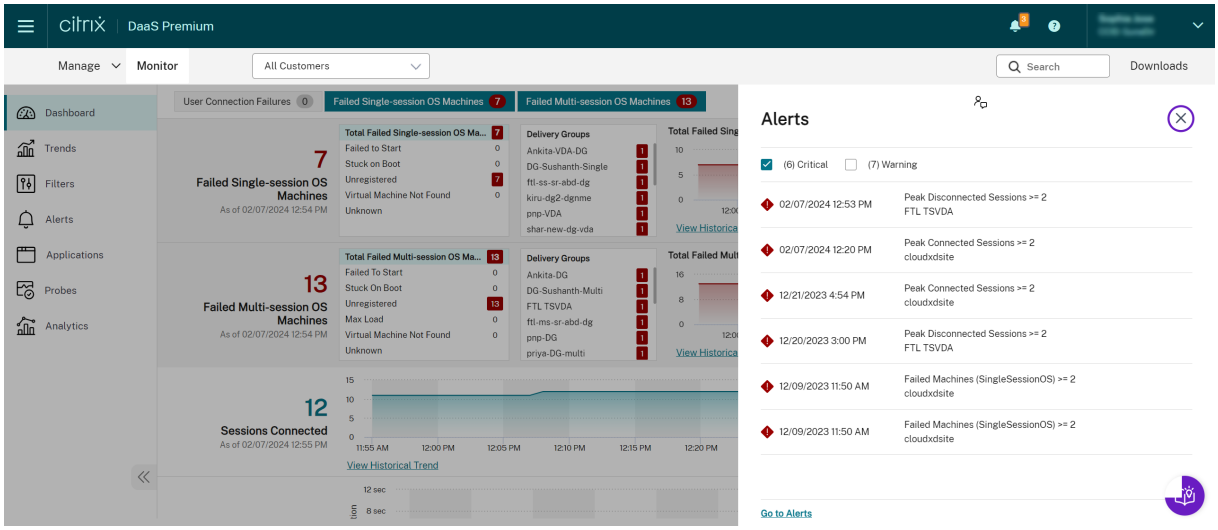
- Résultats de l'analyse
- Nombre d'instances par application
- Pannes et erreurs associées aux applications publiées

Pour obtenir davantage d'informations, veuillez consulter la section Analyses des applications sous **Résolution des problèmes d'applications**.

Alertes et notifications

February 21, 2024

Les alertes sont affichées sur l'onglet Surveiller sur le tableau de bord et dans d'autres vues de haut niveau avec des symboles d'avertissement et d'alerte critique. Les alertes sont mises à jour automatiquement toutes les minutes ; vous pouvez également mettre à jour les alertes à la demande.

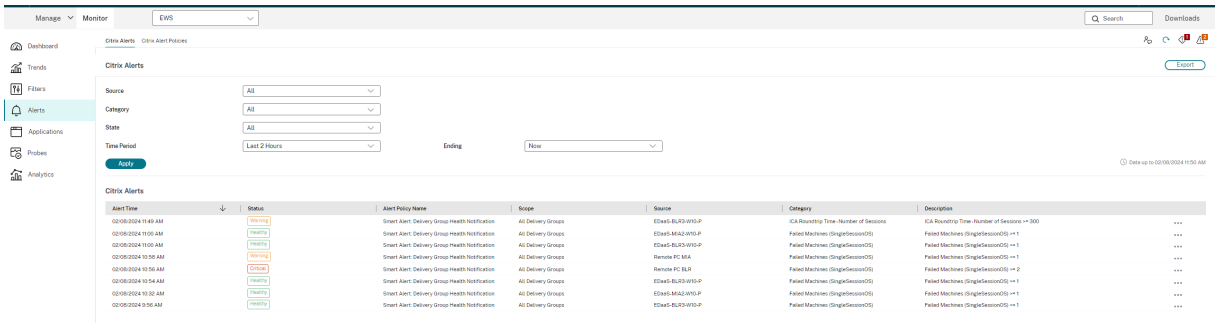


Une alerte d'avertissement (triangle de couleur ambre) indique que le seuil d'avertissement d'une condition a été atteint ou dépassé.

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** en bas de la barre latérale ou en sélectionnant **Alertes** en haut de la page Surveiller.

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 proviennent de composants Citrix. Vous pouvez configurer les alertes Citrix à partir de l'onglet Surveiller 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

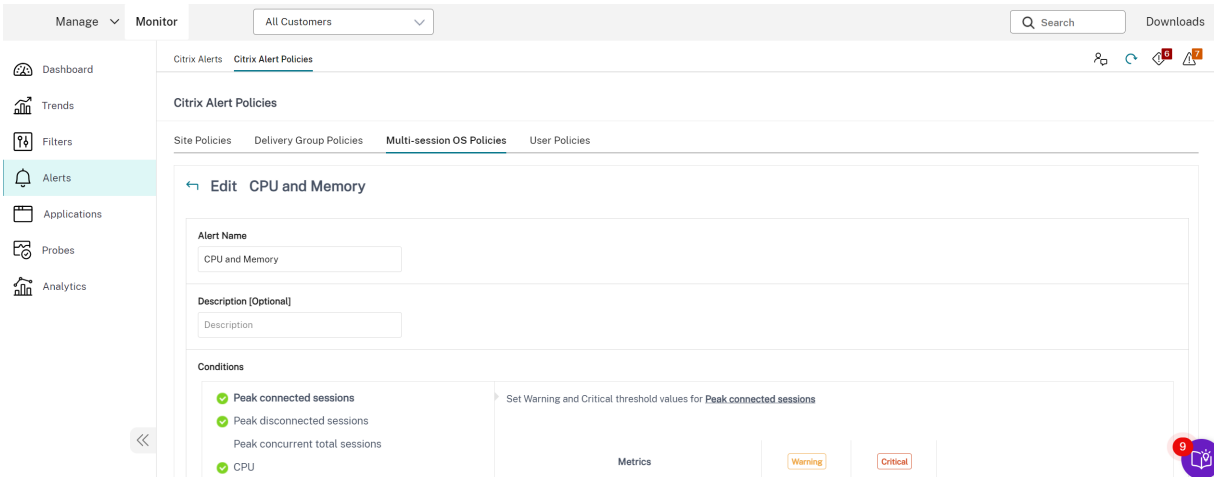
dépassent les seuils que vous avez définis. Pour de plus amples informations sur la configuration des alertes Citrix, consultez la section Créer des stratégies d'alerte.

Stratégies d'alertes intelligentes

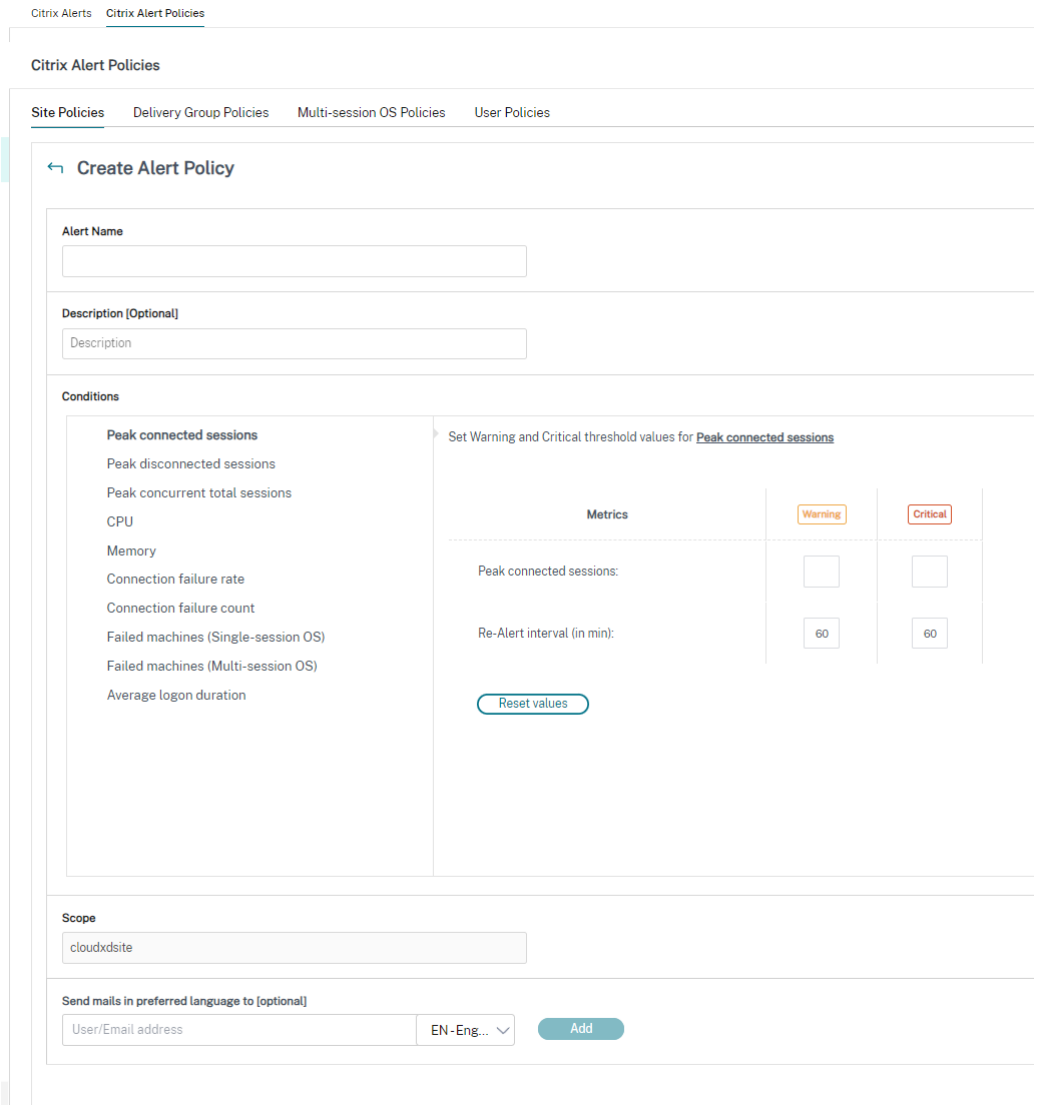
Un ensemble de stratégies d'alerte intégrées avec des valeurs de seuil prédéfinies est disponible pour les groupes de mise à disposition et les VDA avec OS multi-session. Vous pouvez modifier les paramètres de seuil des stratégies d'alerte intégrées dans **Alertes** > **Stratégie d'alerte Citrix**.
Ces 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.

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 nouvelle 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. Les notifications par courrier électronique sont envoyées via SendGrid. Assurez-vous que l'adresse e-mail `donotreplynotifications@citrix.com` est ajoutée à la liste blanche dans votre configuration de messagerie.
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 l'onglet Surveiller 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 l'onglet Surveiller 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 l'onglet Surveiller 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 l'onglet Surveiller 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 l'onglet Surveiller 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 l'onglet Surveiller 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, contacter 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, contacter 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 l'onglet Surveiller.

- Exécuter les diagnostics Citrix Scout pour déterminer la cause. Pour de plus amples informations, consultez la section Résoudre les problèmes utilisateur.

  Conditions de la stratégie intelligente :

  - **Portée :** Groupe de mise à disposition
  - **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 l'onglet Surveiller.

- 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 l'onglet Surveiller 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 de plus amples informations, consultez la section Diagnostiquer les problèmes de connexion 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 l'onglet Surveiller 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

L'onglet Surveiller affiche des alertes pour surveiller l'état de l'hyperviseur. Les alertes provenant de Citrix Hypervisor 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.

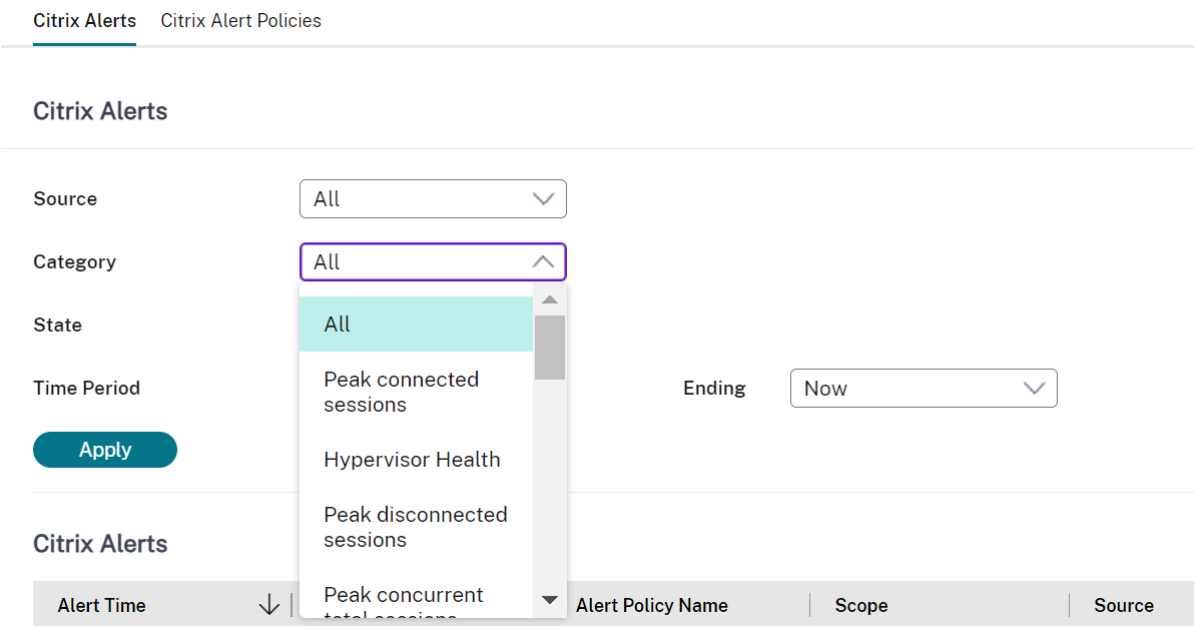
Pour recevoir des alertes d'hyperviseur, assurez-vous qu'une connexion d'hébergement a été créée dans l'onglet Gérer. Pour de plus amples informations, consultez les articles Connexions et ressources. Seules ces connexions sont surveillées pour les alertes d'hyperviseur. Le tableau suivant décrit les différents paramètres et états des alertes d'hyperviseur.

Alerte	Hyperviseurs pris en charge	Déclenchée par	Condition	Configuration
Utilisation du processeur	Citrix Hypervisor, VMware vSphere	Hyperviseur	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	Citrix Hypervisor, VMware vSphere	Hyperviseur	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	Citrix Hypervisor, VMware vSphere	Hyperviseur	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	Hyperviseur	Le seuil d'alerte d'utilisation du disque est atteint ou dépassé	Les seuils d'alerte doivent être configurés dans l'hyperviseur.
État de l'alimentation ou de la connexion de l'hôte	VMware vSphere	Hyperviseur	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	Citrix Hypervisor, 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 l'onglet Surveiller. Toutefois, vous pouvez modifier les préférences de courrier électronique et ignorer une alerte dans l'onglet Surveiller.

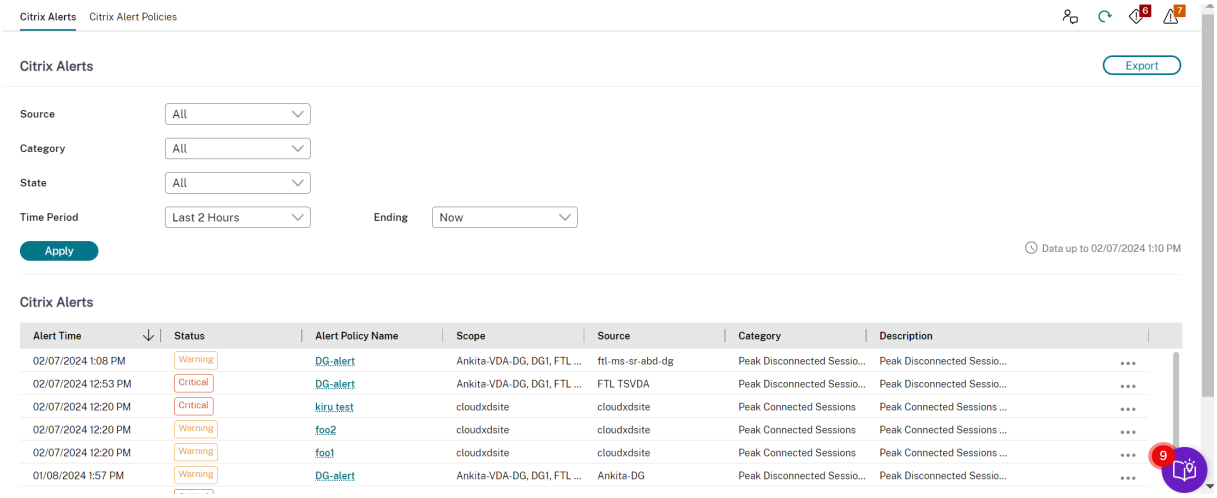
> **Important :**
>
> - Toutes les alertes d'hyperviseur de plus d'un jour sont automatiquement rejetées.
> - Les alertes déclenchées par l'hyperviseur sont récupérées et affichées dans l'onglet Surveiller. Toutefois, les changements apportés dans le cycle de vie/l'état des alertes de l'hyperviseur ne sont pas reflétés dans l'onglet Surveiller.
> - Les alertes qui sont intègres, rejetées ou désactivées dans la console de l'hyperviseur continueront à apparaître dans l'onglet Surveiller et doivent être rejetées explicitement.
> - Les alertes rejetées dans l'onglet Surveiller ne sont pas rejetées automatiquement dans la console de l'hyperviseur.



Une nouvelle catégorie d'alerte appelée **Intégrité de l'hyperviseur** a été ajoutée pour permettre de filtrer uniquement 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

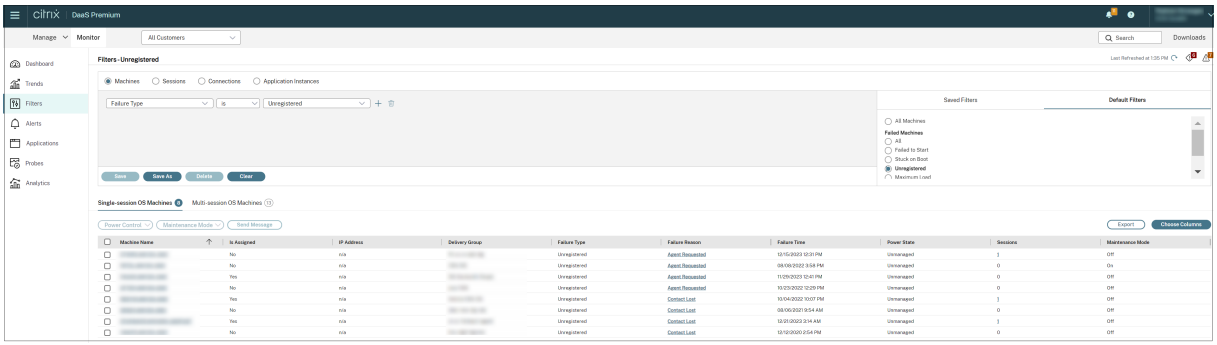


Filtrer les données pour résoudre les échecs

August 18, 2023

Lorsque vous cliquez sur des nombres sur le tableau de bord ou que vous sélectionnez un filtre par défaut prédéfini depuis l'onglet **Filtres**, la vue Filtres s'ouvre pour afficher les données basées sur la machine sélectionnée ou le type d'échec.

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 et enregistrer la recherche pour y accéder plus tard. Vous pouvez modifier un filtre prédéfini et l'enregistrer en tant que filtre enregistré.



1. Sélectionner une vue :

- **Machines**. Sélectionnez Machines avec OS à session unique 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 multi-session 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.

2. Sélectionnez un filtre dans la liste des filtres enregistrés ou par défaut.
3. Utilisez les listes déroulantes pour sélectionner d'autres critères de 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 ouvrir le filtre ultérieurement, dans la vue Filtres, sélectionnez Afficher (machines, sessions, connexions ou instances d'application) et sélectionnez le filtre enregistré.
7. Cliquez sur **Exporter** pour exporter les données vers des fichiers au format CSV. Des données pouvant atteindre 100 000 enregistrements peuvent être exportées.
8. 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.
9. 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 dans le Citrix Director Failure Reasons Troubleshooting Guide.
10. 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.

11. 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 les VDA sont à la version 7.13 ou ultérieure.

> **Remarque :**
>
> La console Gérer 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, l'onglet Surveiller 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 l'onglet Surveiller. Pour mapper le bureau attribué affiché dans StoreFront au nom du groupe de mise à disposition affiché dans l'onglet Surveiller, utilisez la commande PowerShell suivante : Exécutez la commande PowerShell à l'aide du SDK Remote PowerShell, comme décrit dans ce blog.

```
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

January 25, 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

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 par les tendances affichées.

Pour modifier l'étendue par défaut de chaque graphique, appliquez un filtre différent aux données.

> **Remarque :**
>
> - 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 termine 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, mais pas de tableaux.
> - Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) conserve les données historiques pendant 90 jours uniquement. Par conséquent, les tendances et les rapports d'une année dans l'onglet Surveiller montrent les derniers 90 jours de données.

Tendances disponibles

Afficher les tendances des sessions : dans l'onglet Sessions, sélectionnez le groupe de mise à disposition et la période de temps 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 des clients 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 permettent d'afficher et de dépanner les connexions réseau rencontrant des interruptions, ainsi que d'analyser les réseaux offrant une expérience sans problème. 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 des VDA de version 1906 ou ultérieure.

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 Monitor 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.

> **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. L'indice de calculateur de charge est affiché sous forme de pourcentages de CPU totale, de mémoire, de disque ou de sessions et comparé avec le nombre d'utilisateurs connectés dans le dernier intervalle.

Afficher l'utilisation des applications hébergées : à partir de l'onglet Gestion de la capacité, sélectionnez l'onglet Utilisation des applications hébergées, sélectionnez le groupe de mise à disposition et la période de temps pour visualiser 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 indiquée 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 indiquée 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. La page 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. Les économies estimées réalisées en activant Autoscale dans le groupe de mise à disposition sélectionné sont également disponibles, ce pourcentage est calculé en utilisant les coûts par machine.

Les tendances d'utilisation des machines gérées par Autoscale indiquent l'utilisation réelle des machines, ce qui vous permet d'évaluer rapidement les besoins de 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 :**
>
> La grille située sous le graphique affiche les données d'utilisation de la machine basées sur le groupe de mise à disposition en temps réel. Les données incluent la disponibilité de toutes les machines indépendamment de Autoscale. Le nombre de machines affichées dans la colonne du compteur Disponible de la grille inclut les machines en mode de maintenance.

La consolidation des données de surveillance dépend de la période sélectionnée.

- Les données de surveillance pour les périodes d'un jour et d'une semaine sont consolidées par heure.
- Les données de surveillance pour la période d'un mois sont consolidées par jour.

L'état de la machine est lu au moment de la consolidation et toute modification au cours de la période écoulée n'est pas prise en compte. Pour la période de consolidation, reportez-vous à la documentation de l'API Monitor.

Pour plus d'informations sur la surveillance des machines gérées par Autoscale, consultez l'article Autoscale.

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 des VDA de **version 7.11** ou ultérieure.
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.
> - 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 échecs applicatifs : l'onglet "Échecs applicatifs"affiche les échecs associés aux applications publiées sur les VDA.

Cette fonctionnalité requiert des VDA de **version 7.15** ou ultérieure. 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.

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.

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 ODatane ne sont pas localisés, ils 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 la console Gérer sont disponibles pour sélection dans les filtres de tendances jusqu'à ce que les données y étant associées 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.

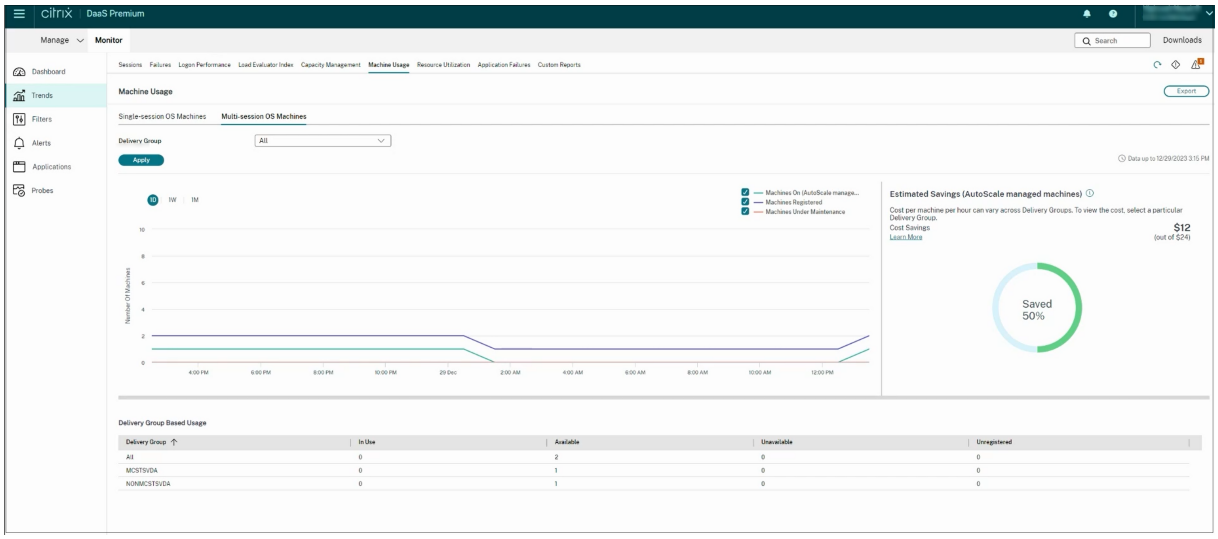
Surveiller les machines gérées par Autoscale

March 30, 2022

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 à partir de l'onglet **Gérer**. Pour plus d'informations, consultez la section Autoscale.
Vous pouvez surveiller les indicateurs clés des machines gérées par Autoscale sous l'onglet **Surveiller**.

Utilisation de machine

La page **Surveiller** > **Tendances** > **Utilisation de machine** affiche le nombre total 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.

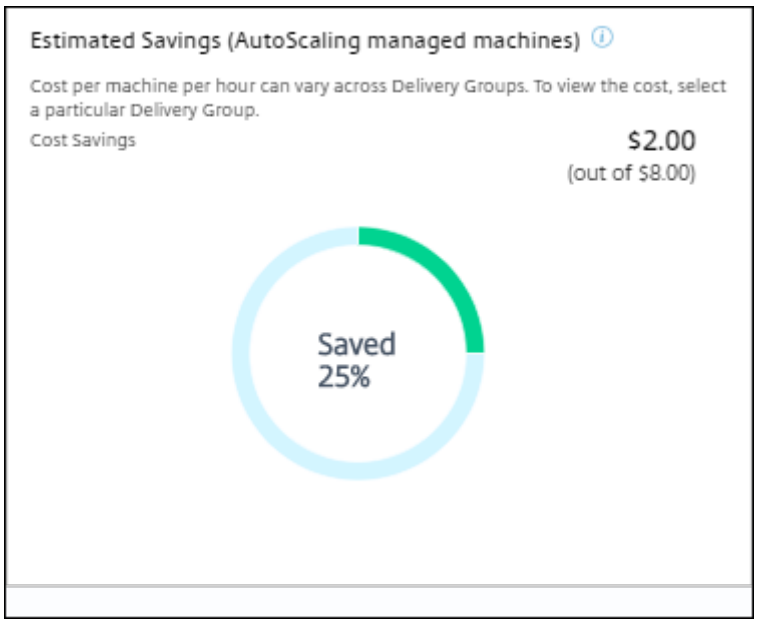


Le graphique représente les indicateurs suivants :

- **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 **Surveiller** > **Tendances** > **Utilisation de machine** 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 **Gérer** > **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 Surveiller affiche des notifications d'alerte qui peuvent être détaillées. Les détails des alertes sont affichés sur la page **Surveiller** > **Alertes**.

- Pour créer une stratégie d'alerte dans un groupe de mise à disposition, accédez à **Surveiller** > **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

- **Surveiller** > **Filtres** > **Machines** affiche l'état d'alimentation de toutes les machines dans un format tabulaire. Vous pouvez filtrer par groupe de mise à disposition spécifique.
- **Surveiller** > **Filtres** > **Sessions** affiche un filtre par nom de machine pour voir les sessions associées et leur état en temps réel.
- Dans **Surveiller** > **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

La page **Surveiller** > **Tendances** > **Index de calculateur de charge** affiche 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 de CPU totale, de mémoire, de disque ou de sessions et comparé avec le nombre d'utilisateurs connectés dans le dernier intervalle.

Dépanner les déploiements

March 30, 2024

En tant qu'administrateur d'assistance, vous pouvez rechercher l'utilisateur qui signale un problème. Vous affichez ensuite 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 suivantes sont disponibles :

- mettre fin à une demande ou à un processus qui ne répond pas
- opérations d'ombrage sur la machine de l'utilisateur
- déconnecter une session qui ne répond pas
- redémarrer la machine
- placer la machine en mode de maintenance
- réinitialiser le profil utilisateur

Résolution des problèmes d'applications

July 25, 2023

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 des VDA de version 7.15 ou ultérieure.

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**. 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, Surveiller 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

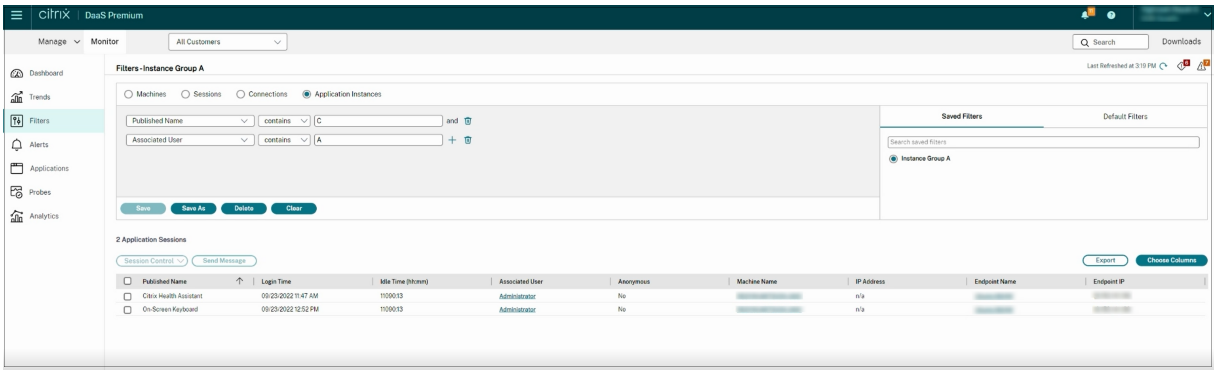
Vous pouvez résoudre les problèmes d'applications et de sessions à l'aide de la mesure de délai d'inactivité pour identifier les instances qui restent inactives au-delà d'une durée spécifique.

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 multi-session 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.

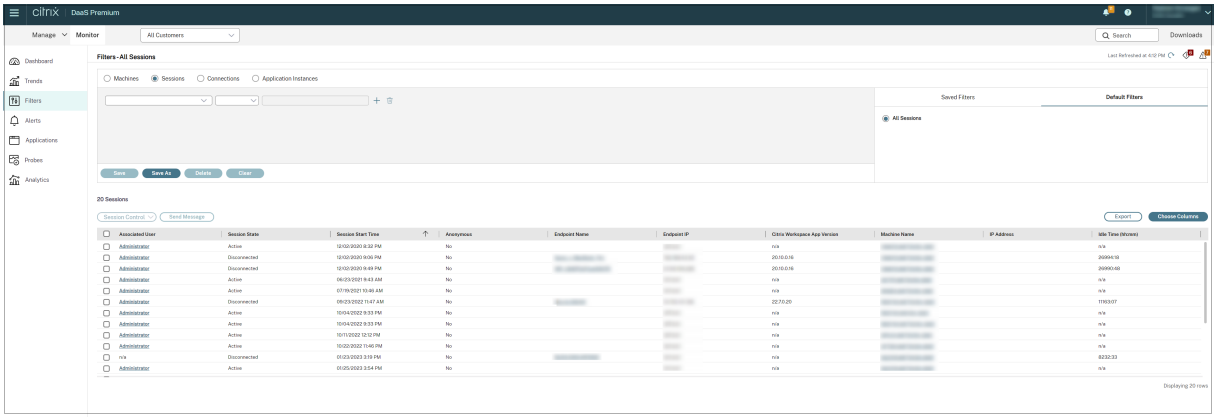
Utilisez ces informations pour identifier les instances d'application qui restent inactives au-delà d'une période de temps spécifique et mettez fin à la session ou déconnectez-les en fonction des besoins. Pour ce faire, sélectionnez **Filtres > Instances d'application** et sélectionnez un filtre pré-enregistré 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.



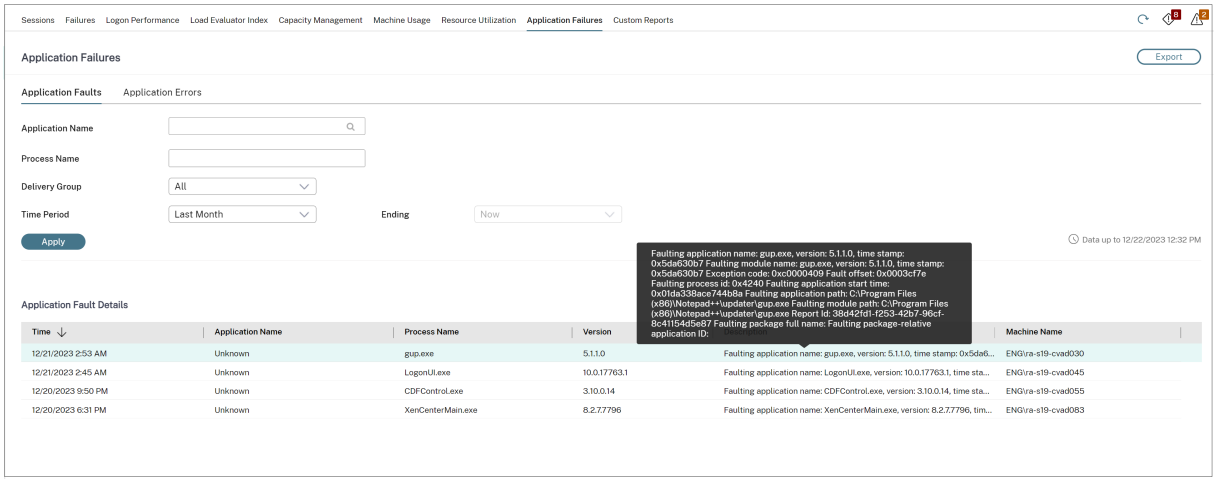
Le **délai d'inactivité** s'affiche en tant que **N/A** lorsque l'instance de la session ou de l'application

- 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.

Pour plus d'informations sur la disponibilité des tendances en matière d'échecs applicatifs, consultez Granularité de données et rétention. 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 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.

Analyse d'application

January 20, 2023

L'analyse d'application automatise les vérifications d'intégrité des applications Citrix Virtual Apps publiées sur un site. Les résultats de l'analyse d'application sont disponibles dans l'onglet **Surveiller** de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Citrix Probe Agent prend en charge les sites hébergés sur Citrix Cloud Japan et Citrix Cloud Government Planes.

Assurez-vous que les machines de point de terminaison exécutant des agents Probe Agent sont des ordinateurs Windows dotés de Citrix Receiver pour Windows version 4.8 ou ultérieure ou de l'application Citrix Workspace pour Windows (anciennement Citrix Receiver pour Windows) version 1808 ou ultérieure. L'application Workspace pour plate-forme Windows universelle (UWP) n'est pas prise en charge.

Exigences :

- Les machines de point de terminaison exécutant des agents Probe Agent sont des ordinateurs Windows dotés de Citrix Receiver pour Windows version 4.8 ou ultérieure ou de l'application Citrix Workspace pour Windows (anciennement Citrix Receiver pour Windows) version 1906 ou ultérieure. L'application Workspace pour plate-forme Windows universelle (UWP) n'est pas prise en charge.
- Citrix Probe Agent prend en charge l'authentification basée sur un formulaire par défaut, telle que prise en charge par Citrix WorkSpace. Citrix Probe Agent ne prend pas en charge d'autres méthodes d'authentification telles que l'authentification unique (SSO) ou l'authentification multifacteur (MFA). De même, Citrix Probe Agent ne fonctionne que lorsqu'aucun serveur proxy ou équilibreur de charge tel que Citrix Gateway ou Citrix ADC n'est déployé.
- Assurez-vous que Microsoft .NET Framework version 4.7.2 ou ultérieure est installé sur la machine de point de terminaison sur laquelle vous souhaitez installer Probe Agent.
- Pour utiliser l'agent dans Citrix Cloud Japan Control Plane, définissez la valeur de registre du chemin "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" sur 2. Pour utiliser l'agent dans Citrix Cloud Government Control Plane, définissez la valeur de registre du chemin "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" sur 3.

Les comptes/autorisations d'utilisateur requis pour exécuter l'analyse d'application sont les suivants :

- Un utilisateur unique de Workspace pour effectuer une analyse sur chaque machine de point de terminaison. L'utilisateur de Workspace n'est pas tenu d'être administrateur ; les analyses peuvent s'exécuter dans un contexte non administrateur.

- Comptes d'utilisateur avec des autorisations d'administrateur Windows pour installer et configurer l'agent Citrix Probe Agent sur les machines de point de terminaison
- Un compte d'utilisateur administrateur complet avec les autorisations suivantes. La réutilisation de comptes d'utilisateur existants pour l'analyse des applications risque de déconnecter les sessions actives des utilisateurs.
  - Autorisations du groupe de mise à disposition :
    - Lecture seule
  - Autorisations de Director :
    - Créer\Modifier\Supprimer les configurations d'analyse
    - Afficher la page Configurations
    - Afficher la page des tendances

Configurer l'analyse d'application

Configurez l'exécution de vos analyses d'application pendant les heures creuses sur plusieurs zones géographiques. Les résultats d'analyse complets peuvent aider à résoudre les problèmes liés aux applications, à la machine d'hébergement ou à la connexion avant que les utilisateurs ne les rencontrent.

Citrix Probe Agent version 2103 prend en charge l'agrégation de sites. Les applications et les bureaux peuvent être énumérés et lancés à partir de sites agrégés. Lorsque vous configurez Probe Agent, sélectionnez l'option **Agrégation de site Workspace (StoreFront) activée** pour activer l'énumération des applications et des bureaux à partir de sites agrégés. Les combinaisons de sites suivantes sont prises en charge :

- Plusieurs sites locaux ayant une URL StoreFront
- Sites locaux et cloud disposant d'une URL StoreFront ou Workspace
- Plusieurs sites cloud disposant d'une seule URL Workspace

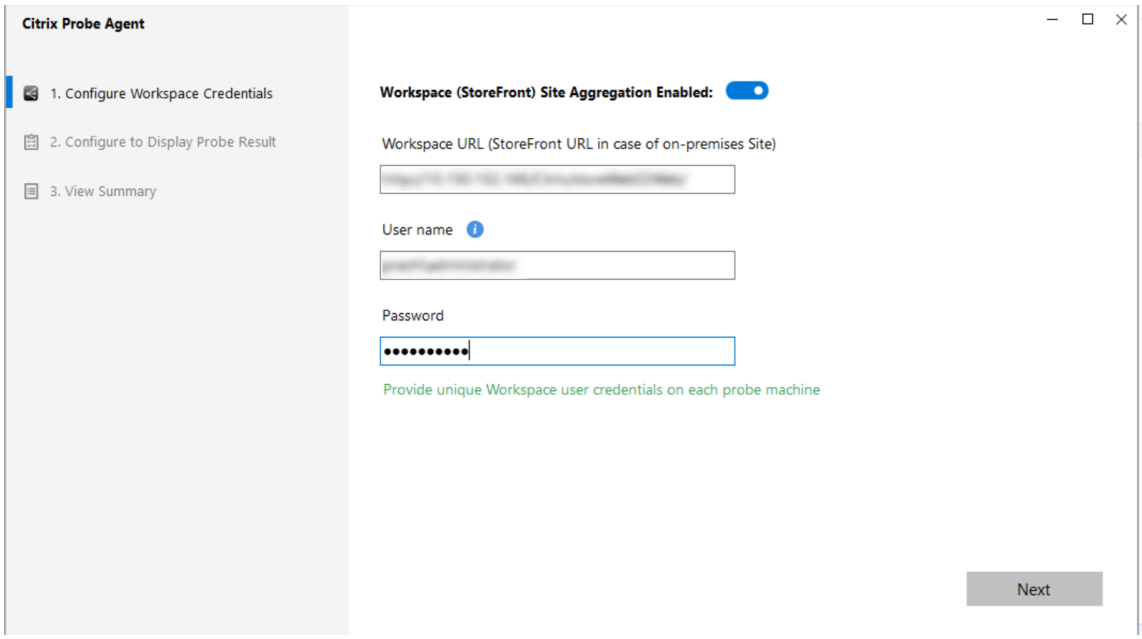
> **Remarque :**
>
> Vous devez créer des administrateurs ou des utilisateurs distincts pour configurer les outils d'analyses (Probe Agent) qui n'ont accès qu'à un seul site.

Étape 1 : Installation et configuration de Citrix Probe Agent

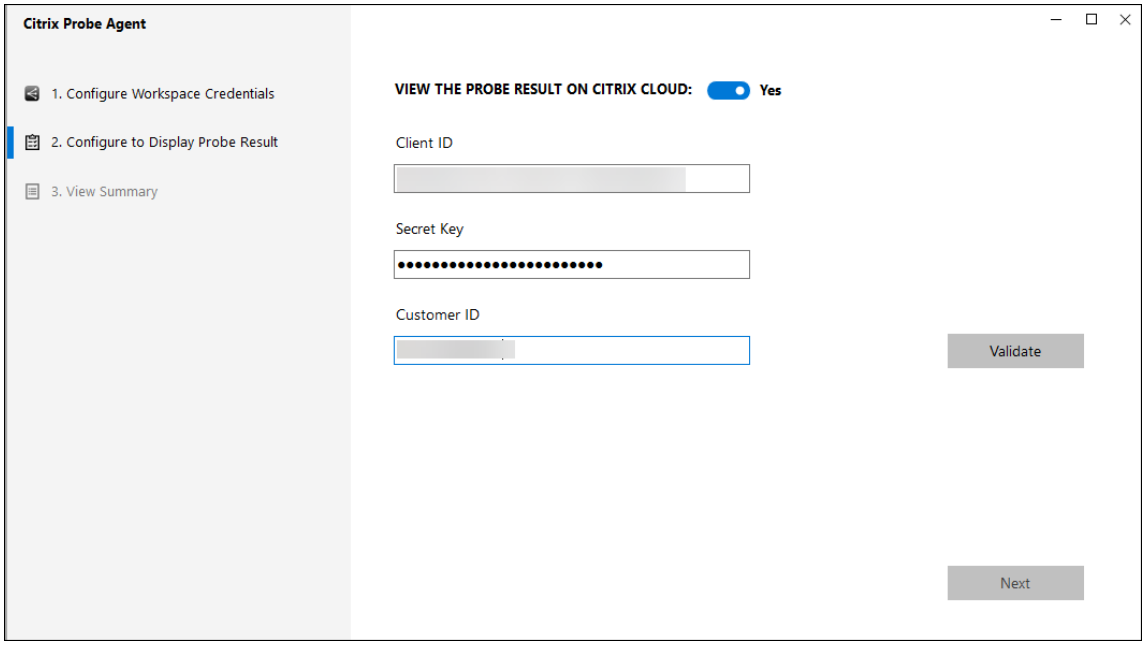
Citrix Probe Agent est un exécutable Windows qui simule le lancement de l'application par l'utilisateur via Citrix Workspace. Il teste les lancements d'applications configurés dans l'onglet Surveiller et communique les résultats dans l'onglet Surveiller.

1. Identifiez les machines de point de terminaison à partir desquelles vous souhaitez exécuter l'analyse d'application.
2. Les utilisateurs avec des autorisations d'administrateur peuvent installer et configurer l'agent Citrix Probe Agent sur la machine de point de terminaison Téléchargez l'exécutable Citrix Probe Agent disponible sur https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Démarrez l'agent et configurez vos informations d'identification Citrix Workspace. Configurez un utilisateur unique de Workspace sur chaque machine de point de terminaison. Les informations d'identification sont cryptées et stockées de manière sécurisée.

   > **Remarques :**
   >
   > - Pour accéder au site à analyser à partir de l'extérieur du réseau, tapez l'URL d'ouverture de session de Citrix Gateway dans le champ **URL de Workspace**. Citrix Gateway achemine automatiquement la demande vers l'URL du site Workspace correspondante.
   > - Utilisez NetBIOS comme nom de domaine dans le champ Nom d'utilisateur. Par exemple, NetBIOS/NomUtilisateur.
   > - L'analyse des applications prend en charge le service Citrix Content Collaboration à l'aide de l'authentification Workspace (AD uniquement).



4. Dans l'onglet **Configurer pour afficher les résultats de l'analyse**, entrez vos informations d'identification pour accéder à Citrix DaaS. Vous pouvez trouver le nom du client, l'ID du client et la clé secrète à partir de la page Accès aux API dans la console Citrix Cloud.



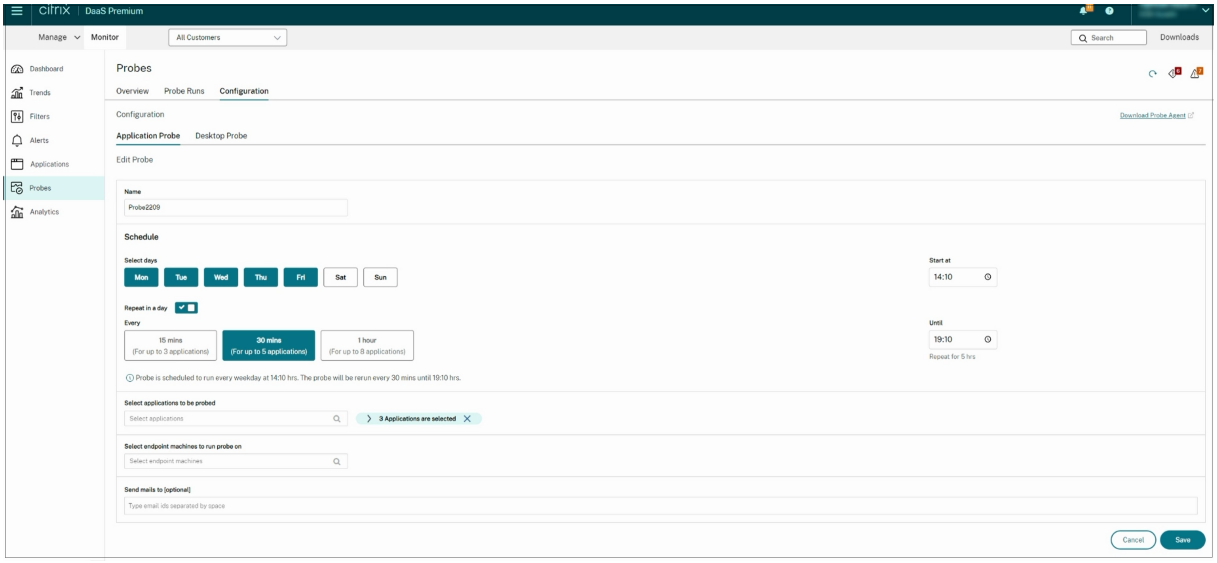
Étape 2 : Configuration de l'analyse d'application dans l'onglet Surveiller

1. Dans Citrix DaaS, accédez à **Configuration** > **Configuration de l'analyse** > **Analyse d'applications** et cliquez sur **Créer une analyse** :
2. Sur la page **Créer une analyse**, entrez le nom de l'analyse.
3. Sélectionnez le calendrier :

    a) Choisissez les jours de la semaine pendant lesquels vous souhaitez que l'analyse soit exécutée.
    b) Entrez l'heure de début à laquelle vous souhaitez que l'analyse s'exécute.
    c) Vous pouvez également choisir l'option **Répéter dans un jour**. Entrez l'heure de fin et l'intervalle pendant lequel vous souhaitez que l'analyse se répète dans un délai d'une journée. Par exemple, la configuration ci-dessous permet d'exécuter des analyses d'application de 12h08 à 16h34, toutes les 30 minutes tous les lundis, mercredis, jeudis et dimanches.

4. Sélectionnez le nombre recommandé d'applications à analyser en fonction de l'intervalle.
5. Sélectionnez les machines de point de terminaison sur lesquelles l'analyse doit s'exécuter.
6. Entrez les adresses e-mail auxquelles les résultats des échecs d'analyse sont envoyés et cliquez sur **Enregistrer**.

Dans cette configuration, les sessions de l'application sont lancées à 12h08, 12h38, 13h08, et ainsi de suite jusqu'à 16h08 tous les lundis, mercredis, jeudis et dimanches.



> **Remarque :**
>
> - Configurez votre serveur de messagerie dans **Alertes** > **Configuration du serveur de messagerie**.
> - Une fois la configuration effectuée dans l'onglet **Surveiller**, l'agent exécute les analyses configurées à partir de l'heure suivante.
> - Les analyses qui ont été configurées avant l'introduction de l'option **Répéter dans un jour** continuent de s'exécuter à l'heure prévue. L'option **Répéter dans un jour** est désactivée par défaut.

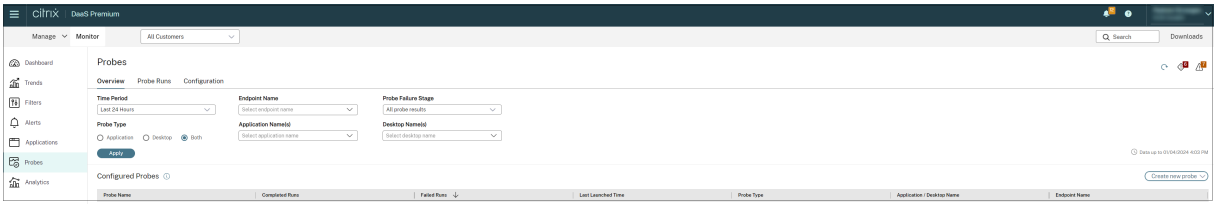
Étape 3 : Exécution de l'analyse

L'agent exécute l'analyse d'application en fonction de la configuration de l'analyse qu'il récupère toutes les heures de l'onglet Surveiller. Il lance des applications sélectionnées en série à l'aide de Workspace. L'agent communique les résultats à l'onglet Surveiller via la base de données de l'onglet Surveiller. Les échecs sont signalés en cinq étapes spécifiques :

- **Accessibilité de Workspace :** l'URL Workspace configurée n'est pas accessible.
- **Authentification de Workspace :** les informations d'identification Workspace configurées ne sont pas valides.
- **Énumération Workspace :** la liste des applications Workspace ne contient pas l'application à tester.
- **Téléchargement ICA :** le fichier ICA n'est pas disponible.
- **Lancement d'applications :** l'application n'a pas pu être lancée.

Étape 4 : Affichage des résultats de l'analyse

Vous pouvez afficher les résultats les plus récents de l'analyse sur la page **Applications** de Citrix DaaS.



Pour une résolution plus poussée, cliquez sur le lien du résultat de l'analyse pour voir plus de détails sur la page **Tendances** > **Résultats de l'analyse d'application**.

Les résultats des analyses consolidés sont disponibles pour les dernières 24 heures ou les 7 derniers jours sur cette page. Vous pouvez voir l'étape à laquelle l'analyse a échoué. Vous pouvez filtrer le tableau pour une application, une étape d'échec d'analyse ou une machine de point de terminaison spécifique.

Analyse de bureaux

February 16, 2023

L'analyse de bureaux automatise les vérifications d'intégrité des bureaux Citrix Virtual Desktops publiés sur un site. Les résultats de l'analyse de bureaux sont disponibles dans Surveiller. Citrix Probe Agent prend désormais en charge les sites hébergés sur Citrix Cloud Japan et Citrix Cloud Government Planes.

Sur la page Configuration de Surveiller, configurez les bureaux à analyser, les machines de point de terminaison sur lesquelles exécuter l'analyse et l'heure de l'analyse. L'agent teste le lancement des bureaux sélectionnés à l'aide de Workspace et renvoie les résultats à Surveiller. Les résultats de l'analyse s'affichent dans l'interface utilisateur de Surveiller : les données des dernières 24 heures sur la page Applications et l'historique des analyses sur la page **Tendances > Résultats de l'analyse > Résultats de l'analyse des bureaux**.

Ici, vous pouvez voir l'étape à laquelle l'échec de l'analyse s'est produit : Accessibilité de Workspace, Authentification Workspace, Énumération Workspace, Téléchargement de fichier ICA ou Lancement de bureaux. Le rapport d'échec est envoyé aux adresses électroniques configurées.

Vous pouvez planifier l'exécution de vos analyses de bureaux pendant les heures creuses sur plusieurs zones géographiques. Les résultats complets peuvent aider à résoudre de manière proactive les problèmes liés aux bureaux provisionnés, aux machines d'hébergement ou aux connexions avant que les utilisateurs ne les rencontrent.

Cette fonctionnalité nécessite Probe Agent 1903 ou version ultérieure.

Exigences :

- Les machines de point de terminaison exécutant des agents Probe Agent sont des ordinateurs Windows dotés de Citrix Receiver pour Windows version 4.8 ou ultérieure ou de l'application Citrix Workspace pour Windows (anciennement Citrix Receiver pour Windows) version 1906 ou ultérieure. L'application Workspace pour plate-forme Windows universelle (UWP) n'est pas prise en charge.
- Citrix Probe Agent prend en charge l'authentification basée sur un formulaire par défaut, telle que prise en charge par StoreFront et Citrix WorkSpace. Citrix Probe Agent ne prend pas en charge d'autres méthodes d'authentification telles que l'authentification unique (SSO) ou l'authentification multifacteur (MFA). De même, Citrix Probe Agent ne fonctionne que lorsqu'aucun serveur proxy ou équilibreur de charge tel que Citrix Gateway ou Citrix ADC n'est déployé.
- Assurez-vous que Microsoft .NET Framework version 4.7.2 ou ultérieure est installé sur la machine de point de terminaison sur laquelle vous souhaitez installer Probe Agent.
- Pour utiliser l'agent dans Citrix Cloud Japan Control Plane, définissez la valeur de registre du chemin "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" sur 2. Pour utiliser l'agent dans Citrix Cloud Government Control Plane, définissez la valeur de registre du chemin "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region" sur 3.

Comptes ou autorisations d'utilisateur requis pour exécuter l'analyse de bureaux :

- Un utilisateur unique de Workspace pour effectuer une analyse sur chaque machine de point de terminaison. L'utilisateur Workspace n'a pas besoin d'être un administrateur ; les analyses peuvent s'exécuter dans un contexte non-administrateur.
- Comptes d'utilisateur avec des autorisations d'administrateur Windows pour installer et configurer l'agent Citrix Probe Agent sur les machines de point de terminaison
- Un compte d'utilisateur administrateur complet ou un rôle personnalisé avec les autorisations suivantes. La réutilisation de comptes d'utilisateur normaux pour l'analyse des bureaux risque de déconnecter les utilisateurs de leurs sessions actives.
  - Autorisations du groupe de mise à disposition :
    - Lecture seule
  - Autorisations de Surveiller :
    - Créer/modifier/supprimer la configuration du serveur de messagerie d'alerte - si le serveur de messagerie n'est pas déjà configuré
    - Créer/modifier/supprimer des configurations d'analyse
    - Afficher la page Configurations
    - Afficher la page des tendances

Configurer l'analyse de bureaux

Vous pouvez planifier l'exécution de vos analyses de bureaux pendant les heures creuses sur plusieurs zones géographiques. Les résultats d'analyse complets peuvent aider à résoudre les problèmes liés aux bureaux, à la machine d'hébergement ou à la connexion avant que les utilisateurs ne les rencontrent.

Citrix Probe Agent version 2103 prend en charge l'agrégation de sites. Les applications et les bureaux peuvent être énumérés et lancés à partir de sites agrégés. Lorsque vous configurez Probe Agent, sélectionnez l'option **Agrégation de site Workspace (StoreFront) activée** pour activer l'énumération des applications et des bureaux à partir de sites agrégés. Les combinaisons de sites suivantes sont prises en charge :

- Plusieurs sites locaux ayant une URL StoreFront
- Sites locaux et cloud disposant d'une URL StoreFront ou Workspace
- Plusieurs sites cloud disposant d'une seule URL Workspace

> **Remarque :**
>
> Vous devez créer des administrateurs ou des utilisateurs distincts pour configurer les outils d'analyses (Probe Agent) qui n'ont accès qu'à un seul site.

Étape 1 : Installation et configuration de Citrix Probe Agent

Citrix Probe Agent est un exécutable Windows qui simule le lancement du bureau par l'utilisateur via Workspace. Il teste les lancements de bureaux configurés dans l'onglet Surveiller et communique les résultats dans l'onglet Surveiller.

1. Identifiez les machines de point de terminaison à partir desquelles vous souhaitez exécuter l'analyse de bureaux.
2. Les utilisateurs avec des autorisations d'administrateur peuvent installer et configurer l'agent Citrix Probe Agent sur la machine de point de terminaison Téléchargez l'exécutable Citrix Probe Agent disponible sur https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Démarrez l'agent et configurez vos informations d'identification Workspace Receiver pour Web. Configurez un utilisateur unique de Workspace sur chaque machine de point de terminaison. Les informations d'identification sont cryptées et stockées de manière sécurisée.

   > **Remarques :**
   >
   > - Pour accéder au site à analyser à partir de l'extérieur du réseau, tapez l'URL de la page de connexion à Citrix Gateway dans le champ URL de Workspace. Citrix

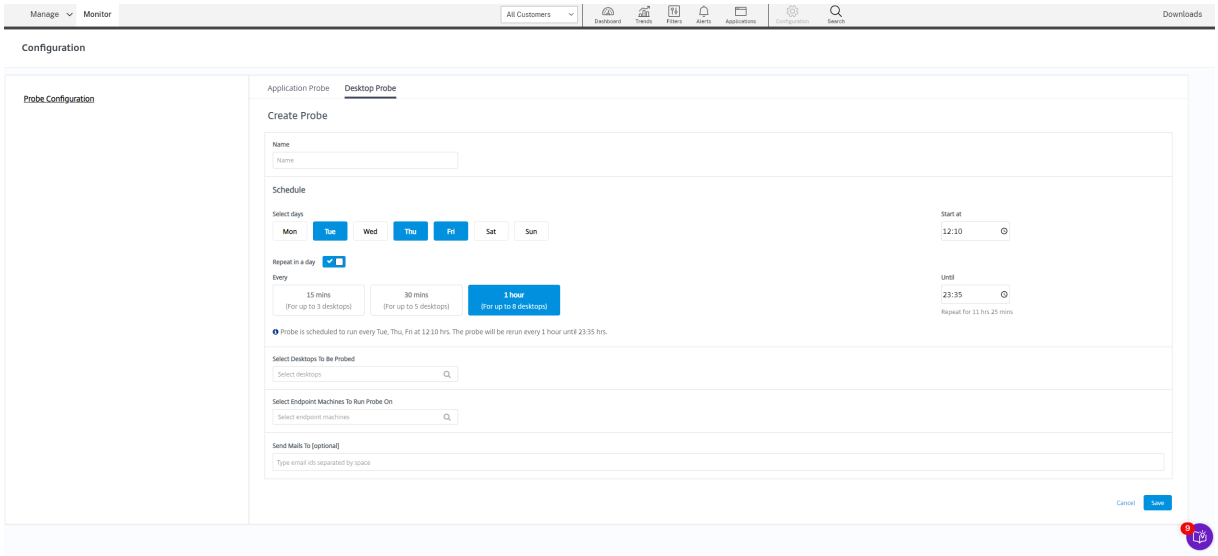
> Gateway achemine automatiquement la demande vers l'URL du site Workspace correspondante. Cette fonctionnalité est disponible pour Citrix Gateway version 12.1 ou ultérieure.
> - Utilisez NetBIOS comme nom de domaine dans le champ Nom d'utilisateur. Par exemple, NetBIOS/NomUtilisateur.
> - L'analyse de bureaux prend en charge le service Citrix Content Collaboration à l'aide de l'authentification Workspace (AD uniquement).
> - Vous devez activer l'ouverture de session interactive pour l'utilisateur StoreFront unique configuré.

4. Dans l'onglet **Configurer pour afficher les résultats de l'analyse**, entrez vos informations d'identification Surveiller. Vous pouvez trouver le nom du client, l'ID du client et la clé secrète à partir de la page Accès aux API dans la console Citrix Cloud.

Étape 2 : Configuration de l'analyse de bureaux dans Surveiller

1. Dans Citrix DaaS, accédez à **Configuration** > **Configuration de l'analyse** > **Analyse d'applications** et cliquez sur **Créer une analyse**.
2. Sur la page **Créer une analyse**, entrez le nom de l'analyse.
3. Sélectionnez le calendrier :
    a) Choisissez les jours de la semaine pendant lesquels vous souhaitez que l'analyse soit exécutée.
    b) Entrez l'heure de début à laquelle vous souhaitez que l'analyse s'exécute.
    c) Vous pouvez également choisir l'option **Répéter dans un jour**. Entrez l'heure de fin et l'intervalle pendant lequel vous souhaitez que l'analyse se répète dans un délai d'une journée. Par exemple, la configuration ci-dessous permet d'exécuter des analyses de bureau de 12h10 à 23h35, en répétant toutes les heures tous les mardis, jeudis et vendredis.
4. Sélectionnez le nombre recommandé de bureaux à analyser en fonction de l'intervalle.
5. Sélectionnez les machines de point de terminaison sur lesquelles l'analyse doit s'exécuter.
6. Entrez les adresses e-mail auxquelles les résultats des échecs d'analyse sont envoyés et cliquez sur **Enregistrer**.

Dans cette configuration, les sessions de bureau sont lancées à 12h10, 13h10, 14h10, et ainsi de suite jusqu'à 23h10 tous les mardis, jeudis et vendredis.



> **Remarque :**
>
> - Configurez votre serveur de messagerie dans **Alertes** > **Configuration du serveur de messagerie**.
> - Une fois la configuration de l'analyse de bureau terminée, l'agent exécute les analyses configurées à partir de l'heure suivante.
> - Les analyses qui ont été configurées avant l'introduction de l'option **Répéter dans un jour** continuent de s'exécuter à l'heure prévue. L'option **Répéter dans un jour** est désactivée par défaut.

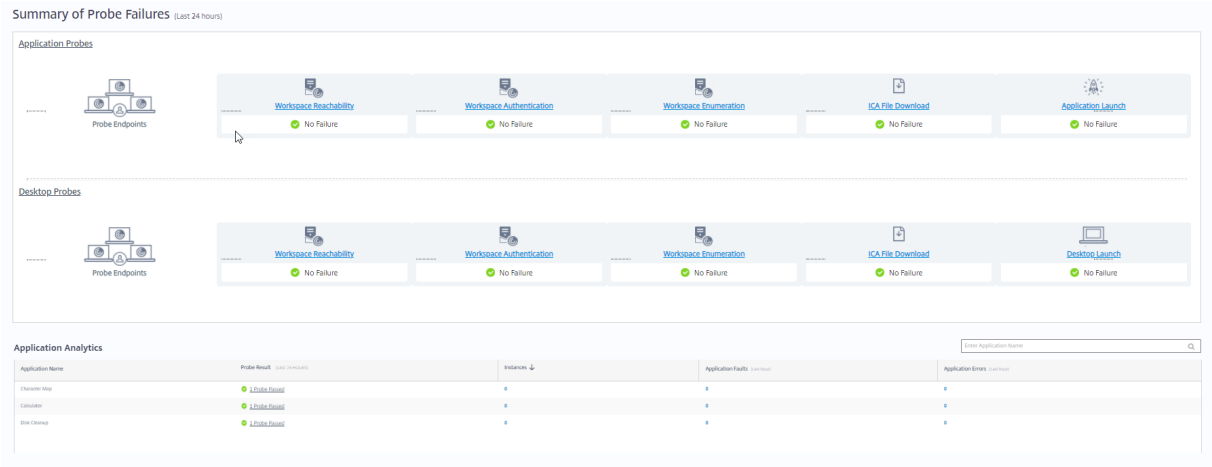
Étape 3 : Exécution de l'analyse

L'agent exécute l'analyse de bureaux en fonction de la configuration de l'analyse qu'il récupère périodiquement de Surveiller. Il lance les bureaux sélectionnés en série à l'aide de Workspace. L'agent communique les résultats à l'onglet Surveiller via la base de données de l'onglet Surveiller. Les échecs sont signalés en cinq étapes spécifiques :

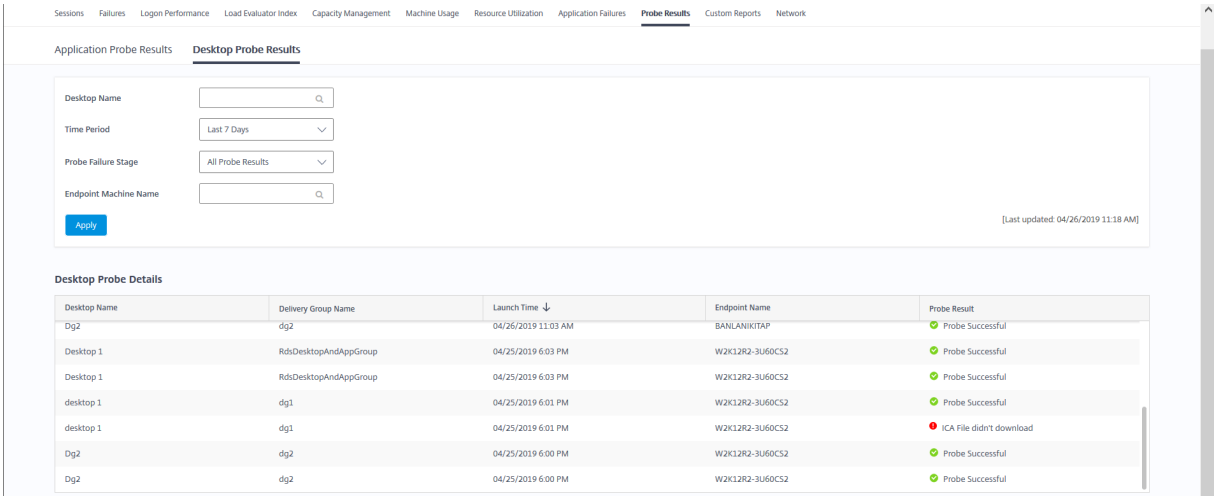
- **Accessibilité de Workspace :** l'URL Workspace configurée n'est pas accessible.
- **Authentification de Workspace :** les informations d'identification Workspace configurées ne sont pas valides.
- **Énumération Workspace :** la liste des bureaux ne contient pas le bureau à tester.
- **Téléchargement ICA :** le fichier ICA n'est pas disponible.
- **Lancement de bureaux** : le bureau ne peut pas être lancé.

Étape 4 : Affichage des résultats de l'analyse

Vous pouvez afficher les résultats les plus récents de l'analyse sur la page **Bureaux**.



Pour une résolution plus poussée, cliquez sur le lien du résultat de l'analyse pour voir plus de détails sur la page **Tendances** > **Résultats de l'analyse** > **Résultats de l'analyse de bureaux**.



Les résultats des analyses consolidés sont disponibles pour les dernières 24 heures ou les 7 derniers jours sur cette page. Vous pouvez voir l'étape à laquelle l'analyse a échoué. Vous pouvez filtrer le tableau pour un bureau, une étape d'échec d'analyse ou une machine de point de terminaison spécifique.

Dépanner les machines

May 17, 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 l'onglet Surveiller 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 dans le Citrix Director Failure Reasons Troubleshooting Guide.

Cliquez sur le lien du nom d'une machine pour accéder à la page **Détails de la machine**.

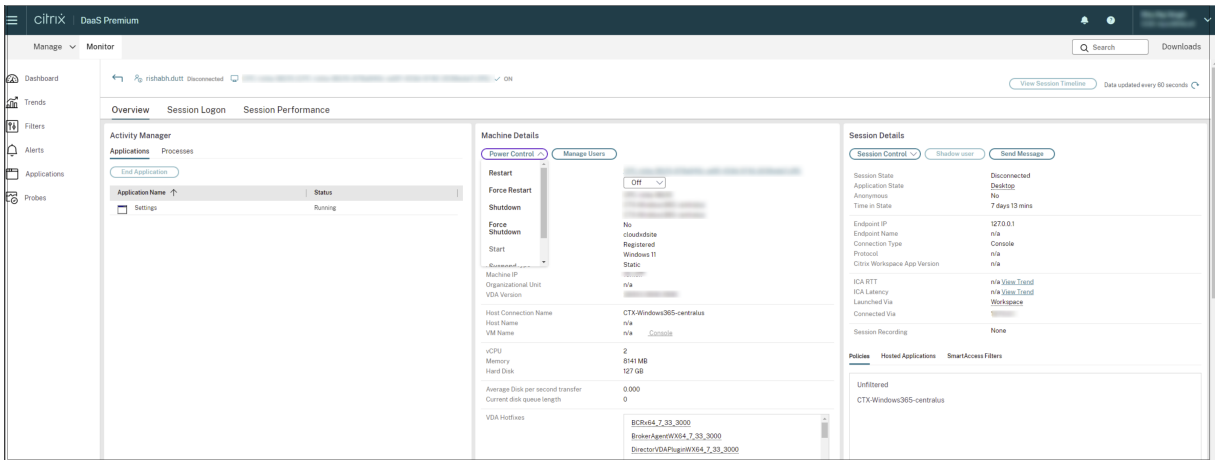
La page Détails de la machine présente les détails de la machine, les détails de l'infrastructure, et les détails des correctifs appliqués sur la machine.

Prise en charge de HDX Plus pour Windows 365 PC Cloud et Azure Virtual Desktop :

> **Remarque :**
>
> Pour HDX Plus pour Windows 365 PC Cloud, seules les options de contrôle de l'alimentation Redémarrer et Forcer le redémarrage sont disponibles. Pour Azure Virtual Desktop (AVD), toutes les options de contrôle de l'alimentation sont disponibles.

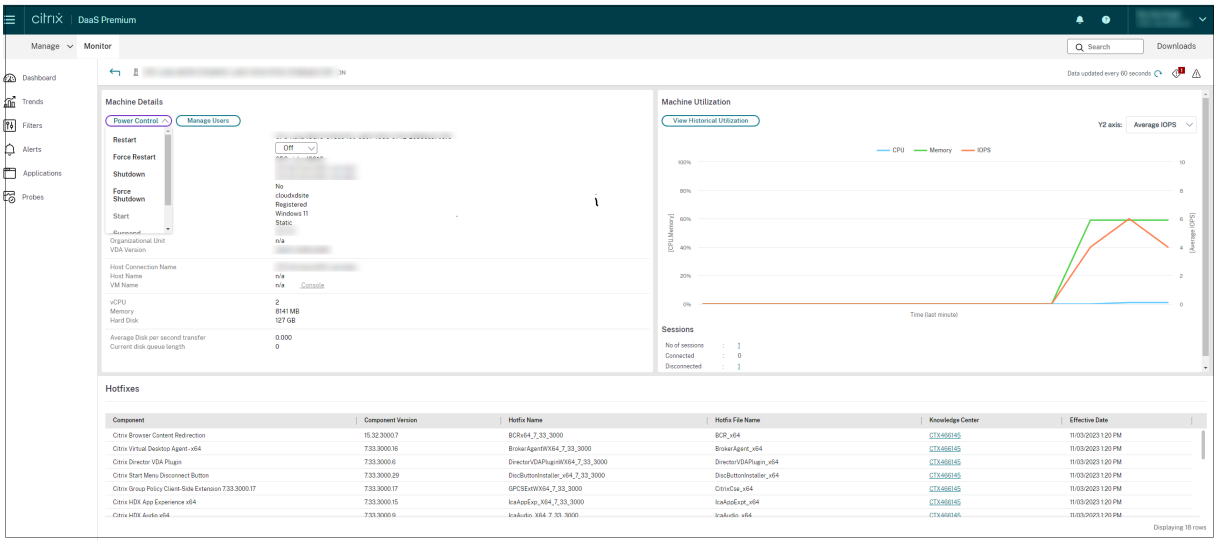
Vous pouvez consulter les options de contrôle de l'alimentation disponibles à l'aide de l'une des méthodes suivantes :

Cliquez sur la liste déroulante **Filtres** >**Sessions** > **Afficher les détails** > **Détails de la machine** > **Contrôle de l'alimentation**, puis sélectionnez une option pour attribuer l'option de contrôle de l'alimentation requise pour une machine.



Ou

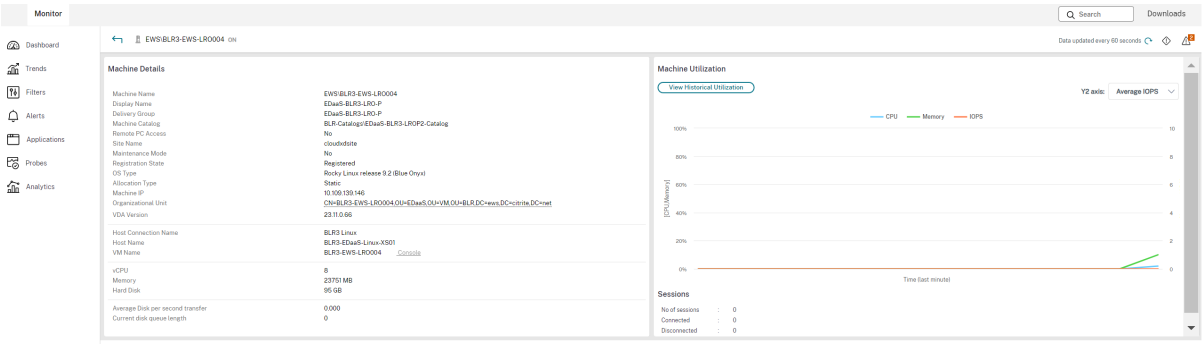
Cliquez sur la liste déroulante **Filtres** > **Machine** > **Détails de la machine** > **Contrôle de l'alimentation**, puis sélectionnez une option pour attribuer l'option de contrôle d'alimentation requise pour une machine.



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 la version 7.14 ou ultérieure du VDA.

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.
- Les graphiques d'utilisation du GPU AMD ne sont disponibles que pour les VDA exécutant Citrix Virtual Apps and Desktops 7 2212 ou version ultérieure.

- 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.

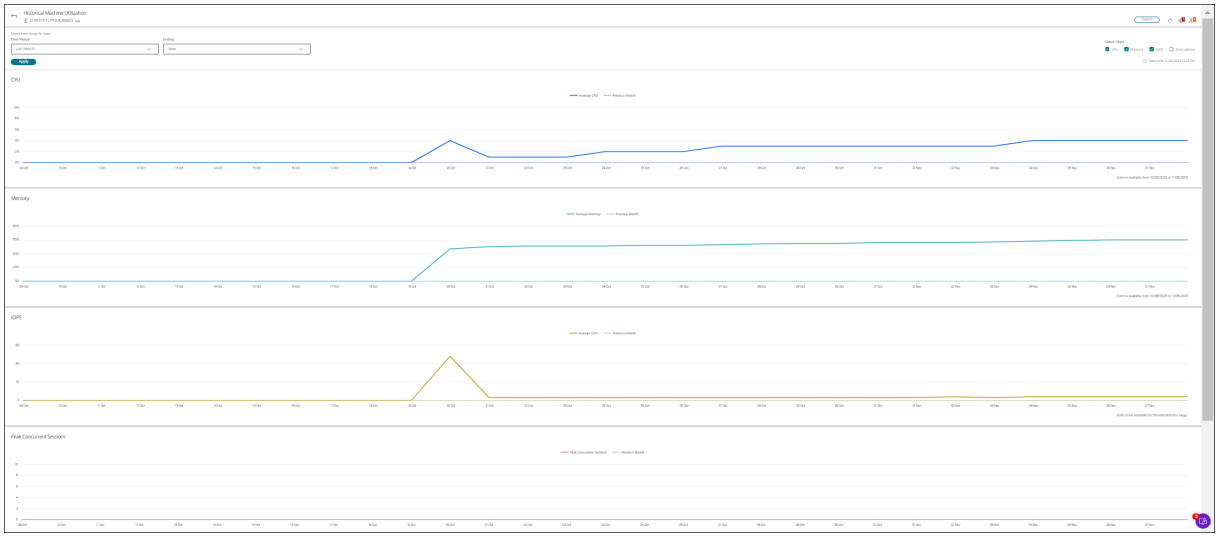
> **Remarque :**
>
> Le paramètre de stratégie Surveillance, **Activer le suivi des processus**, doit être défini sur « Autorisé » pour collecter et afficher les données dans le tableau des 10 processus les plus utilisés sur la page Utilisation historique des machines. La collecte n'est pas autorisée 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.

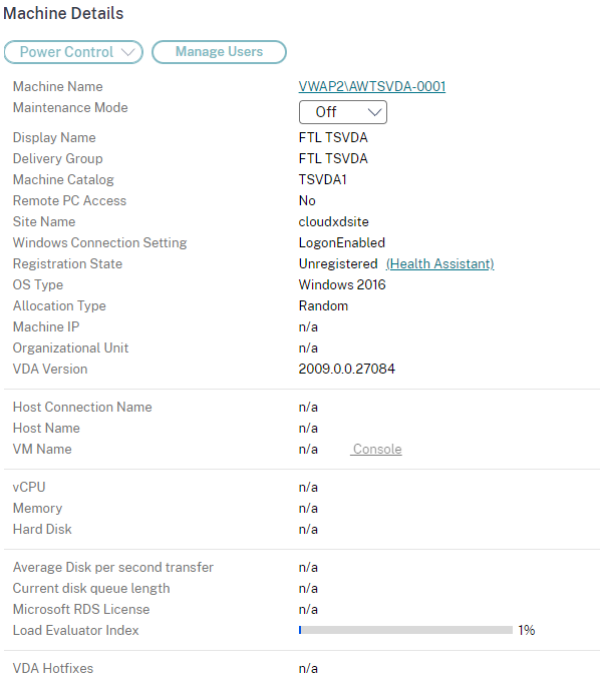
1. Cliquez sur **Exporter** pour exporter les données d'utilisation des ressources pendant la période sélectionnée. Pour de plus amples informations, consultez la section Exporter des rapports dans Surveiller les déploiements.
2. Sous les graphiques, le tableau dresse la liste des 10 processus utilisant 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 ».
   > - Si un site appartenant au plan Citrix Cloud Japan ou Citrix Cloud Government contient plus de 5 000 machines, les données de processus sont disponibles pour un maximum de 2 000 machines uniquement. La stratégie de surveillance des processus doit être activée sur ces machines.

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 du service de surveillance. De cette façon, vous n'avez pas besoin de XenCenter pour résoudre les problèmes sur les VDA hébergés par XenServer. La version 7.3 ou ultérieure du serveur XenServer hébergeant la machine est requise et doit être accessible depuis l'interface utilisateur du service de surveillance.



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.
> - L'accès à la console est lancé 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.

Inspecter les machines ayant fait récemment l'objet d'une action d'alimentation

Vous pouvez désormais inspecter les machines grâce à l'état des actions d'alimentation. Cette fonctionnalité vous permet d'analyser les éléments suivants :

- Échec de mise sous tension entraînant des problèmes pour l'utilisateur
- Échec de mise hors tension qui augmente les coûts

> **Remarque :**
>
> Les données ne sont disponibles que pour les machines à alimentation gérée. Les données ne sont pas disponibles pour les actions d'alimentation effectuées avant la prise en charge de la fonctionnalité.

Vous pouvez consulter l'état des actions d'alimentation des machines de la manière suivante :

À partir de l'onglet **Filtres** > **Machines**. Dans ce cas, les colonnes **Durée de l'action d'alimentation** et **Résultat de l'action d'alimentation** sont visibles par défaut. Vous pouvez également sélectionner les colonnes que vous souhaitez afficher.

À partir de l'onglet **Optimisation des coûts**. Dans ce cas, le filtre par défaut **Action d'alimentation déclenchée par** est défini sur *Autoscale* et **Résultat de l'action d'alimentation** est défini sur *Échec*.

Grâce à cette fonctionnalité, vous pouvez afficher les détails des contrôles d'action d'alimentation. Par exemple, vous pouvez voir qui a déclenché l'action, quelle action a modifié l'état de l'alimentation, la raison de l'échec et l'heure à laquelle l'action s'est terminée. Vous pouvez également exporter ces informations.

Les filtres suivants sont ajoutés pour afficher l'état de l'action d'alimentation :

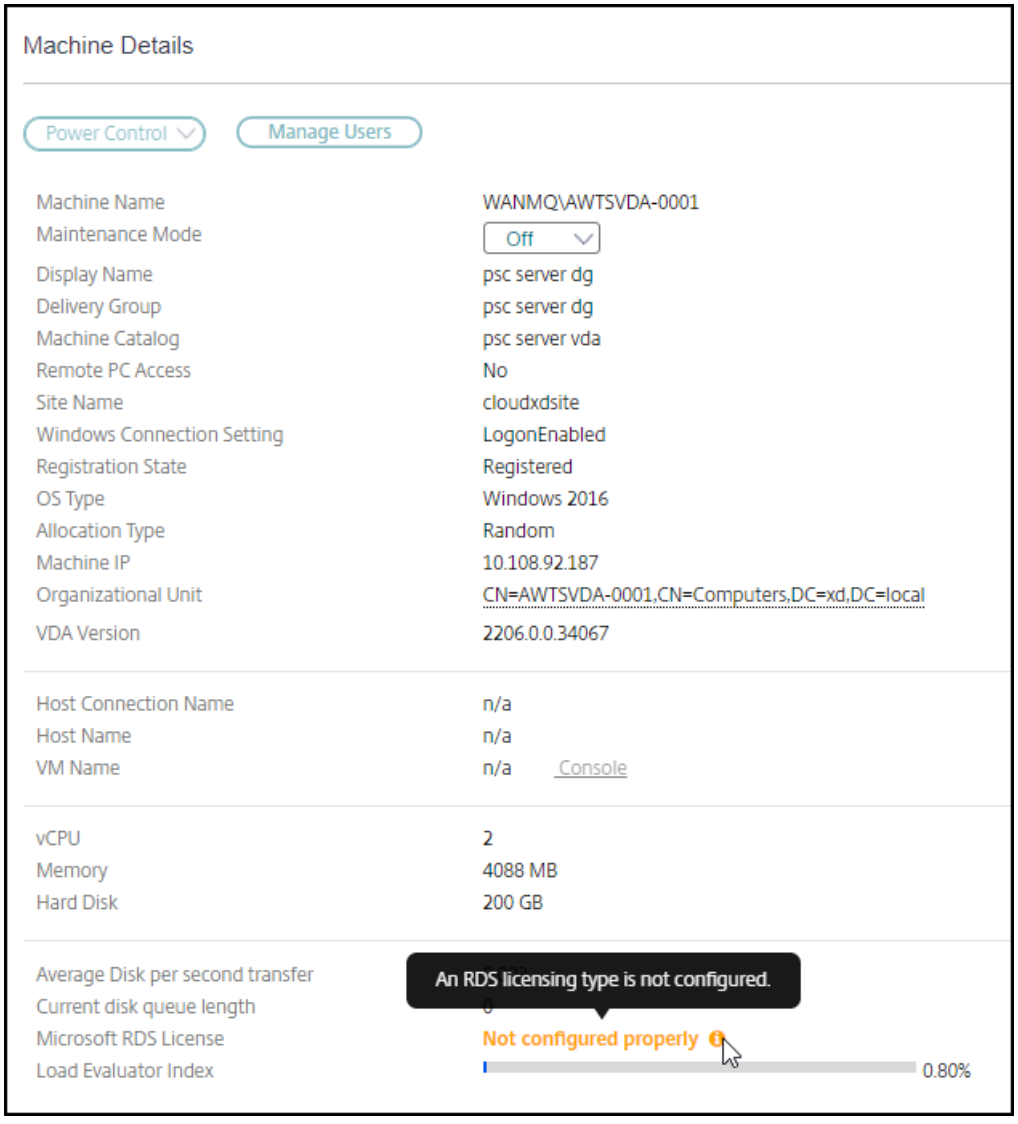
Filtre	Description
Résultat de l'action d'alimentation	Affiche le résultat de l'action d'alimentation. Les valeurs de filtre possibles sont « Succès » et « Échec ».
Action d'alimentation déclenchée par	Affiche l'utilisateur ou l'élément qui a déclenché l'action d'alimentation. Les valeurs de filtre possibles sont les suivantes • Autoscale : cette valeur s'affiche lorsqu'une action d'alimentation est déclenchée par les éléments suivants

Filtre	Description
	• Lorsque l'administrateur arrête une machine virtuelle pour rétablir l'état initial du disque du système d'exploitation de la machine virtuelle. • Lorsqu'une machine virtuelle est arrêtée ou suspendue en fonction des stratégies définies. • Lorsqu'une machine virtuelle est mise à disposition en fonction de la taille du pool ou de la configuration de la taille du tampon. • Admin : cette valeur s'affiche lorsqu'une action d'alimentation est déclenchée par un administrateur. Par exemple, lorsque l'administrateur demande la désactivation, l'activation, la suspension, la reprise ou le redémarrage d'une machine virtuelle. • Utilisateur : cette valeur s'affiche lorsqu'une action d'alimentation est déclenchée par un utilisateur. Par exemple, lorsqu'un utilisateur réinitialise ou active la machine virtuelle, ou reprend le travail sur celle-ci. • Autres : cette valeur s'affiche lorsqu'une action d'alimentation est déclenchée pour des raisons planifiées et inconnues.
Dernière action d'alimentation	Affiche l'action d'alimentation exacte qui s'est produite sur la machine, telle que la mise sous tension, la mise hors tension, l'arrêt, le redémarrage, la réinitialisation, la reprise, etc.
Durée de l'action d'alimentation	Heure à laquelle l'action d'alimentation est terminée. Les valeurs de filtre possibles sont les suivantes : dernière minute, 5 dernières minutes, 30 dernières minutes, dernière heure, aujourd'hui, dernières 24 heures et hier.

Filtre	Description
Raison de l'échec de l'action d'alimentation	Affiche la raison de l'échec. Les valeurs de filtre possibles sont les suivantes : Échec signalé par l'hyperviseur, Débit maximal de l'hyperviseur dépassé, Erreur inconnue et Aucun. Si l'action est réussie, « Aucun » s'affiche.

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 de la licence RDS pour les machines sous période de grâce avec licence valide affiche un 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.

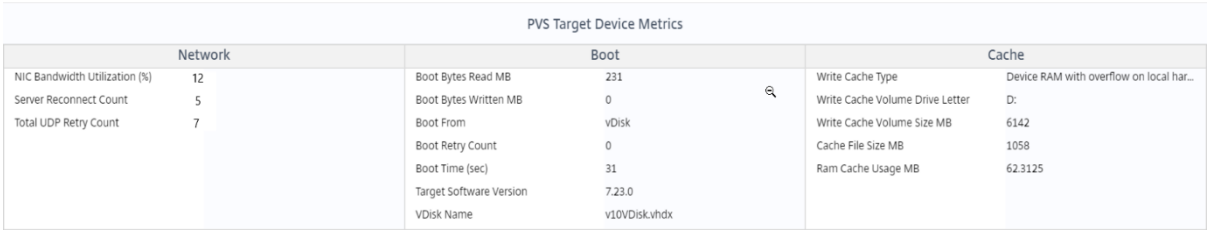
Type de message	Messages dans le service de surveillance
Erreur	Disponible pour les VDA versions 7.16 et ultérieures.
Erreur	Les nouvelles connexions RDS ne sont pas autorisées.
Erreur	La licence RDS a dépassé sa période de grâce.
Erreur	Aucun serveur de licences n'est configuré pour le niveau d'OS requis 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.

Type de message	Messages dans le service de surveillance
Avertissement	Avec le type de licence d'accès client par appareil, la licence de l'appareil client n'a pas pu 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.

Mesures des machines cibles PVS

Vous pouvez afficher l'état des machines cibles PVS pour les machines avec OS mono-session et multi-session sur la page **Détails de la machine** dans Monitor. Plusieurs mesures sont disponibles sur ce panneau : **Réseau**, **Démarrage** et **Cache**. Ces mesures vous aident à surveiller et à dépanner les machines cibles PVS pour vous assurer qu'elles sont opérationnelles.



Réseau :

- Utilisation de la bande passante réseau : utilisation moyenne de la bande passante sur toutes les cartes réseau.
- Nombre de reconnexions au serveur : nombre de fois où le serveur s'est reconnecté en raison de problèmes de réseau ou de rééquilibrage de serveurs ou d'arrêts et de redémarrages de Citrix Provisioning Stream Service.
- Nombre total de tentatives UDP : nombre de fois que la machine cible du provisioning a tenté de se reconnecter au serveur de provisioning à l'aide d'UDP. Cette mesure vous aide à savoir s'il existe des problèmes de réseau dans Citrix Provisioning Stream Service (par exemple, des configurations de commutateur incorrectes).

Démarrage :

- Octets de démarrage lus Mo : octets lus lors du démarrage.
- Octets de démarrage écrits Mo : octets écrits lors du démarrage.

- Démarrer depuis : support de démarrage (vDisk, disque local, etc.).
- Nombre de tentatives de démarrage : nombre de tentatives de démarrage de la machine.
- Temps de démarrage : temps de démarrage de la machine, en secondes. Par défaut, il y a un délai de 5 secondes entre les nouvelles tentatives. Si ce délai se transforme en deux chiffres, le temps de démarrage augmente sensiblement. Vérifiez votre configuration de provisioning pour résoudre ce problème.
- Version du logiciel cible : version du logiciel de la machine cible du provisioning.
- Nom du vDisk : vDisk à partir duquel la machine cible du provisioning démarre.

Cache :

- Type de cache d'écriture : le vDisk peut être défini sur différents types de cache. Pour obtenir davantage d'informations, veuillez consulter l'article CTX119469 du centre de connaissances.
- Lettre du lecteur de volume du cache d'écriture : lettre de lecteur pour les types de cache d'écriture impliquant des lecteurs.
- Taille du volume du cache d'écriture Mo : taille totale du volume configuré pour le cache d'écriture.
- Taille du fichier cache Mo : taille actuelle du fichier cache (cache sur la RAM de la machine avec débordement sur le disque dur).
- Utilisation du cache RAM Mo : taille actuelle du cache RAM (cache sur la RAM de la machine avec débordement sur le disque dur). Utilisez le débordement sur le disque uniquement si nécessaire. Cette mesure est utile lors de la définition ou de l'optimisation de la taille appropriée du cache RAM.

Pour plus d'informations, consultez la section Utilisation de la barre d'état sur une machine cible.

Les mesures de provisioning des machines cibles sont disponibles uniquement sur :

- Provisioning des machines.
- Provisioning des machines cibles version 7.19 et ultérieure.
- VDA version 2003 et ultérieure.

> **Remarque :**
>
> Les mesures pour le nombre de reconnexions au serveur et le nombre de tentatives UDP ne sont disponibles que pour la version 1912 CU2 ou ultérieure.

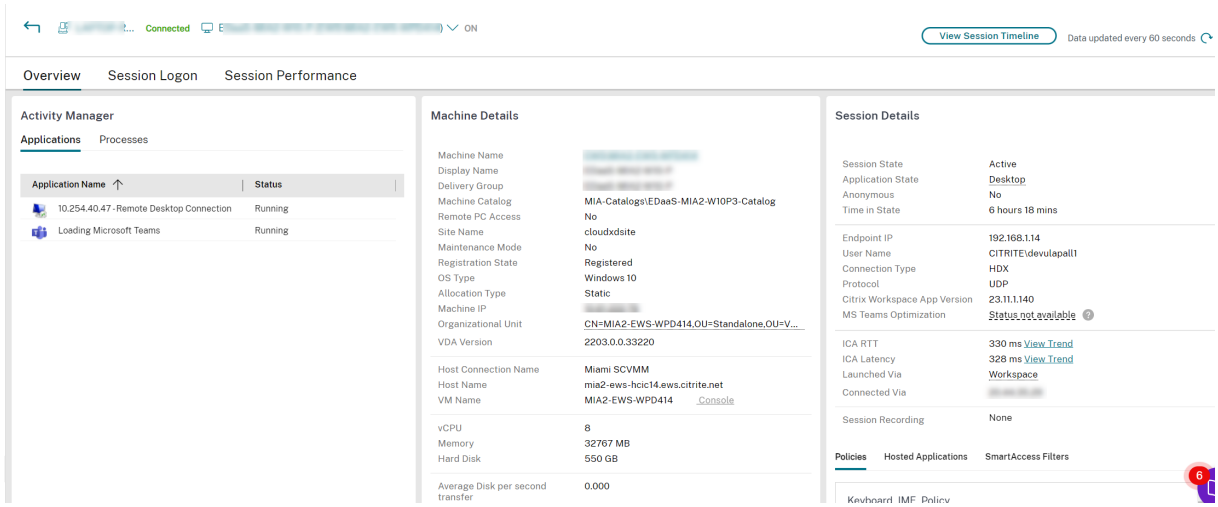
Résoudre les problèmes utilisateur

May 17, 2024

Utilisez la vue **Service d'assistance** de l'onglet Surveiller (page **Gestionnaire d'activités**) pour afficher des informations sur l'utilisateur ou le point de terminaison :

Cliquez sur **Afficher les détails** dans le gestionnaire d'activités de l'utilisateur pour ouvrir la page **Détails de l'utilisateur**.

Cliquez sur **Afficher les détails** depuis le gestionnaire d'activités du point de terminaison pour ouvrir la page **Détails du point de terminaison**.



Si l'utilisateur a démarré plusieurs sessions, le sélecteur de session s'affiche.

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.
- Résolvez le problème avec les actions recommandées dans le tableau suivant, et, si nécessaire, informez l'administrateur du problème.

État d'optimisation de Microsoft Teams

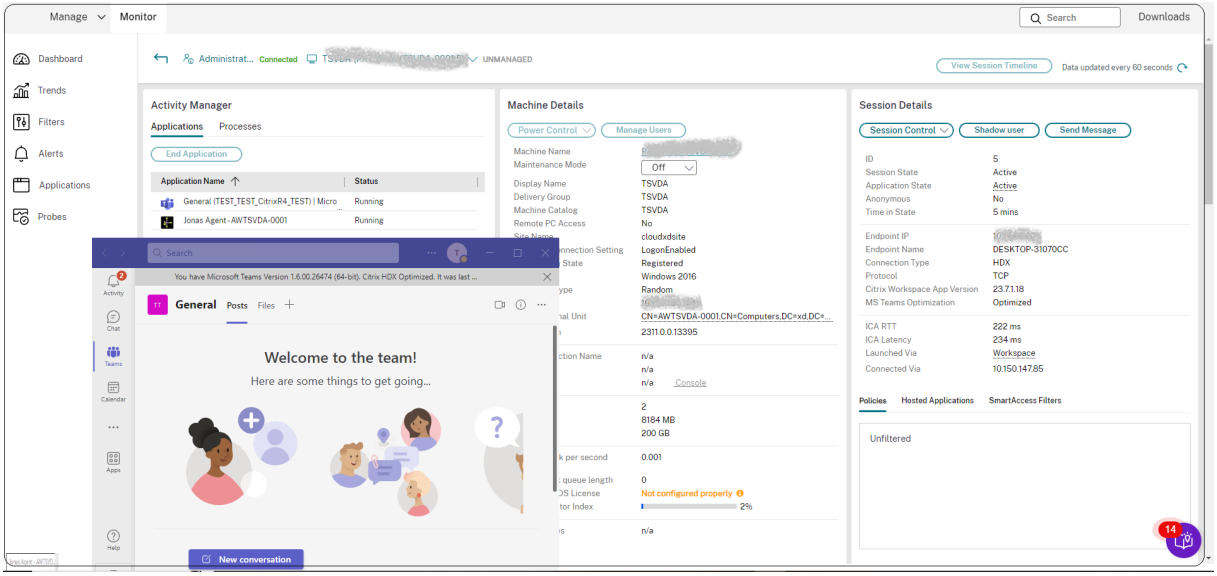
Citrix Monitor affiche l'état d'optimisation de Microsoft Teams pour les sessions HDX dans la page **Détails de l'utilisateur** > panneau **Détails de la session** > champ **Optimisation MS Teams**. L'optimisation de Microsoft Teams est essentielle pour une meilleure expérience utilisateur, notamment 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 Monitor prend en charge Microsoft Teams 2.1 ou une version antérieure.

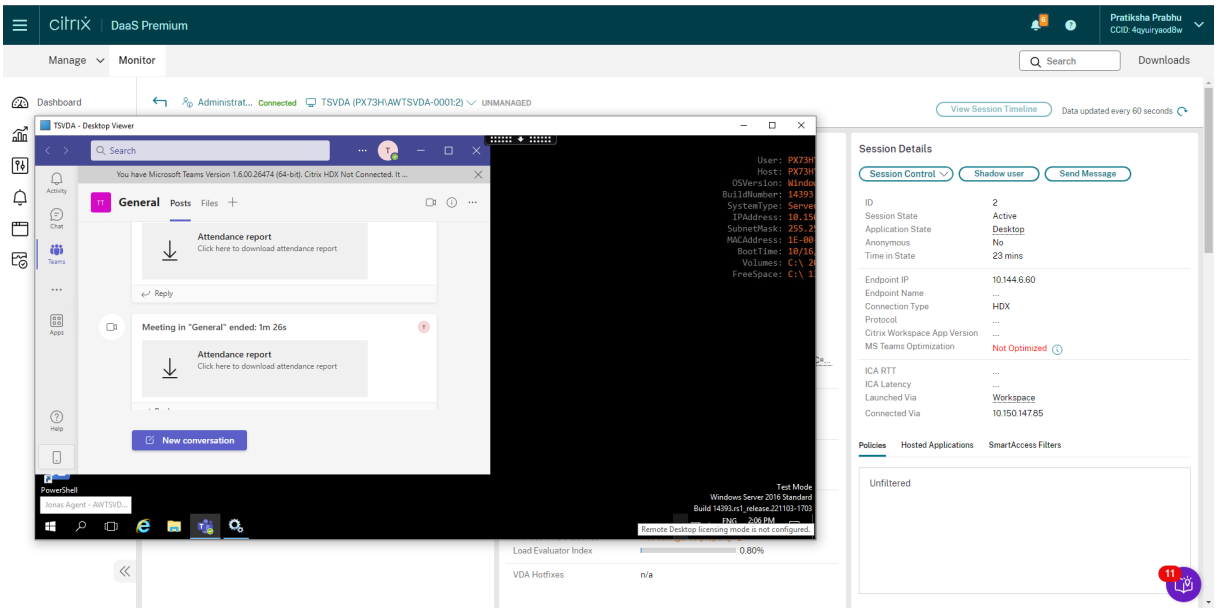
Logiciels requis :

- 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

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
Identifier les éléments impliqués dans l'établissement de la session	Vue Analyser la topologie 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
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, à partir de la vue Détails de l'utilisateur, vérifiez le panneau Détails de la machine.

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

La recherche de nom d'utilisateur est effectuée dans tous les services Active Directory configurés.

Lorsque vous entrez un nom de machine à plusieurs utilisateurs dans le champ Rechercher, les détails de la machine s'affichent pour la machine spécifiée.

Lorsque vous entrez un nom de point de terminaison dans le champ Rechercher, les sessions non authentifiées (anonymes) et authentifiées connectées à un point de terminaison spécifique sont répertoriées. Cette liste 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 l'onglet **Surveiller**.

Diagnostiquer les problèmes de démarrage de session

February 21, 2024

Outre les phases de processus d'ouverture de session mentionnées dans la section Diagnostiquer les problèmes de connexion utilisateur, Monitor 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 du point de terminaison**. 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.

Pré-requis

Assurez-vous que les conditions préalables suivantes sont remplies pour que les données de durée de démarrage de session soient affichées :

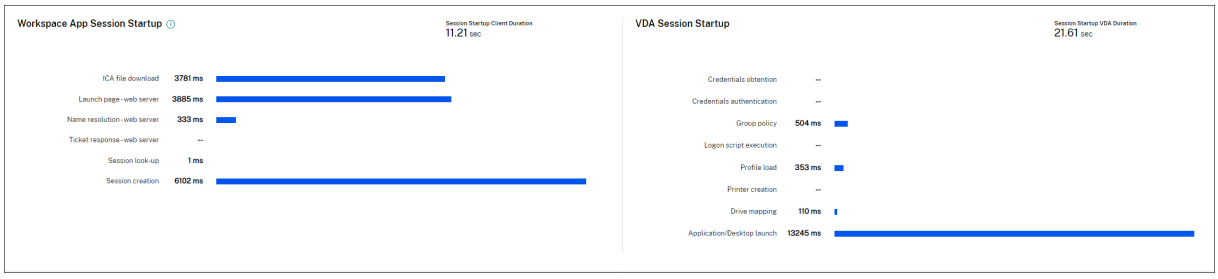
- VDA 1903 ou version ultérieure.
- Le service EUEM (End User Experience Monitoring) de Citrix doit être exécuté sur le VDA.

Limitations

Les limitations suivantes s'appliquent lorsque le service de surveillance 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.
- IFDCD n'est disponible que lorsque l'application Workspace est détectée lors du lancement à partir d'un navigateur.
- Pour les lancements de session à partir de macOS, 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 Monitor 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 commence aussi près que

possible de l'heure de la demande (clic de souris) et se termine lorsque la connexion ICA entre la machine client et le VDA a été établie. Pour 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 (IFDCD)

IFDCD est le 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 sont les suivantes :

- 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 existante 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 indique 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 être artificiellement gonflée si un utilisateur ne parvient pas à fournir les informations d'identification en temps opportun, et n'est donc pas inclus 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 requis par le VDA pour authentifier les informations d'identification de l'utilisateur auprès du fournisseur d'authentification, qui peut être Kerberos, Active Directory ou une interface de fournisseur de support de sécurité (SSPI).

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.

Vous pouvez rendre asynchrones les scripts de connexion de l'utilisateur ou du groupe. Optimisez 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, ce qui consomme des ressources supplémentaires. Parfois, cela peut consommer une portion importante du processeur. Utilisez les **dossiers de base des services Terminal Server** avec des dossiers personnels redirigés pour atténuer ce problème. En général, utilisez 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, aucune valeur n'est 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. Reconfigurez 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 pour désactiver les canaux virtuels inutilisés, tels que le mappage audio ou de port COM, afin d'optimiser le protocole ICA et d'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. Usernit.exe exécute des scripts d'ouverture de session, rétablit les connexions réseau, puis démarre explorer.exe, l'interface utilisateur Windows. 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 la création de session sur VDA.

Diagnostiquer les problèmes de connexion utilisateur

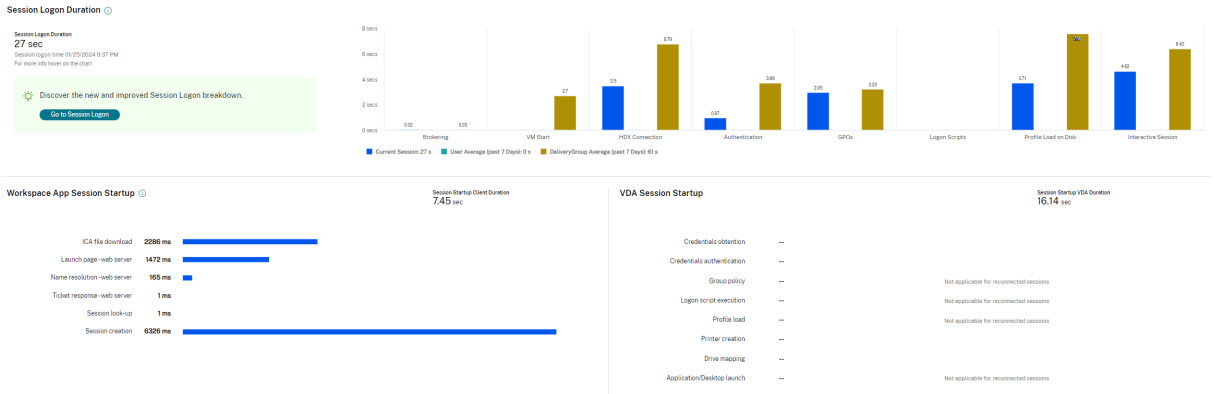
November 24, 2023

Utilisez les données de durée d'ouverture de session pour résoudre les problèmes d'ouverture de session 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.

Dans la vue Détails de l'utilisateur, la durée est affichée sous la forme d'une valeur numérique en dessous de laquelle l'heure d'ouverture de session est affichée ainsi qu'un graphique des phases du processus d'ouverture de session.

Lorsque les utilisateurs ouvrent une session sur Citrix Virtual Apps and Desktops, Monitor Service suit les phases du processus d'ouverture de session depuis la connexion de l'utilisateur à partir de l'application Citrix Workspace jusqu'au moment où le bureau est prêt à être utilisé.



Le nombre élevé sur la gauche est la durée totale d'ouverture de session et il est calculé en combinant la durée nécessaire à l'établissement de la connexion et à l'obtention d'un bureau à partir du Delivery Controller avec le temps nécessaire pour authentifier et ouvrir la session sur un bureau virtuel. Les informations de durée sont présentées en secondes (ou fractions de secondes).

Conditions préalables

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.

> **Remarque :**
>
> La durée de connexion est prise en charge uniquement sur le shell Windows par défaut (explorer.exe) et non sur les shells personnalisés.

Étapes pour résoudre les problèmes d'ouverture de session utilisateur

1. Dans la vue **Détails de l'utilisateur**, résolvez l'état d'ouverture de session à l'aide du panneau Durée de l'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 VM

Si la session requiert le démarrage d'une machine, durée requise pour démarrer la machine virtuelle.

Connexion HDX

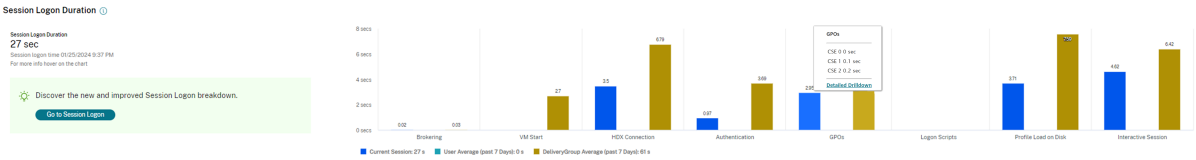
Durée requise pour effectuer les étapes permettant d'établir la connexion HDX du client vers la machine virtuelle.

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 **Analyse détaillée** 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 https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277416(v=technet.10).

Scripts d'ouverture de session

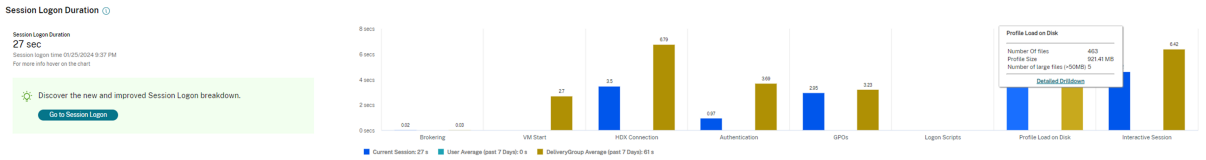
Si des scripts de connexion sont configurés pour la session, durée requise pour l'exécution des scripts de connexion.

Chargement du profil

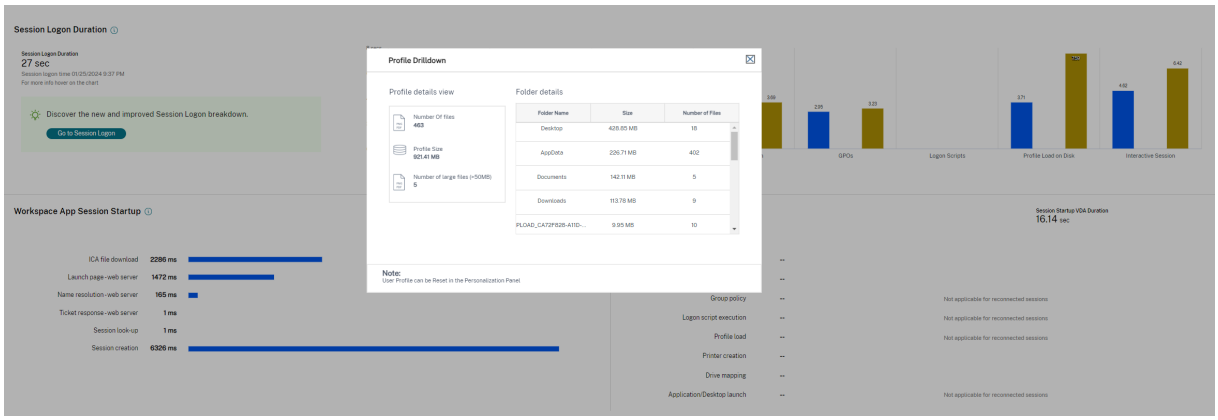
Si des paramètres de profil sont configurés pour l'utilisateur ou la machine virtuelle, durée requise pour charger le profil utilisateur.

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 et 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. Ces informations supplémentaires peuvent aider à résoudre les problèmes de chargement de profil.



Cliquez sur **Analyse détaillée** pour afficher des détails sur chaque dossier individuel du dossier racine du profil (par exemple, C:/Users/nom d'utilisateur), sa taille et le nombre de fichiers (y compris les fichiers contenus dans les dossiers imbriqués).



Le détail des profils est disponible sur les VDA 1811 et versions ultérieures. 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 noms de dossier sont visibles. Pour masquer les noms de dossier, modifiez les valeurs de registre sur la machine VDA en procédant comme suit :

> **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 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 les détails 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

Durée requise pour transférer le contrôle du clavier et de la souris à l'utilisateur après chargement du profil utilisateur. 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
- la durée de chaque phase secondaire
- le délai cumulé total entre ces sous-phases

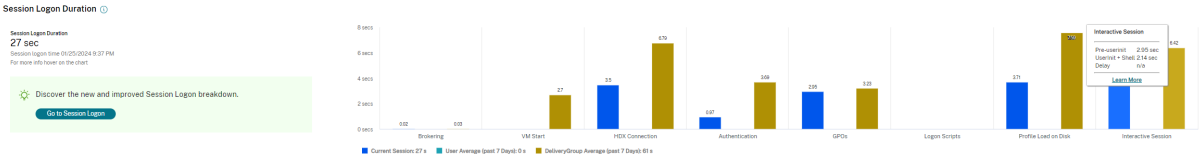
> **Remarque :**
>
> Cette fonctionnalité est disponible sur la version 1811 et ultérieure des VDA. Si vous avez lancé des sessions sur des sites antérieurs à 7.18 et que vous avez ensuite mis à niveau vers 7.18, le message « Exploration non disponible en raison d'une erreur du serveur » s'affiche. Toutefois, 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 VM (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 https://docs.microsoft.com/en-us/previous-versions/ms813609(v=msdn.10) 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 VM ou Négociation.

Observer les utilisateurs

November 17, 2022

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 Windows 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.

La fonctionnalité d'observation est lancée 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 Citrix Cloud.

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 :**
>
> - L'onglet Surveiller utilise le nom de domaine complet pour se connecter au VDA Linux cible. Assurez-vous que le client du service de surveillance 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 du service de surveillance 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 d'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.

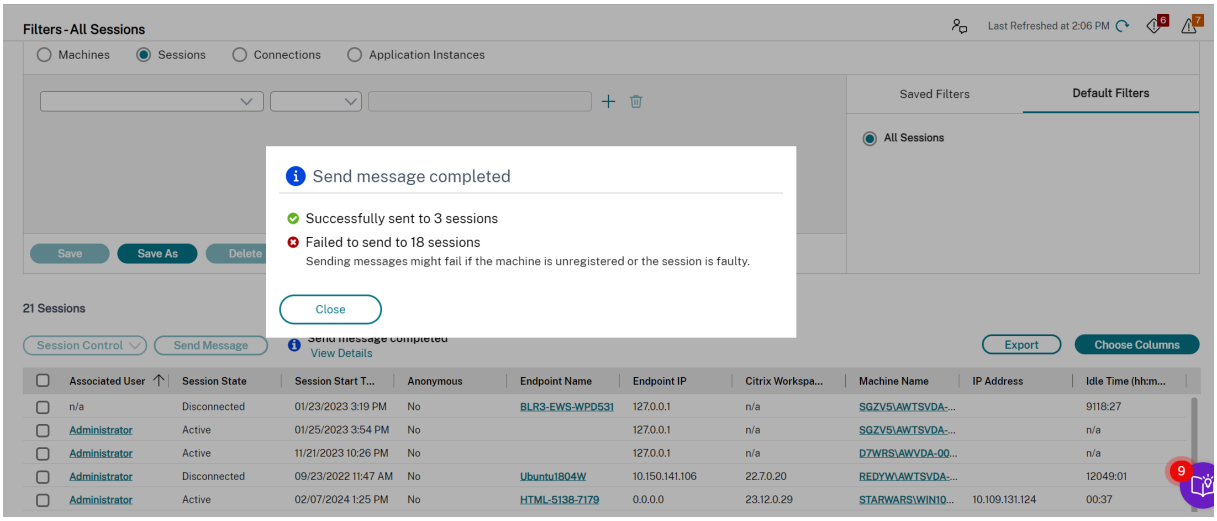
Envoyer des messages aux utilisateurs

January 25, 2024

À partir de l'onglet Surveiller, envoyez un message à un utilisateur qui est connecté à une ou plusieurs machines. Par exemple, 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.

Pour envoyer un message à un utilisateur, procédez comme suit :

1. Accédez à **Surveiller** > **Filtres** > **Machines** > **Toutes les machines**.
2. Sélectionnez une machine à laquelle vous souhaitez envoyer un message, puis cliquez sur **Envoyer un message**.
3. Tapez votre message et cliquez sur **Envoyer**.



L'envoi de messages peut échouer si les machines ne sont pas enregistrées ou si les sessions sont défectueuses.

Si le message est envoyé, un message de confirmation s'affiche dans l'onglet Surveiller. Si la machine de l'utilisateur est connectée, le message s'affiche.

Si le message n'a pas pu être envoyé, un message d'erreur s'affiche dans l'onglet Surveiller. Résoudre le problème en fonction du message d'erreur. Lorsque vous avez terminé, tapez le sujet et le texte du message, puis cliquez sur **Réessayer**.

Si vous choisissez d'envoyer des messages en masse à toutes les sessions connectées, la progression de l'opération s'affiche en pourcentage. Une fois l'opération terminée, le nombre de messages envoyés et le nombre d'échecs sont affichés. L'état d'envoi des messages s'avère particulièrement utile pour administrer des sites volumineux. Il vous permet de déterminer si le message doit être renvoyé à certains utilisateurs.

Résoudre les échecs applicatifs

February 16, 2023

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.

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.
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.

Désactiver la visibilité des applications en cours d'exécution

Par défaut, le Gestionnaire d'activités 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'activités. 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. Pour ce faire, sur le VDA, modifiez la clé de registre dans HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. 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.

> **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.

Restaurer les connexions aux bureaux

March 30, 2022

Dans l'onglet Surveiller, vérifiez l'état de connexion de l'utilisateur pour la machine actuelle 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. Redémarrer la machine de l'utilisateur	Sur la page Détails de l'utilisateur, assurez-vous que le mode maintenance est désactivé. Sélectionnez la machine et cliquez sur **Redémarrer**. Utilisez cette option si la machine de l'utilisateur ne répond pas ou ne parvient pas à se connecter, comme lorsque la machine utilise une quantité élevée de ressources UC, ce qui peut rendre le processeur inutilisable.

Restaurer les sessions

March 30, 2022

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.

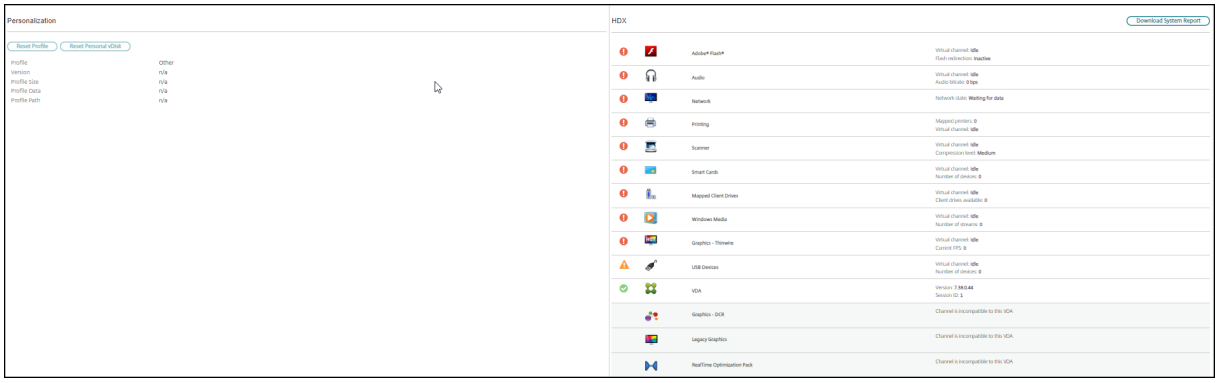
Action	Description
Arrêter les applications ou processus qui ne répondent pas	Cliquez sur l'onglet **Applications**. Sélectionnez toute application qui ne répond pas et cliquez sur **Arrêter l'application**. Sélectionnez également un processus correspondant qui ne répond pas et cliquez sur **Arrêter 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.
Fermer 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

November 24, 2023

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. Pour ce faire, dans le panneau HDX, cliquez sur **Télécharger le rapport système**.

Réinitialiser un profil utilisateur

April 27, 2022

> **Avertissement :**
>
> Si un profil est réinitialisé, bien que les dossiers et les fichiers de l'utilisateur soient enregistrés et copiés dans le nouveau profil, la plupart des données de profil utilisateur sont supprimées (par exemple, le Registre est réinitialisé et les paramètres d'application peuvent être supprimés).

1. À partir de l'onglet Surveiller, 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.

> **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. Ceci garantit que le profil approprié est réinitialisé. Pour un profil utilisateur Citrix, le profil est déjà réinitialisé lorsque le bureau de l'utilisateur s'affiche. Pour 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.

Les étapes précédentes supposent que vous utilisiez Citrix Virtual Desktops (VDA de bureau). 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.

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.

Les dossiers (et leurs fichiers) provenant du profil de l'utilisateur sont enregistrés et copiés vers le nouveau profil. Ils sont copiés dans l'ordre indiqué :

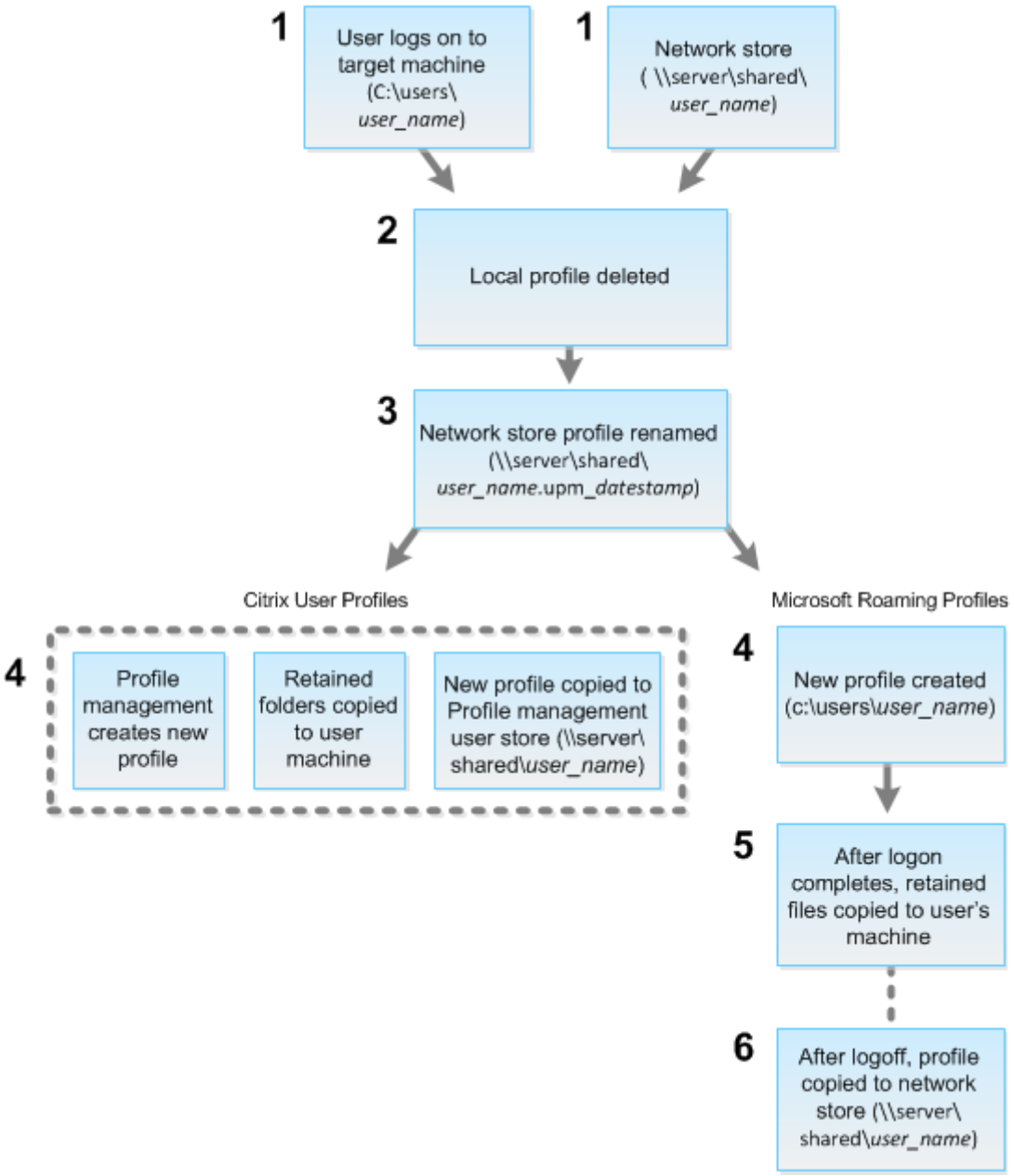
- Bureau
- Cookies
- Favoris
- Documents
- Images
- Musique
- Vidéos

> **Remarque :**
>
> Dans Windows 8 ou version ultérieure, les cookies ne sont pas copiés lorsque les profils sont réinitialisés.

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 l'onglet Surveiller ou en utilisant le kit de développement PowerShell), le service de surveillance identifie d'abord le profil utilisateur en cours d'utilisation et émet une commande de réinitialisation appropriée. Le service de surveillance 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 le service de surveillance 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 Profile Management traite l'utilisateur, 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 de Profile Management, et les dossiers sont copiés dans le profil réseau, et l'utilisateur peut ouvrir une session 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 nouveau 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 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.

Enregistrer des sessions

February 21, 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 Monitor. Cette fonctionnalité est disponible pour les clients de sites **Premium**.

Enregistrement de session dynamique

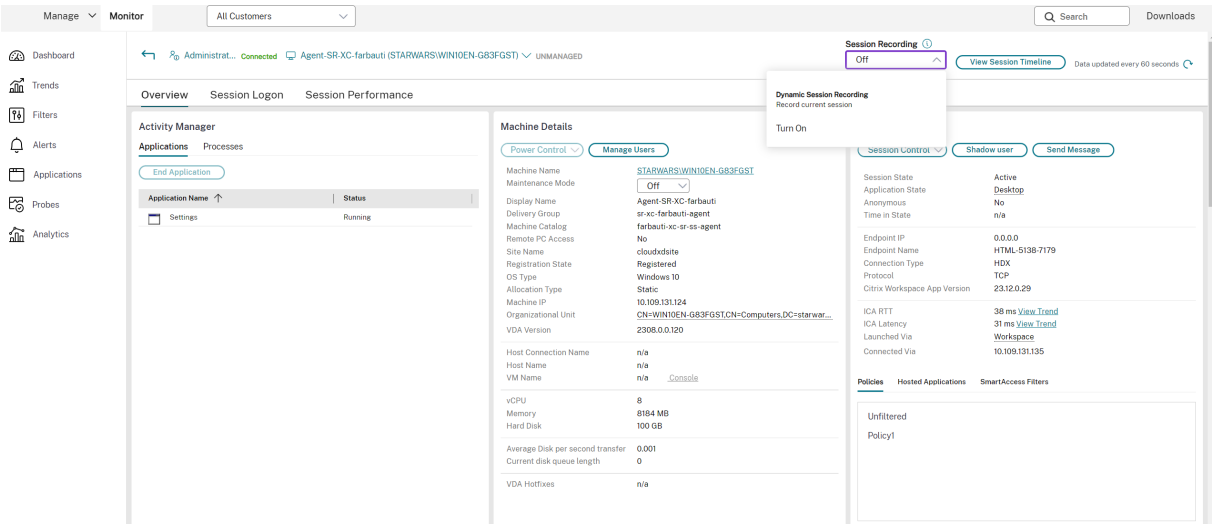
Vous pouvez enregistrer la session active en cours à l'aide des commandes d'enregistrement de session de l'écran **Détails de l'utilisateur**. Pour en savoir plus sur l'enregistrement dynamique de session, consultez l'article sur le service d'enregistrement de session.

Contrôles d'enregistrement de session dans Monitor

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.
- Désactiver : désactive l'enregistrement des sessions pour l'utilisateur.

Le panneau **Stratégies** affiche le nom de la stratégie d'enregistrement de session active.



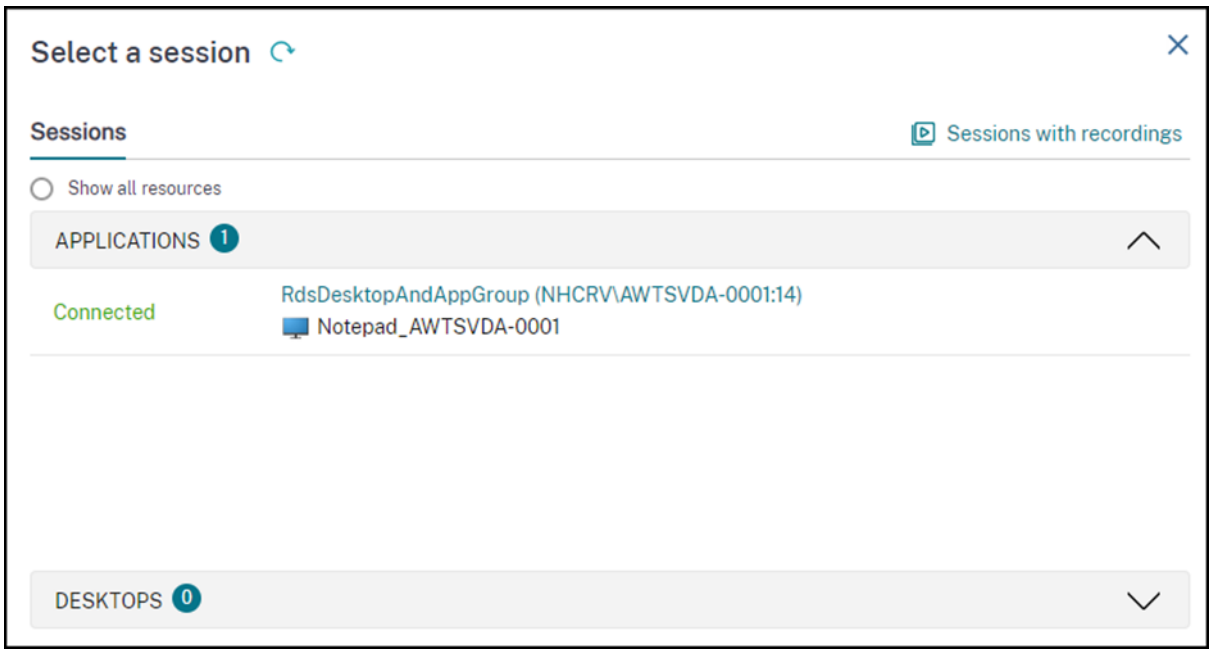
Le panneau **Détails de la machine** affiche l'état de la stratégie d'enregistrement de session pour la machine.

Visionnez les sessions en direct et enregistrées

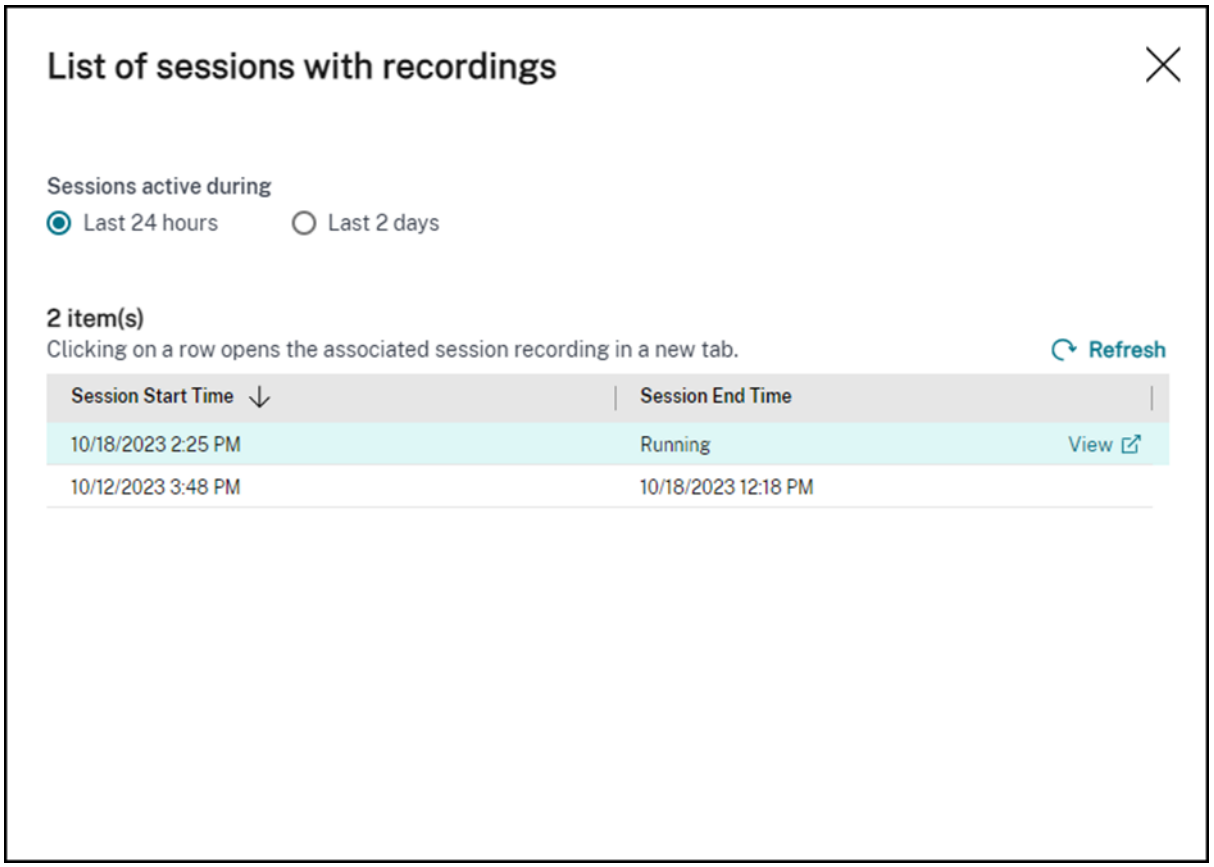
Vous pouvez visionner des sessions utilisateur enregistrées et en direct pour comprendre les problèmes rencontrés par l'utilisateur. Avec l'accès rapide aux enregistrements et aux mesures relatives aux sessions dans la console Monitor, vous n'avez plus besoin de rechercher les enregistrements sur plusieurs 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 le VDA et les serveurs d'enregistrement de session version 2308 ou ultérieure.

Monitor 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 12, 2024

Citrix Monitor prend en charge trois éditions du service Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service). Il s'agit de **Premium**, **Citrix DaaS Advanced** et **Citrix DaaS Advanced Plus**. Les fonctionnalités spécifiques de Citrix Monitor, les versions de VDA, les composants dépendants et leurs éditions de licence respectives sont répertoriés dans le tableau suivant.

Fonctionnalité	Dépendances - version min requise	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Utilisation du GPU en temps réel disponible pour les GPU AMD	VDA 7 2212 exécutant Windows 64 bits	Oui	Oui	Oui
Accès à Citrix Analytics for Performance - Détails de la session	Droits Citrix Analytics for Performance	Oui	Oui	Oui
Reconnexion automatique de session	VDA 1906	Oui	Oui	Oui
Durée du démarrage de session	VDA 1903	Oui	Oui	Oui
Analyse de bureaux	Citrix Probe Agent 1903	Oui	Non	Non

Fonctionnalité	Dépendances - version min requise	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Durée Citrix Profile Management dans Chargement du profil	VDA 1903	Oui	Oui	Oui
Détails du profil	VDA 1811	Oui	Oui	Oui
Surveillance des alertes d'hyperviseur	Aucune	Oui	Non	Non
Analyse d'application	Citrix Application Probe Agent 1811	Oui	Non	Non
Intégrité des licences Microsoft RDS	VDA 7.16	Oui	Oui	Oui
Accès à la console de la machine à partir de Surveiller	Hyperviseur XenServer 7.3	Oui	Oui	Oui
Exportation de données de filtres	Aucune	Oui	Oui	Oui
Détails de la session interactive	VDA 1808	Oui	Oui	Oui
Détails GPO	VDA 1808	Oui	Oui	Oui
Données historiques de machine disponibles à l'aide de l'API OData	Aucune	Oui	Oui	Oui
Stratégies d'alertes intelligentes	Aucune	Oui	Non	Non

Fonctionnalité	Dépendances - version min requise	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Lien Health Assistant	Aucune	Oui	Oui	Oui
Détails de la session interactive	Aucune	Oui	Oui	Oui
Analyse des applications	VDA 7.15	Oui	Oui	Oui
OData API V.4	Aucune	Oui	Oui	Oui
Observation des utilisateurs VDA Linux	VDA 7.16	Oui	Oui	Oui
Accès à la console machine	Aucune	Oui	Oui	Oui
Détection des défaillances applicatives	VDA 7.15	Oui	Oui	Oui
Résolution des problèmes centrée sur les applications	VDA 7.13	Oui	Oui	Oui
Contrôle des disques	VDA 7.14	Oui	Oui	Oui
Suivi GPU	VDA 7.14	Oui	Oui	Oui
Protocole de transport sur le panneau Détails de la session	VDA 7.13	Oui	Oui	Oui
Descriptions claires des échecs de connexion et de machine	VDA 7.x	Oui	Oui	Oui

Fonctionnalité	Dépendances - version min requise	Premium	Citrix DaaS Advanced	Citrix DaaS Advanced Plus
Rétention des données d'historique	VDA 7.x	Oui	Non	Non
Rapports personnalisés	VDA 7.x	Oui	Non	Non
Rapports d'utilisation des ressources	VDA 7.11	Oui	Oui	Oui
Alertes étendues pour les conditions CPU, mémoire et RTT ICA	VDA 7.11	Oui	Non	Non
Amélioration de l'exportation des rapports	VDA 7.x	Oui	Oui	Oui
Répartition de la durée d'ouverture de session	VDA 7.x	Oui	Oui	Oui
Analyse et alertes proactives	VDA 7.x	Oui	Non	Non
Utilisation d'applications hébergées	VDA 7.x	Oui	Non	Non
Utilisation des OS mono-session et multi-session	VDA 7.x	Oui	Non	Non
Prise en charge du canal virtuel Framehawk	VDA 7.6	Oui	Oui	Oui

Administration déléguée et surveillance

March 30, 2022

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.

Les permissions d'administration déterminent l'interface de surveillance 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.

La surveillance prend désormais en charge les rôles d'administrateur délégué qui vous permettent d'attribuer des rôles personnalisés ou intégrés aux administrateurs. Le rôle détermine les autorisations disponibles et donc la manière dont un administrateur utilise la surveillance. Vous pouvez également définir l'étendue applicable à ces rôles. L'étendue définit les objets pour lesquels le rôle est applicable.

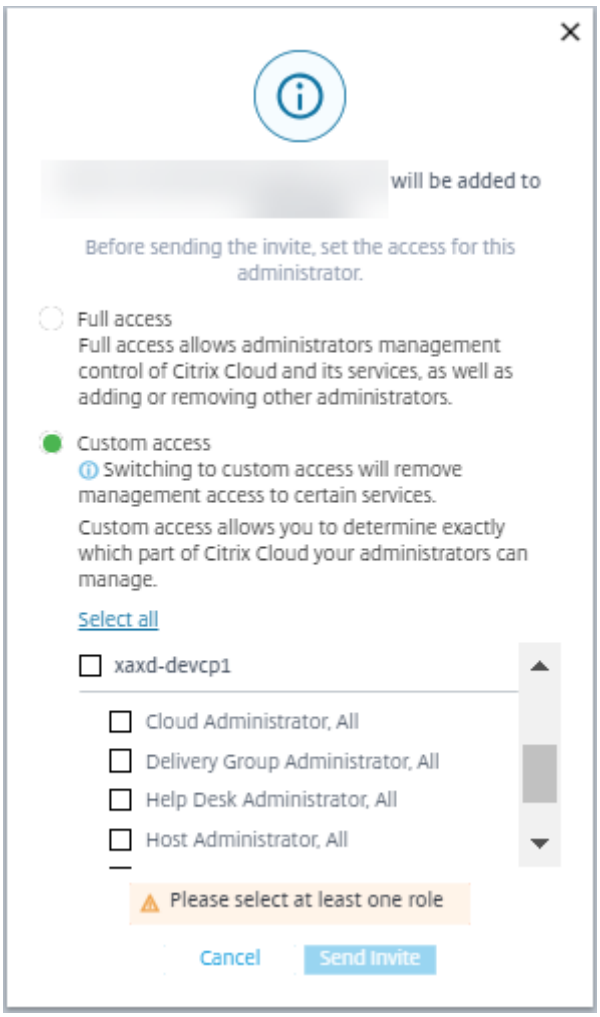
Pour de plus amples informations sur la création d'administrateurs délégués, veuillez consulter l'article Administration déléguée.

Les rôles et les permissions intégrés déterminent la manière dont les administrateurs utilisent la fonctionnalité **Surveiller** :

Rôle d'administrateur	Autorisations dans l'onglet Surveiller
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	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.

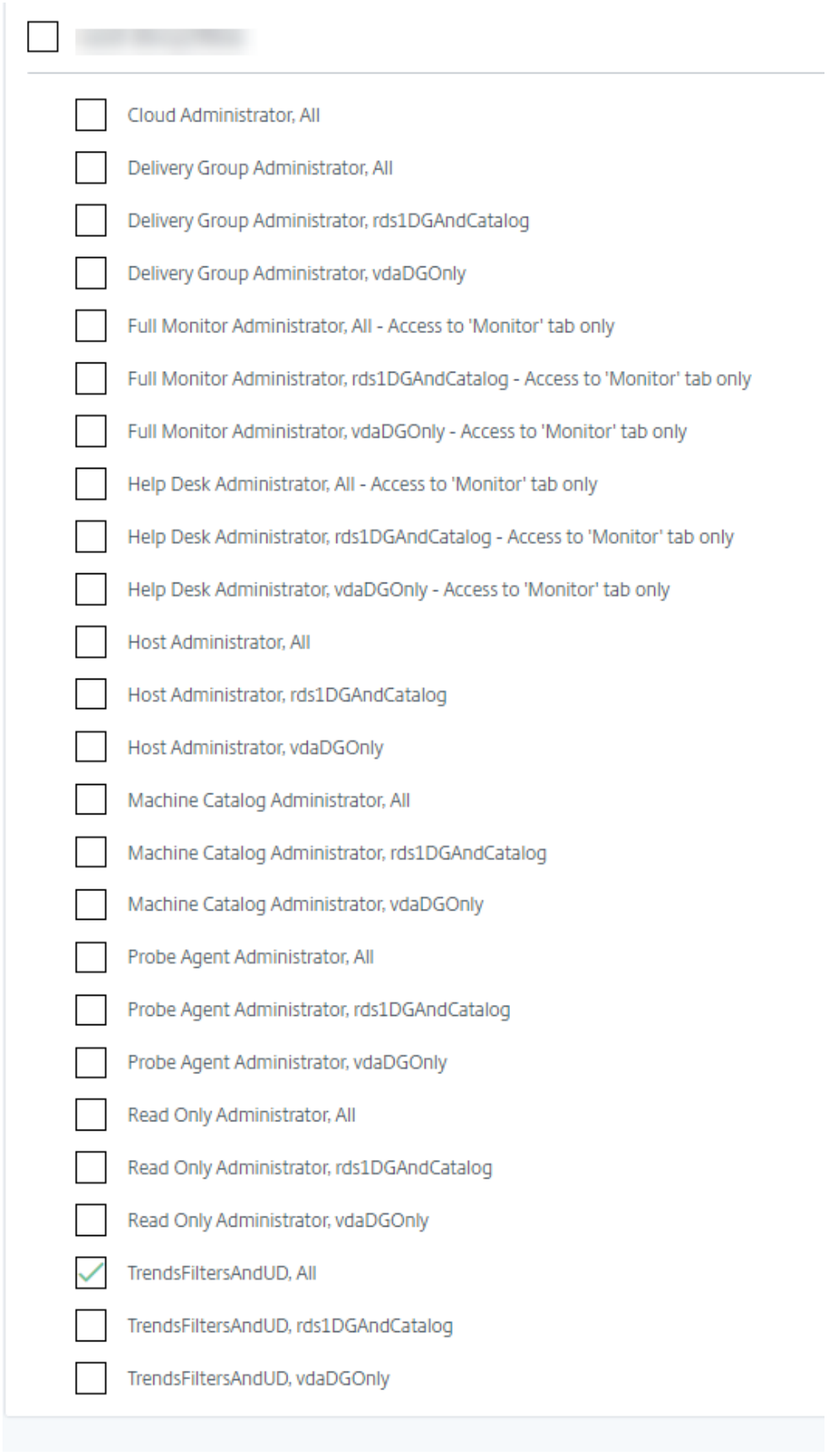
Rôle d'administrateur	Autorisations dans l'onglet Surveiller
Administrateur en lecture seule	Peut accéder à toutes les vues et afficher tous les objets dans les étendues spécifiées en plus des informations globales. Peut télécharger des rapports à partir de canaux HDX et peut exporter les données de 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 support technique	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 d'hôte	Aucun accès. Cet administrateur n'est pas pris en charge pour l'onglet Surveiller et ne peut pas afficher les données.
Administrateur Probe Agent	Accès en lecture seule à la page Applications, ne peut accéder à aucune autre vue. Destiné spécifiquement à exécuter Citrix Probe Agent sur les machines de point de terminaison.
Administrateur complet de surveillance	Accès complet à toutes les vues et commandes de l'onglet **Surveiller**
Session Administrator	Permet d'afficher les groupes de mise à disposition et de gérer leurs sessions et machines associées sur la page **Filtres** de l'onglet **Surveiller**.

Pour attribuer un rôle (intégré ou personnalisé) à un utilisateur, à partir du menu Citrix Cloud, accédez à **Gestion des identités et des accès** > **Administrateurs**. Lorsque vous ajoutez ou modifiez l'accès d'un administrateur à partir de cette section, vous pouvez sélectionner **Accès personnalisé** et l'un des rôles répertoriés.



Vous pouvez définir des rôles et des étendues personnalisés dans **Configuration complète > Administrateurs > Administrateurs**.

Les rôles intégrés et les rôles personnalisés sont répertoriés pour la sélection avec étendue personnalisée.



Granularité de données et rétention

January 20, 2023

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. Récupérez les valeurs minimales et maximales de SummaryDate pour une table de synthèse particulière pour déterminer le premier et le dernier intervalle d'agrégation pour une granularité de données 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 de synthèse des données brutes doit prendre en compte le fait qu'aucune donnée de synthèse pour les intervalles partiels susceptibles de se produire ou pour le début et la fin de la période de temps.
- **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 existe des espaces dans les données de synthèse du nombre de connexions actives, mais les instances de session sont 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 le service Monitor est une fonction de la période de temps (T) demandée. Les règles sont les suivantes :

- 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. Cela garantit de meilleures performances tout en conservant la granularité nécessaire pour la création de rapports.

	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

	Nom du paramètre	Nettoyage affecté	Jours de rétention pour Premium	Jours de rétention pour Advanced
4	GroomDeletedRetentionDays	Les entités Machine, Catalog, DesktopGroup et Hypervisor qui possèdent un LifecycleState « Supprimé ». Cette opération supprime également tout enregistrement Session, SessionDetail, Summary, Failure ou LoadIndex.	90	31
5	GroomSummariesRetentionDays	Enregistrements Desktop-GroupSummary, FailureLogSummary et LoadIndexSummary. Données agrégées : granularité quotidienne.	365	31

	Nom du paramètre	Nettoyage affecté	Jours de rétention pour Premium	Jours de rétention pour Advanced
6	GroomMachineHotfixLogRetentionDays	Correctifs à chaud appliquées aux machines VDA et Controller	90	31
7	GroomHourlyRetentionDays	Données agrégées : granularité horaire	32	31
8	GroomApplicationInstanceRetentionDays	Historique des instances d'application	90	Sans objet
9	GroomNotificationLogRetentionDays	Enregistrements de journal de notification	90	Sans objet
10	GroomResourceUsageRawDataRetentionDays	Données brutes d'utilisation des ressources : données brutes	2	3
11	GroomResourceUsageHourlyDataRetentionDays	Données de synthèse d'utilisation des ressources : granularité par heure	30	30
12	GroomResourceUsageDailyDataRetentionDays	Données de synthèse d'utilisation des ressources : granularité par jour	365	31

	Nom du paramètre	Nettoyage affecté	Jours de rétention pour Premium	Jours de rétention pour Advanced
13	GroomProcessUsageRawDataRetentionDays	Agent d'utilisation des processus : données brutes	1	1
14	GroomProcessUsageHourDataRetentionDays	Agent d'utilisation des processus : granularité par heure	7	7
15	GroomProcessUsageDayDataRetentionDays	Agent d'utilisation des processus : granularité par jour	30	30
16	GroomSessionMetricsDataRetentionDays	Données de mesure de session	1	1
17	GroomMachineMetricsDataRetentionDays	Données de mesure de machine	3	3
18	GroomMachineMetricsSummaryDataRetentionDays	Données de synthèse de mesure de machine	365	31
19	GroomApplicationErrorsRetentionDays	Données d'erreur d'application	1	1
20	GroomApplicationFailuresRetentionDays	Données d'échec d'application	1	1

> **Attention :**
>
> Vous ne pouvez pas modifier les valeurs de la base de données Monitoring du service.

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.** Ce sont les 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.

Diagnostic de lancement de session

March 30, 2024

> **Remarque :**
>
> Les diagnostics de lancement de session sont actuellement en version préliminaire.

Les lancements de session impliquent plusieurs composants Citrix. Pour diagnostiquer les échecs de lancement de session, utilisez Citrix Monitor (c'est-à-dire le service Citrix Director) pour cibler le composant et l'étape exacts où le problème s'est produit. Appliquez les actions recommandées pour résoudre le problème. L'application Citrix Workspace génère un ID de transaction à 32 chiffres (8-4-4-4-12) qui peut être utilisé pour diagnostiquer les échecs de lancement de session.

> **Remarque :**
>
> Cette fonctionnalité n'est disponible que pour les clients cloud des États-Unis, de l'AP-S et de l'UE. Elle n'est pas disponible au Japon et dans les régions gouvernementales.

Pré-requis

Si vous utilisez Citrix DaaS, l'intégration est automatique. Les clients cloud qui utilisent un magasin StoreFront local doivent s'assurer qu'une version de StoreFront prise en charge est intégrée.

- Si vous utilisez Citrix Analytics for Performance, consultez Sources de données pour connaître les étapes à suivre pour intégrer StoreFront sur site.
- Si vous n'utilisez pas Citrix Analytics for Performance :

  1. Accédez à `https://analytics.cloud.com/unified-datasources/perf/Citrix%20Virtual%20Apps%20and%20Desktops/site-details`.
  2. Cliquez sur **Connect to StoreFront deployment**, entrez les détails et téléchargez le fichier de configuration. Pour plus d'informations, consultez Intégration de sites locaux à l'aide de StoreFront.

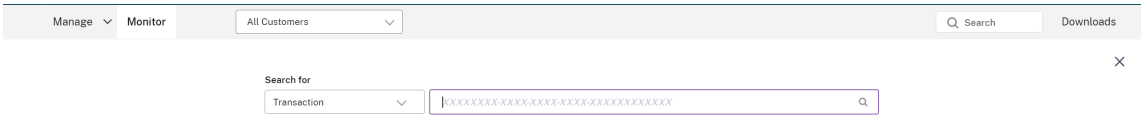
  > **Remarque :**
  >
  > Les administrateurs ayant le rôle Administrateur cloud sont autorisés à intégrer les déploiements StoreFront, tandis que les administrateurs ayant le rôle Administrateur de moniteur complet peuvent uniquement consulter les déploiements StoreFront.

Les versions minimales prises en charge des autres composants sont les suivantes :

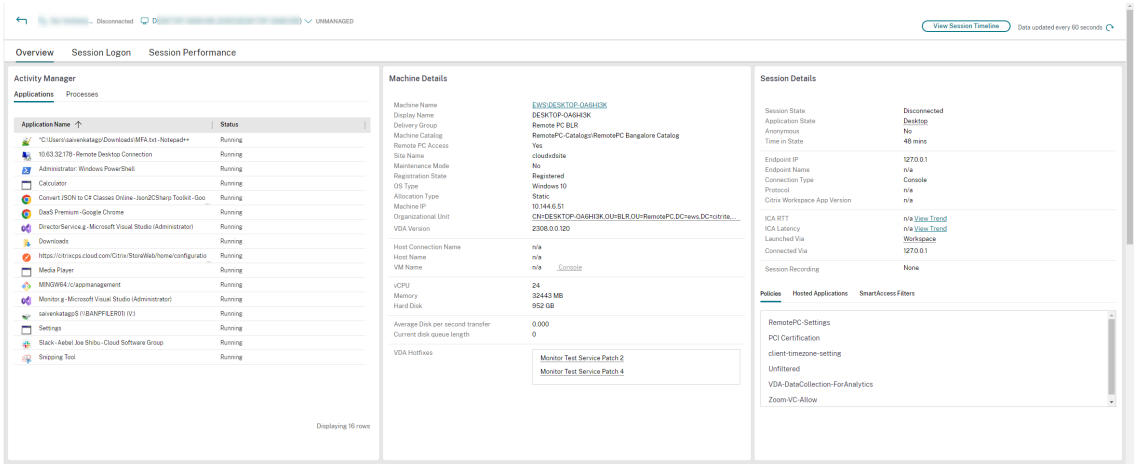
- Application Citrix Workspace pour Windows 2109
- Application Citrix Workspace pour Mac 2112
- Application Citrix Workspace pour Linux 2112
- Application Citrix Workspace pour HTML5 2110
- Application Citrix Workspace pour Chrome 2110
- Application Citrix Workspace pour Android 2110
- Version du VDA Citrix Virtual Apps and Desktops 2112
- Citrix StoreFront 1912 LTSR CU4

Étapes pour diagnostiquer l'échec du lancement de session

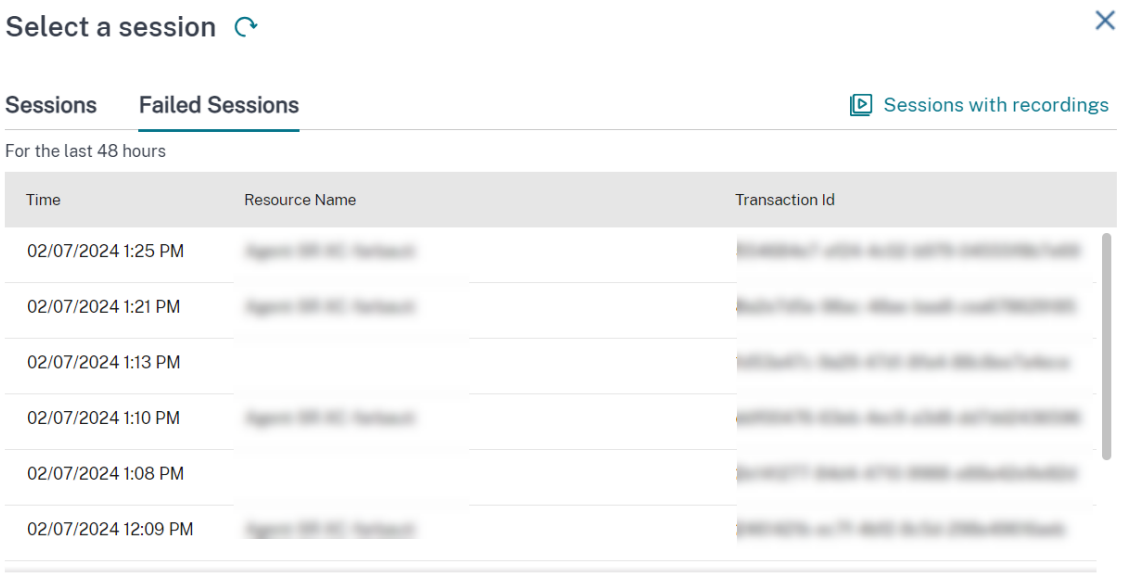
1. Copiez l'ID de transaction du lancement de session ayant échoué à partir de l'application Citrix Workspace.
2. Dans l'interface utilisateur de Monitor, recherchez l'ID de transaction à 32 chiffres et cliquez sur **Détails**.



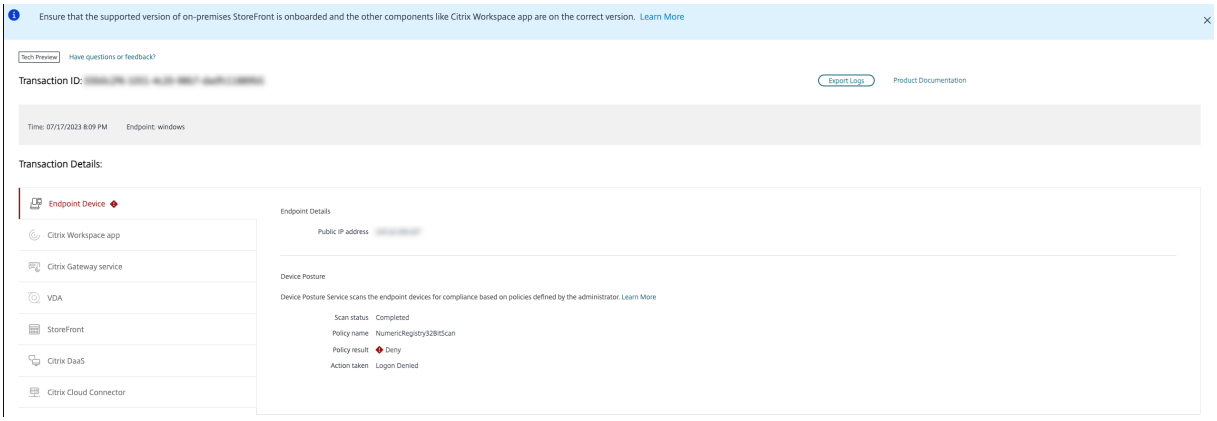
3. Si l'ID de transaction n'est pas disponible, effectuez une recherche à l'aide du nom d'utilisateur. Le gestionnaire d'activités de l'utilisateur s'affiche.



4. Cliquez sur le sélecteur de session. Accédez à l'onglet **Sessions ayant échoué**. La liste des sessions qui ont échoué au cours des dernières 48 heures s'affiche. Cliquez sur la session sélectionnée.



5. Citrix Monitor affiche des informations clés concernant la transaction, telles que le nom d'utilisateur, l'horodatage et l'application ou le bureau sur lequel l'échec s'est produit.
6. Le panneau Détails de la transaction contient une liste de composants indiquant l'occurrence de l'échec.
7. Cliquez sur **Machine de point de terminaison** dans la liste des composants pour afficher l'état de l'analyse de l'état de l'appareil. Le service de détermination de l'état de l'appareil analyse la machine de point de terminaison à des fins de vérification de conformité en fonction des stratégies définies par l'administrateur.



L'état de l'analyse, le nom de la stratégie, le résultat de la stratégie et l'action entreprise sont affichés. Assurez-vous que le service de détermination de l'état de l'appareil est configuré avec DaaS, comme le décrit l'article sur les états de l'appareil. Les erreurs enregistrées par l'état de l'appareil sont décrites dans les journaux des erreurs enregistrées au niveau de l'état de l'appareil.

1. Cliquez sur le nom d'un autre composant pour vérifier les champs Détails du composant et Détails de la dernière défaillance connue.
2. Les champs Raison de l'échec et Code d'erreur s'affichent. Cliquez sur le lien **En savoir plus sur l'erreur** pour afficher le code d'erreur spécifique dans la section Codes d'erreur qui contient la description détaillée et l'action recommandée.
3. Vous pouvez exporter les journaux pour les consulter. Le fichier journal répertorie les étapes de lancement de session dans l'ordre chronologique et indique le composant exact et le stade où l'échec s'est produit.
4. Si plusieurs échecs se sont produits sur les composants, seuls les détails du dernier échec connu sont affichés sur la page Transaction. Les journaux exportés contiennent les détails de tous les échecs liés à la transaction.

> **Remarque :**
>
> Les codes d'erreur et les informations de diagnostic côté client ne sont disponibles que lorsque Citrix StoreFront est intégré et envoie des données. Pour plus d'informations sur l'intégration de StoreFront, consultez la section Conditions préalables.

Agent Broker

bka.prepare.session.failure.validation

- Description : échec de la validation de la demande de préparation de session.
- Action recommandée : réessayez. Si l'échec se répète, vérifiez que les connecteurs se trouvent dans un état d'intégrité normal.

bka.prepare.session.failure.rejected

- Description : le VDA ne peut pas accepter la demande de lancement.
- Action recommandée : redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.

bka.hdx.prepare.failure.general

- Description : échec de préparation HDX.
- Action recommandée : redémarrez le VDA.

bka.hdx.validate.failure.ticket_not_found

- Description : le ticket référencé ou le lancement ne figurent pas dans le cache de lancement.
- Action recommandée : assurez-vous que le VDA peut communiquer avec le connecteur.

bka.ticketing.validate.failure.unlicensed

- Description : impossible de vérifier la licence pour le lancement.
- Action recommandée : contactez le support Citrix.

bka.ticketing.validate.failure.general

- Description : échec générique lors de la validation d'un ticket.
- Action recommandée : collectez les journaux sur le VDA et contactez le support Citrix.

bka.set.configuration.failure.policy

- Description : une erreur s'est produite lors de la définition des stratégies.
- Action recommandée : redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.

bka.set.configuration.failure

- Description : une erreur s'est produite lors de la configuration des paramètres.
- Action recommandée : redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.

Broker

brk.validate.credentials.failure.invalid

- Description : échec de la validation des informations d'identification en raison d'un problème. La raison peut être développée dans le paramètre du message.
- Action recommandée : réessayez. Si l'échec se répète, vérifiez que les connecteurs se trouvent dans un état d'intégrité normal.

brk.resolve.machine.failure.general

- Description : échec de l'énumération ou de la résolution du nœud de calcul (worker). La raison peut être développée dans le paramètre du message.
- Action recommandée : assurez-vous que les machines capables de lancer cette application sont enregistrées auprès du broker. Assurez-vous que toutes les machines disponibles n'ont pas atteint leur capacité.

brk.license.check.failure.constraints

- Description : les contraintes de licence ont fait échouer le lancement de session.
- Action recommandée : assurez-vous que des licences sont disponibles pour ce type d'application ou de bureau.

brk.resolve.machine.failure.timeout

- Description : le broker a expiré lors du contact avec la base de données.
- Action recommandée : problèmes de communication avec la base de données du site. Contactez le support Citrix.

brk.poweron.forlaunch.queued.failure.general

- Description : l'action d'alimentation placée en file d'attente a échoué.
- Action recommandée : problèmes de communication avec la base de données du site. Contactez le support Citrix.

brk.set.configuration.failure.general

- Description : erreur non spécifiée lors de la définition de la configuration sur le VDA cible.

- Action recommandée : redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.

brk.prepare.session.failure.host_unreachable

- Description : échec de communication avec le VDA.
- Action recommandée : redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.

brk.prepare.session.failure.general

- Description : échec de la préparation de la session sur le VDA, erreurs UnsupportedClientType ou ConnectionRefused.
- Action recommandée : redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.

brk.validate.ticket.failure.license

- Description : échec de récupération d'une licence valide pour cette session.
- Action recommandée : vérifiez l'état d'intégrité du site et assurez-vous que tous les connecteurs et le Citrix DDC sont opérationnels.

brk.validate.ticket.failure.general

- Description : appel de création de tickets non valide.
- Action recommandée : contactez le support Citrix.

brk.reverse.prepare.failure.general

- Description : échec générique lors du lancement de la session.
- Action recommandée : vérifiez l'état d'intégrité du site et assurez-vous que tous les connecteurs et le Citrix DDC sont opérationnels.

brk.reverse.prepare.failure.lease_revoked

- Description : la location de cette session a été révoquée.
- Action recommandée : réessayez. Si l'échec se répète, vérifiez que les connecteurs se trouvent dans un état d'intégrité normal.

brk.reverse.prepare.failure.resource_unavailable

- Description : la ressource est déjà utilisée ou est temporairement indisponible.
- Action recommandée : réessayez. Si l'échec se répète, vérifiez que les connecteurs se trouvent dans un état d'intégrité normal.

brk.reverse.prepare.failure.app_protection

- Description : la protection des applications est manquante et est requise pour cette session.
- Action recommandée : assurez-vous que la protection des applications est activée sur ce VDA ou supprimez cette exigence de l'application.

HDX VDA Linux

VDA_LINUX_ERR_RECONNECT_PRE_LOGOFF

- Description : la reconnexion à une session en état de pré-fermeture de session n'est pas autorisée.
- Action recommandée : réessayez de lancer la session plus tard. Cela permet à la session de se fermer.

VDA_LINUX_ERR_RECONNECT_NO_SESSION

- Description : reconnexion à une session qui n'est pas en cours de fermeture.
- Action recommandée : réessayez de lancer la session plus tard. En cas d'échec, contactez le support Citrix.

VDA_LINUX_ERR_SAME_KEY

- Description : préparation d'une connexion (il existe une session existante avec la même clé de session).
- Action recommandée : contactez le support Citrix.

VDA_LINUX_ERR_GET_FQDN

- Description : échec d'obtention du nom de domaine complet de ce VDA.
- Action recommandée : vérifiez que la configuration DNS sur le VDA est correcte

VDA_LINUX_ERR_NO_CGP_LISTENER

- Description : aucun écouteur CGP n'est en cours d'exécution.
- Action recommandée : vérifiez que la stratégie **Connexions de fiabilité de session** est activée. Vérifiez que l'écouteur CGP écoute le port attendu dans le VDA (le port par défaut est 2598 et peut être modifié via la stratégie **Numéro de port de la fiabilité de session**).

VDA_LINUX_ERR_DTLS_CONNECT

- Description : échec de l'établissement d'une connexion DTLS au service Gateway.
- Action recommandée : vérifiez que le nom de domaine complet de Citrix Gateway Service est accessible à partir du VDA. Vérifiez que le chemin `/var/xdl/keystore/cacerts` existe dans le VDA. Supprimez `/var/xdl/keystore` et exécutez `/var/xdl/split_ca_bundle.sh` pour régénérer les certificats d'autorité de certification. Vérifiez que le nom de domaine complet de Gateway Service est approuvé par le VDA.

VDA_LINUX_ERR_ACCEPT_EDT_CONNECT

- Description : échec de l'acceptation de la négociation EDT du client.
- Action recommandée : contactez le support Citrix.

VDA_LINUX_ERR_TCP_CONNECT

- Description : échec de l'établissement d'une connexion TCP à Gateway Service.
- Action recommandée : vérifiez que le nom de domaine complet de Citrix Gateway Service est accessible à partir du VDA.

VDA_LINUX_ERR_TLS_CONNECT

- Description : échec de l'établissement d'une négociation TLS vers Gateway Service
- Action recommandée : vérifiez que le chemin `/var/xdl/keystore/cacerts` existe dans le VDA. Supprimez `/var/xdl/keystore` et exécutez `/var/xdl/split_ca_bundle.sh` pour régénérer les certificats d'autorité de certification. Vérifiez que le nom de domaine complet de Gateway Service est approuvé.

VDA_LINUX_ERR_RDVZ_HANDSHAKE

- Description : échec de l'établissement de la négociation de Rendez-vous avec Gateway Service.
- Action recommandée : contactez le support Citrix.

VDA_LINUX_ERR_ACCEPT_ICA_CONNECT

- Description : échec de l'acceptation d'une connexion ICA.
- Action recommandée : contactez le support Citrix.

VDA_LINUX_ERR_RECONNECT_TO_ANON_SESSION_NOT_ALLOWED

- Description : la reconnexion à une session anonyme n'est pas autorisée.
- Action recommandée : contactez le support Citrix.

VDA_LINUX_ERR_CONN_NOT_ALLOWED

- Description : la connexion n'est pas autorisée.
- Action recommandée : si le code de résultat est 3, vérifiez que la licence n'a pas expiré ; sinon, réessayez de lancer la session plus tard. Si vous ne parvenez pas à résoudre ce problème, contactez le support Citrix.

VDA_LINUX_ERR_CONN_GENERAL

- Description : échec de validation de la connexion.
- Action recommandée : contactez le support Citrix.

VDA_LINUX_ERR_USER_CANCELLED_LOGIN

- Description : l'utilisateur final a annulé l'ouverture de session.
- Action recommandée : cette erreur est attendue lorsque l'authentification unique (SSO) est désactivée et que l'utilisateur clique sur le bouton « Annuler » dans la boîte de connexion ; sinon, contactez le support Citrix.

VDA_LINUX_ERR_GET_TARGET

- Description : échec de l'obtention de la session cible.
- Action recommandée : contactez le support Citrix.

VDA_LINUX_ERR_START_LOGON_TIMERS

- Description : échec du démarrage des horloges d'ouverture de session.
- Action recommandée : contactez le support Citrix.

VDA_LINUX_ERR_SEND_CMD_TO_TARGET

- Description : échec de l'envoi de la commande à la session cible.
- Action recommandée : contactez le support Citrix.

VDA_LINUX_ERR_POST_RECONNECT_EVENT

- Description : échec de publication d'un événement de reconnexion.
- Action recommandée : contactez le support Citrix.

VDA_LINUX_ERR_RECONNECT_TIMEOUT

- Description : reconnexion après le délai d'expiration de la session utilisateur.
- Action recommandée : contactez le support Citrix.

HDX VDA Windows

RENDEZVOUS_CONNECT_FAILED_TCP

- Description : une tentative de connexion sortante du transport Rendezvous via TCP a échoué.
- Action recommandée : des échecs sporadiques peuvent survenir en raison de mauvaises conditions du réseau. Il s'agit du comportement attendu. Vérifiez la configuration du VDA si cela se produit fréquemment, puis contactez le support Citrix.

RENDEZVOUS_CONNECT_FAILED_EDT

- Description : une tentative de connexion sortante du transport Rendezvous via TCP a échoué.
- Action recommandée : des échecs sporadiques peuvent survenir en raison de mauvaises conditions du réseau. Il s'agit du comportement attendu. Vérifiez la configuration du VDA si cela se produit fréquemment, puis contactez le support Citrix.

RENDEZVOUS_CONNECT_FAILED_PROXY

- Description : une tentative de connexion sortante du transport Rendezvous a échoué en raison d'une configuration de proxy non valide.
- Action recommandée : vérifiez la configuration du proxy Rendez-vous. Contactez le support Citrix.

RENDEZVOUS_CONNECT_FAILED_DTLS

- Description : une tentative de connexion sortante du transport Rendezvous a échoué en raison de l'échec de la négociation de transport sécurisé.
- Action recommandée : vérifiez la configuration de Rendez-vous et la configuration cryptographique. Contactez le support Citrix.

RENDEZVOUS_CONNECT_FAILED_TLS

- Description : une tentative de connexion sortante du transport Rendezvous a échoué en raison de l'échec de la négociation de transport sécurisé.
- Action recommandée : vérifiez la configuration de Rendez-vous, la configuration cryptographique et contactez le support Citrix.

RENDEZVOUS_CONNECT_FAILED_CGP

- Description : une tentative de connexion sortante du transport Rendezvous a échoué en raison d'un problème de configuration CGP.
- Action recommandée : vérifiez que le CGP (fiabilité de session) est activé et que les ports CGP sont écoutés. Contactez le support Citrix.

CGP_SR_SUSPEND_RESUME_FAILED_TIMEOUT

- Description : l'interruption du réseau n'a pas été résolue en raison du délai d'expiration ; la fiabilité de session n'a pas pu reprendre la connexion.
- Action recommandée : des échecs sporadiques peuvent survenir en raison de mauvaises conditions du réseau. Il s'agit du comportement attendu.

CGP_SR_SUSPEND_RESUME_FAILED

- Description : l'interruption du réseau n'a pas été résolue en raison d'une erreur imprévue ; la fiabilité de session n'a pas pu reprendre la connexion.
- Action recommandée : des échecs sporadiques peuvent survenir en raison de mauvaises conditions du réseau. Il s'agit du comportement attendu.

PREPARE_RECONNECT_REJECTED

- Description : le VDA a rejeté une demande de reconnexion provenant d'une connexion ICA entrante en raison d'une clé de session non valide.

- Action recommandée : vérifiez la configuration du VDA. Contactez le support Citrix.

Error: PREPARE_REJECTED

- Description : le VDA a rejeté une demande de connexion provenant d'une connexion ICA entrante en raison d'une clé de session non valide.
- Action recommandée : vérifiez la configuration du VDA. Contactez le support Citrix.

PREPARE_LISTENING_FAILED

- Description : le VDA n'a pas réussi à démarrer les écouteurs pour la connexion ICA entrante.
- Action recommandée : vérifiez la configuration réseau ; vérifiez que les ports d'écoute ne sont pas utilisés par d'autres applications ; contactez le support Citrix.

RENDEZVOUSCONNECTIONREQ_FAILED

- Description : le VDA n'a pas réussi à demander à la pile ICA de démarrer une connexion Rendezvous sortante.
- Action recommandée : vérifiez la configuration de Rendezvous ; vérifiez la configuration du proxy Rendezvous ; vérifiez la configuration CGP (fiabilité de session) ; contactez le support Citrix.

RENDEZVOUSCONNECTIONREQ_FAILED_PROXYCONFIG

- Description : le VDA n'a pas réussi à demander à la pile ICA de démarrer une connexion Rendezvous sortante en raison d'une erreur de configuration du proxy.
- Action recommandée : vérifiez la configuration du proxy Rendez-vous. Contactez le support Citrix.

ESTABLISH_SESSION_FAILED

- Description : le VDA n'a pas réussi à créer une session pour la connexion ICA entrante ou n'a pas réussi à se connecter à une session existante.
- Action recommandée : contactez le support Citrix.

ICA_ESTABLISH_FAILED

- Description : les connexions ICA sont acceptées ou la négociation a échoué.
- Action recommandée : contactez le support Citrix.

VALIDATE_FAILED

- Description : le broker n'a pas réussi à valider une demande de connexion ICA entrante provenant du VDA.
- Action recommandée : contactez le support Citrix.

VALIDATE_TICKETING_FAILED

- Description : le broker n'a pas réussi à valider une demande de connexion ICA entrante provenant du VDA en raison d'un problème de ticket.
- Action recommandée : contactez le support Citrix.

MCS

brk.poweron.forlaunch.execution.generalfailure

- Description : erreurs générales.
- Action recommandée : contactez le support Citrix.

brk.poweron.forlaunch.execution.insufficientresourcefailure

- Description : une opération d'hyperviseur ne peut pas être effectuée en raison de ressources insuffisantes sur l'hyperviseur.
- Action recommandée : vérifiez le quota de ressources dans l'hyperviseur. Si vous ne trouvez pas de solution, contactez le support Citrix.

brk.poweron.forlaunch.execution.nosuchmanagedmachine

- Description : il n'existe pas d'identifiant de machine.
- Action recommandée : vérifiez l'ID de la machine dans l'hyperviseur. Si vous ne trouvez pas de solution, contactez le support Citrix.

brk.poweron.forlaunch.execution.hypervisorconnectionfailure

- Description : impossible d'établir une connexion à l'hyperviseur. Par exemple, l'adresse de l'infrastructure d'hébergement n'a pas été trouvée.
- Action recommandée : vérifiez que l'adresse de l'infrastructure d'hébergement est correcte. Si vous ne trouvez pas de solution, contactez le support Citrix.

brk.poweron.forlaunch.execution.invalidcredentialsfailure

- Description : informations d'identification non valides.
- Action recommandée : vérifiez les informations d'identification pour la connexion à l'hyperviseur. Si vous ne trouvez pas de solution, contactez le support Citrix.

brk.poweron.forlaunch.execution.authorizationfailure

- Description : privilèges ou informations d'identification insuffisant(e)s.
- Action recommandée : vérifiez l'autorisation attribuée aux informations d'identification pour la connexion à l'hyperviseur. Si vous ne trouvez pas de solution, contactez le support Citrix.

brk.poweron.forlaunch.execution.sslcertauthfailure

- Description : une connexion ne peut pas être établie en raison d'un problème d'authentification SSL.
- Action recommandée : vérifiez le certificat de connexion de l'hyperviseur. Si vous ne trouvez pas de solution, contactez le support Citrix.

brk.poweron.forlaunch.execution.ratelimitedfailure

- Description : la connexion cloud indique qu'elle limite le débit.
- Action recommandée : réessayez la connexion ultérieurement si la demande est bloquée par la limitation de débit de l'hyperviseur. Si vous ne trouvez pas de solution, contactez le support Citrix.

brk.poweron.forlaunch.execution.connectorconnectionfailure

- Description : des erreurs existent sur le Cloud Connector. Par exemple, un délai d'expiration se produit lors de l'attente de la connexion. Une fois le délai d'expiration atteint, le Cloud Connector est déconnecté.
- Action recommandée : redémarrez le Cloud Connector. En cas d'échec, contactez le support Citrix.

brk.poweron.forlaunch.execution.remotehclserverconnectionfailure

- Description : aucune erreur n'a été détectée sur le plug-in ou le point de terminaison HCL/proxy distant lors de la configuration de la connexion au plug-in.
- Action recommandée : redémarrez le connecteur. En cas d'échec, contactez le support Citrix.

brk.poweron.forlaunch.execution.expiredcredentialsfailure

- Description : des informations d'identification expirées ont été fournies.
- Action recommandée : actualisez les informations d'identification expirées utilisées par la connexion à l'hyperviseur.

brk.poweron.forlaunch.execution.mcsmachinemanagementcustomfailure

- Description : erreurs lors de la création de la machine.
- Action recommandée : contactez le support Citrix.

brk.poweron.forlaunch.execution.detachdiskfailed

- Description : le disque de détachement utilisé par la machine virtuelle a échoué.
- Action recommandée : contactez le support Citrix.

brk.poweron.forlaunch.execution.createclonefailed

- Description : la création d'un disque clone a échoué dans l'hyperviseur.
- Action recommandée : contactez le support Citrix.

brk.poweron.forlaunch.execution.provisionedvmnotfound

- Description : la machine virtuelle provisionnée est introuvable.
- Action recommandée : supprimez la machine virtuelle provisionnée du catalogue. En cas d'échec, contactez le support Citrix.

brk.poweron.forlaunch.execution.invalidvmstate

- Description : l'opération ne peut pas se poursuivre en raison d'un état de machine virtuelle non valide.
- Action recommandée : redémarrez d'abord la machine virtuelle, puis recommencez l'opération.

brk.poweron.forlaunch.execution.insufficientresources

- Description : ressources insuffisantes pendant le fonctionnement.
- Action recommandée : vérifiez le quota de ressources utilisé par l'hyperviseur.

brk.poweron.forlaunch.execution.hypervisorinmaintenancemode

- Description : l'opération ne peut pas se poursuivre car l'hyperviseur est en mode de maintenance.
- Action recommandée : vérifiez si l'hyperviseur est en mode de maintenance.

brk.poweron.forlaunch.execution.delayed

- Description : l'opération est placée en file d'attente.
- Action recommandée : attendez la fin du processus. Si l'opération échoue, contactez le support Citrix.

brk.poweron.forlaunch.execution.recreatevmfailed

- Description : la recréation de la machine virtuelle a échoué.
- Action recommandée : contactez le support Citrix.

brk.poweron.forlaunch.execution.unknownvirtualmachine

- Description : machine virtuelle inconnue.
- Action recommandée : contactez le support Citrix.

brk.poweron.forlaunch.execution.ratelimitexceed

- Description : la connexion au cloud limite le débit.
- Action recommandée : réessayez la connexion ultérieurement si la demande est bloquée par la limitation de débit de l'hyperviseur.

brk.poweron.forlaunch.execution.virtualdisknotyetonstorage

- Description : le disque virtuel n'est pas stocké.
- Action recommandée : réessayez ultérieurement. En cas d'échec, contactez le support Citrix.

Profile Management

xendesktop.upm.userprofile.error.failure

- Description : Citrix Profile Management n'a pas réussi à traiter le profil utilisateur. Utilisez plutôt un profil temporaire.

- Action recommandée : cette erreur n'entraîne pas d'échec d'ouverture de session. Citrix Profile Management utilise un profil temporaire à la place. Pour résoudre l'erreur, consultez les journaux des événements Windows.

xendesktop.upm.userprofile.error.timeout

- Description : Citrix Profile Management n'a pas réussi à traiter le profil utilisateur dans le délai spécifié.
- Action recommandée : cette erreur n'entraîne pas d'échec d'ouverture de session. Citrix Profile Management continue de traiter le profil utilisateur. Pour résoudre l'erreur, consultez les journaux Citrix Profile Management.

Agent WEM

wem.agent.userpolicy.error.failure

- Description : l'agent Workspace Environment Management (WEM) n'a pas pu traiter les stratégies de groupe pour l'utilisateur. L'ouverture de session de l'utilisateur se poursuit.
- Action recommandée : cette erreur n'entraîne pas d'échec d'ouverture de session. Pour plus d'informations, consultez la documentation du produit WEM, ainsi que les journaux de service de l'agent WEM.

wem.agent.userpolicy.error.timeout

- Description : l'agent Workspace Environment Management (WEM) n'a pas pu traiter les stratégies de groupe pour l'utilisateur dans le délai spécifié. L'ouverture de session de l'utilisateur se poursuit.
- Action recommandée : cette erreur n'entraîne pas d'échec d'ouverture de session. Pour plus d'informations, consultez la documentation du produit WEM, ainsi que les journaux de service de l'agent WEM.

Post-lancement Android

SessionManager.Launch.EngineLoadFailed

- Description : échec du chargement ou de l'initialisation du moteur ICA.
- Action recommandée : contactez le support Citrix.

SessionManager.Launch.ConnectionFailed

- Description : le moteur a été interrompu avant la connexion.
- Action recommandée : contactez le support Citrix.

SessionManager.Launch.LogonFailed

- Description : la session a été déconnectée avant la fin de l'ouverture de session.
- Action recommandée : contactez le support Citrix.

SessionManager.LeaseResolution.Failed

- Description : impossible de tenter le lancement de la location.
- Action recommandée : contactez le support Citrix.

SessionManager.clxmtp.SoftDeny

- Description : la négociation CLXMTP du moteur a échoué (refus flexible).
- Action recommandée : contactez le support Citrix.

SessionManager.clxmtp.SoftDeny_Implicit

- Description : la connexion CLXMTP du moteur a échoué (refus flexible implicite).
- Action recommandée : contactez le support Citrix.

Transport.Connect.NoCGP_Fail

- Description : échec de la connexion (CGP désactivé).
- Action recommandée : contactez le support Citrix.

Transport.Connect.FallbackFail

- Description : échec de connexion. Tentative de retour ICA.
- Action recommandée : contactez le support Citrix.

Transport.Connect.Fail

- Description : la connexion n'est pas disponible.
- Action recommandée : contactez le support Citrix.

Pré-lancement Android

CWA-ICADOWNLOAD_ERR_00001

- Description : le type de demande d'envoi ICA est incorrect.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00002

- Description : la demande ICA n'est pas valide.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00003

- Description : le magasin a la valeur NULL pour la demande ICA.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00004

- Description : l'URL du magasin a la valeur NULL pour la demande ICA.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00005

- Description : le paramètre de ressource a la valeur NULL pour la demande ICA.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00006

- Description : le paramètre de ressource fourni pour la demande ICA n'est pas un type de ressource valide.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00007

- Description : le paramètre de ressource fourni pour la demande ICA a la valeur NULL pour l'URL de lancement ICA.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00008

- Description : la demande ICA a la valeur NULL avec les paramètres de l'Authentication Manager.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00009

- Description : le corps de la demande ICA a la valeur NULL.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000010

- Description : échec de création d'une entité HTTP à partir du corps de la demande ICA.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000011

- Description : échec du téléchargement du fichier ICA en raison d'une exception liée à la création de la demande de l'Authentication Manager
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000012

- Description : échec du téléchargement du fichier ICA en raison d'une exception liée à l'exécution de la demande de l'Authentication Manager.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000013

- Description : échec du téléchargement du fichier ICA en raison d'une réponse inattendue de la demande de l'Authentication Manager.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000014

- Description : échec du téléchargement du fichier ICA lors de la copie de l'élément inputStream à partir de la réponse de l'Authentication Manager.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000015

- Description : échec de l'analyse du document ICA à l'aide de l'élément inputStream à partir de la réponse de l'Authentication Manager.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000016

- Description : le document ICA téléchargé a la valeur null sans exception.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000017

- Description : échec du téléchargement du fichier ICA en raison de l'échec d'une réponse.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000018

- Description : la ressource n'est pas disponible.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000019

- Description : la ressource à lancer n'existe pas, n'est pas activée ou n'est pas visible pour un utilisateur.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000020

- Description : il n'y a plus de sessions actives.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000021

- Description : le serveur ne possède pas la licence requise pour effectuer l'activité demandée.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000022

- Description : aucun poste de travail n'est disponible.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000023

- Description : impossible de se connecter au poste de travail. Le serveur a refusé la connexion.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000024

- Description : le poste de travail est en cours de maintenance et n'est pas disponible.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000025

- Description : impossible de lancer la ressource en raison d'une erreur `resourceerror` dans le fichier ICA.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000026

- Description : impossible de lancer la ressource en raison d'une erreur `generalapplauncherror` dans le fichier ICA.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000027

- Description : impossible de lancer la ressource en raison d'une erreur inconnue dans le fichier ICA.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000028

- Description : impossible de lancer la ressource en raison d'une erreur de redémarrage dans le fichier ICA.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000029

- Description : impossible de lancer la ressource en raison d'une erreur de reprise dans le fichier ICA.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000030

- Description : impossible de lancer la ressource en raison d'une erreur non définie dans le fichier ICA.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_000031

- Description : impossible de télécharger le fichier ICA. Toutefois, le code d'erreur n'est pas trouvé dans le mappage défini.
- Action recommandée : contactez le support Citrix.

Post-lancement Linux

SessionManager.Launch.EngineLoadFailed

- Description : impossible de charger le moteur ICA.
- Action recommandée : contactez le support Citrix.

SessionManager.Launch.Failed

- Description : échec du lancement de la session.
- Action recommandée : contactez le support Citrix.

SessionManager.Launch.ConnectionFailed

- Description : le moteur a été interrompu avant la connexion.
- Action recommandée : recherchez les autres erreurs associées à la tentative de lancement.

SessionManager.Launch.LogonFailed

- Description : la session a été déconnectée avant la fin de l'ouverture de session.
- Action recommandée : cette erreur indique un échec de connexion, y compris éventuellement un échec de saisie manuelle des informations d'identification par l'utilisateur. Vérifiez comment l'utilisateur a tenté de se connecter au VDA distant.

SessionManager.LeaseResolution.Failed

- Description : impossible de tenter le lancement de la location.
- Action recommandée : vérifiez que les locations ont été synchronisées avec la machine cliente et qu'elles sont toujours valides. L'utilisateur peut se connecter à Citrix Workspace en mode en ligne pour déclencher la (re) synchronisation des locations. Recherchez les erreurs envoyées par les composants Gateway ou Cloud Connector. Ces erreurs peuvent indiquer les raisons de l'échec.

Transport.Connect.NoCGP_Fail

- Description : échec de la connexion (CGP désactivé).
- Action recommandée : déterminez pourquoi le client n'est pas en mesure de contacter un VDA via TCP ou EDT.

Transport.Connect.FallbackFail

- Description : échec de connexion. Tentative de retour ICA.
- Action recommandée : déterminez pourquoi le client n'est pas en mesure de contacter une instance Gateway, Connector ou un VDA via TCP ou EDT.

Transport.Connect.Fail

- Description : l'application Citrix Workspace n'a pas réussi à se connecter à l'instance Gateway, Connector ou au VDA via TCP, EDT ou UDP.
- Action recommandée : déterminez pourquoi le client n'est pas en mesure de contacter l'instance Gateway, Connector ou le VDA via TCP, EDT ou UDP. Le pare-feu entre le client et l'hôte peut ne pas autoriser les protocoles (UDP/TCP) ou les ports requis.

SessionManager.clxmtp.SoftDeny

- Description : la négociation CLXMTP du moteur a échoué (refus flexible).

- Action recommandée : cette erreur n'indique pas que le lancement doit échouer. Elle indique que le moteur ne peut pas réussir via un chemin réseau spécifique. Recherchez les erreurs envoyées par les composants Gateway ou Cloud Connector. Ces erreurs peuvent indiquer les raisons de l'échec.

SessionManager.clxmtp.SoftDeny_Implicit

- Description : la connexion CLXMTP du moteur a échoué (refus flexible implicite).
- Action recommandée : cette erreur n'indique pas que le lancement doit échouer. Elle indique que le moteur ne peut pas réussir via un chemin réseau spécifique. Déterminez pourquoi le client ne peut pas contacter un composant Connector ou Gateway. Cet hôte peut être inaccessible en raison de la topologie du réseau ou des restrictions de pare-feu.

Pré-lancement Linux

CWA-ICADOWNLOAD_ERR_00001

- Description : impossible de se connecter au magasin en raison de l'absence de réponse de l'application Citrix Workspace.
- Action recommandée : vérifiez si Citrix Workspace ou StoreFront sont arrêtés. Vérifiez également la connectivité Internet.

CWA-ICADOWNLOAD_ERR_00002

- Description : l'utilisateur a annulé le lancement de la session.
- Action recommandée : relancez la session après un certain temps.

CWA-ICADOWNLOAD_ERR_00003

- Description : impossible de se connecter au magasin. Vérifiez que les certificats de serveur sont valides.
- Action recommandée : vérifiez si les certificats de serveur sont installés et actifs.

CWA-ICADOWNLOAD_ERR_00004

- Description : la ressource à lancer n'existe pas, n'est pas activée ou n'est pas visible pour un utilisateur.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00005

- Description : les postes de travail ne sont pas disponibles pour cette demande.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00006

- Description : le serveur ne possède pas la licence requise pour effectuer l'activité demandée.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00007

- Description : le serveur a refusé la connexion au poste de travail.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00008

- Description : le poste de travail demandé est en cours de maintenance et n'est pas disponible.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00009

- Description : la limite maximale de sessions est atteinte.
- Action recommandée : vous avez atteint la limite de session maximale configurée par un administrateur. Redémarrez la session.

CWA-ICADOWNLOAD_ERR_000010

- Description : erreur générale qui ne peut pas être spécifiée davantage.
- Action recommandée : contactez le support Citrix.

Post-lancement Mac

Le bureau n'a pas pu démarrer

- Description : le bureau « Nom du bureau » n'a pas pu démarrer. ID de transaction - « ID de transaction ».
- Action recommandée : contactez votre administrateur en lui fournissant les détails de l'erreur.

La visionneuse n'a pas pu démarrer

- Description : la visionneuse n'a pas pu démarrer. ID de transaction - « ID de transaction ».
- Action recommandée : contactez votre administrateur en lui fournissant les détails de l'erreur.

Le bureau n'a pas pu démarrer

- Description : le bureau « Nom du bureau » fait l'objet d'une maintenance planifiée. ID de transaction - « ID de transaction ».
- Action recommandée : contactez votre administrateur en lui fournissant les détails de l'erreur.

L'application n'a pas pu démarrer

- Description : « Nom de l'application » n'a pas pu démarrer.
- Action recommandée : contactez votre administrateur en lui fournissant les détails de l'erreur.

L'application n'a pas pu démarrer

- Description : « Nom de l'application » n'a pas pu démarrer. ID de transaction - « ID de transaction ».
- Action recommandée : contactez votre administrateur en lui fournissant les détails de l'erreur.

Le bureau n'a pas pu démarrer

- Description : le bureau « Nom du bureau » n'a pas pu démarrer.
- Action recommandée : contactez votre administrateur en lui fournissant les détails de l'erreur.

Le bureau n'a pas pu démarrer

- Description : le bureau « Nom du bureau » n'a pas pu démarrer. ID de transaction - « ID de transaction ».
- Action recommandée : contactez votre administrateur en lui fournissant les détails de l'erreur.

La visionneuse n'a pas pu démarrer

- Description : la visionneuse n'a pas pu ouvrir « Nom de l'application ». ID de transaction - « ID de transaction ».
- Action recommandée : contactez votre administrateur en lui fournissant les détails de l'erreur.

La visionneuse n'a pas pu démarrer

- Description : la visionneuse n'a pas pu ouvrir « Nom du bureau ». ID de transaction - « ID de transaction ».
- Action recommandée : contactez votre administrateur en lui fournissant les détails de l'erreur.

Le bureau n'a pas pu démarrer

- Description : le bureau « Nom du bureau » fait l'objet d'une maintenance planifiée.
- Action recommandée : contactez votre administrateur en lui fournissant les détails de l'erreur.

Le bureau n'a pas pu démarrer

- Description : le bureau « Nom du bureau » fait l'objet d'une maintenance planifiée. ID de transaction - « ID de transaction ».
- Action recommandée : contactez votre administrateur en lui fournissant les détails de l'erreur.

Impossible de se connecter au bureau

- Description : impossible de se connecter à « Nom du bureau ». ID de transaction - « ID de transaction ». Réessayez plus tard.
- Action recommandée : si le problème persiste, contactez votre administrateur en lui fournissant les détails de l'erreur.

Pré-lancement Mac

CWA-ICADOWNLOAD_ERR_00001

- Description : le fichier ICA n'est pas valide.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00002

- Description : la demande de lancement a expiré.
- Action recommandée : vérifiez la connexion Internet ou contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00003

- Description : le serveur n'a pas répondu.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00004

- Description : la ressource à lancer n'existe pas, n'est pas activée ou n'est pas visible pour l'utilisateur.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00005

- Description : le serveur n'est pas accessible.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00006

- Description : erreur lors du lancement de la visionneuse.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00007

- Description : échec du lancement d'un événement ouvert Apple.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00008

- Description : le chemin de la visionneuse n'est pas accessible.
- Action recommandée : contactez le support Citrix.

CWA-ICADOWNLOAD_ERR_00009

- Description : l'utilisateur a annulé l'authentification.
- Action recommandée : demandez à l'utilisateur de relancer la ressource.

CWA-ICADOWNLOAD_ERR_000010

- Description : l'utilisateur a annulé la fenêtre LSI.
- Action recommandée : demandez à l'utilisateur de relancer la ressource.

CWA-ICADOWNLOAD_ERR_000011

- Description : le poste de travail demandé est en cours de maintenance et ne peut pas être utilisé.
- Action recommandée : demandez à l'utilisateur de réessayer une fois que la maintenance est terminée et que le poste de travail est prêt à être utilisé.

CWA-ICADOWNLOAD_ERR_000012

- Description : les informations de connexion de l'utilisateur doivent être modifiées.
- Action recommandée : demandez à l'utilisateur de modifier ses identifiants de connexion.

CWA-ICADOWNLOAD_ERR_000013

- Description : la session qui connecte la ressource n'est plus active.
- Action recommandée : demandez à l'utilisateur de réessayer ou contactez votre support technique Citrix pour obtenir de l'aide.

CWA-ICADOWNLOAD_ERR_000014

- Description : impossible de télécharger le fichier ICA.
- Action recommandée : contactez le support Citrix.

Post-lancement Windows

SessionManager.Launch.EngineLoadFailed

- Description : les principaux composants permettant d'établir une connexion à un poste de travail ou à une application distante n'ont pas pu être chargés ou initialisés correctement. Des détails supplémentaires peuvent être fournis dans le message d'erreur.
- Action recommandée : l'application Citrix Workspace ne fonctionne pas comme prévu. Une DLL de canal virtuel tierce (non Citrix) ou un autre composant système peut être à l'origine de ce problème. Il peut être nécessaire de collecter et de soumettre des traces CDF pour déterminer la nature de l'échec.

SessionManager.Launch.ConnectionFailed

- Description : cette erreur est un échec générique indiquant qu'une tentative de lancement a échoué. D'autres erreurs envoyées peuvent indiquer une cause.
- Action recommandée : recherchez les autres erreurs associées à la tentative de lancement.

SessionManager.Launch.LogonFailed

- Description : cette erreur indique qu'une connexion à un poste de travail ou à une application distante a été établie. Toutefois, la session s'est déconnectée sans terminer la connexion Windows (ou un autre système d'exploitation).
- Action recommandée : cette erreur indique un échec de connexion, notamment un échec de la saisie manuelle des informations d'identification par l'utilisateur. Vérifiez comment l'utilisateur a tenté de se connecter au VDA distant.

SessionManager.Launch.Cancelled

- Description : la tentative de connexion du moteur Citrix a été annulée, probablement à la suite d'une action de l'utilisateur.
- Action recommandée : cette erreur indique pourquoi une connexion n'a pas été établie avec succès, mais indique probablement un comportement correct.

SessionManager.LeaseResolution.Failed

- Description : indique qu'un lancement hors ligne (« basé sur la location ») a échoué. Cet échec est dû au fait qu'une location valide et obligatoire pour la ressource n'a pas été trouvée sur la machine cliente. En outre, les composants Gateway ou Cloud Connector ont rejeté la demande de lancement ou la demande de lancement n'était pas valide.
- Action recommandée : vérifiez que les locations ont été synchronisées avec la machine cliente et qu'elles sont toujours valides. L'utilisateur peut se connecter à Citrix Workspace en mode en ligne pour déclencher la (re) synchronisation des locations. Recherchez les erreurs envoyées par les composants Gateway ou Cloud Connector. Ces erreurs peuvent indiquer les raisons de l'échec.

SessionManager.clxmtp.SoftDeny

- Description : un lancement de location a été tenté ; un composant Connector ou Gateway a informé le client qu'il ne pouvait pas terminer le lancement demandé. Toutefois, les autres composants Connector ou Gateway peuvent faciliter le lancement.

- Action recommandée : cette erreur n'indique pas que le lancement doit échouer. Elle indique que le moteur ne peut pas réussir via un chemin réseau spécifique. Recherchez les erreurs envoyées par les composants Gateway ou Cloud Connector. Ces erreurs peuvent indiquer les raisons de l'échec.

SessionManager.clxmtp.SoftDeny_Implicit

- Description : une tentative de lancement de location a été effectuée et un composant Connector ou Gateway n'a pas pu être atteint. Toutefois, les autres composants Connector ou Gateway peuvent faciliter le lancement.
- Action recommandée : cette erreur n'indique pas que le lancement doit échouer. Elle indique que le moteur ne peut pas réussir via un chemin réseau spécifique. Déterminez pourquoi le client ne peut pas contacter un composant Connector ou Gateway. Cet hôte peut être inaccessible en raison de la topologie du réseau ou des restrictions de pare-feu.

Transport.Connect.NoCGP_Fail

- Description : les composants principaux de l'application Citrix Workspace (moteur) n'ont pas réussi à se connecter à un hôte VDA via le protocole ICA (port 1494). Les tentatives de connexion à un composant Gateway ou à un VDA via le protocole CGP n'ont pas été effectuées si cet événement a été envoyé.
- Action recommandée : déterminez pourquoi le client n'est pas en mesure de contacter un VDA via TCP ou EDT.

Transport.Connect.FallbackFail

- Description : les composants principaux de l'application Citrix Workspace (moteur) n'ont pas réussi à se connecter à un hôte VDA via le protocole ICA (port 1494). Après cet échec, l'application Citrix Workspace ne parvient pas à se connecter à un composant Gateway ou à un VDA via le protocole CGP (port 2598).
- Action recommandée : déterminez pourquoi le client n'est pas en mesure de contacter un composant Gateway, Connector ou un VDA via TCP ou EDT.

Transport.Connect.Fail

- Description : les composants principaux de l'application Citrix Workspace (moteur) n'ont pas réussi à se connecter à un composant Gateway ou à un VDA via le protocole CGP (port 2598). Les tentatives de connexion à un VDA via le protocole ICA n'ont pas été effectuées si cet événement a été émis.

- Action recommandée : déterminez pourquoi le client n'est pas en mesure de contacter un composant Gateway, Connector ou un VDA via TCP ou EDT.

Pré-lancement Windows

CWA-ICADOWNLOAD_ERR_00001

- Description : impossible de se connecter au magasin en raison de l'absence de réponse de l'application Citrix Workspace.
- Action recommandée : vérifiez si Citrix Workspace ou StoreFront sont arrêtés. Vérifiez également la connectivité Internet.

CWA-ICADOWNLOAD_ERR_00002

- Description : l'utilisateur a annulé le lancement de la session.
- Action recommandée : relancez la session après un certain temps.

CWA-ICADOWNLOAD_ERR_00003

- Description : impossible de se connecter au magasin. Vérifiez que les certificats de serveur sont valides.
- Action recommandée : contactez votre administrateur informatique pour lui fournir les détails de l'erreur.

CWA-ICADOWNLOAD_ERR_00004

- Description : la ressource à lancer n'existe pas, n'est pas activée ou n'est pas visible pour un utilisateur.
- Action recommandée : contactez votre administrateur informatique pour lui fournir les détails de l'erreur.

CWA-ICADOWNLOAD_ERR_00005

- Description : les postes de travail ne sont pas disponibles pour cette demande.
- Action recommandée : contactez votre administrateur informatique pour lui fournir les détails de l'erreur.

CWA-ICADOWNLOAD_ERR_00006

- Description : le serveur ne possède pas la licence requise pour effectuer l'activité demandée.
- Action recommandée : contactez votre administrateur informatique pour lui fournir les détails de l'erreur.

CWA-ICADOWNLOAD_ERR_00007

- Description : le serveur a refusé la connexion au poste de travail.
- Action recommandée : contactez votre administrateur informatique pour lui fournir les détails de l'erreur.

CWA-ICADOWNLOAD_ERR_00008

- Description : le poste de travail demandé est en cours de maintenance et n'est pas disponible.
- Action recommandée : contactez votre administrateur informatique pour lui fournir les détails de l'erreur.

CWA-ICADOWNLOAD_ERR_00009

- Description : la limite maximale de sessions est atteinte.
- Action recommandée : vous avez atteint la limite de session maximale configurée par un administrateur. Redémarrez la session.

CWA-ICADOWNLOAD_ERR_000010

- Description : erreur générale qui ne peut pas être spécifiée davantage.
- Action recommandée : contactez votre administrateur informatique pour lui fournir les détails de l'erreur.

Workspace

StoreLaunchIcaEndpoint.LaunchFailed

- Description : une erreur s'est produite lors du lancement.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops. Contactez le support Citrix.

StoreLaunchSessionEndpoint.BadRequest

- Description : les paramètres de la demande de lancement n'étaient pas valides ou étaient vides.
- Action recommandée : contactez le support Citrix.

StoreLaunchSessionEndpoint.FarmUnavailable

- Description : aucune ferme n'était disponible pour le lancement.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops.

StoreLaunchSessionEndpoint.Error

- Description : une erreur interne s'est produite lors du lancement.
- Action recommandée : contactez le support Citrix.

StoreGetIcaFileEndpoint.BadRequest

- Description : aucun ticket de lancement n'a été fourni dans la demande.
- Action recommandée : contactez le support Citrix.

StoreGetIcaFileEndpoint.RetrieveIcaFileForTicketFailed

- Description : Workspace n'a pas pu récupérer le fichier ICA.
- Action recommandée : contactez le support Citrix.

StoreGetIcaFileEndpoint.Error

- Description : Workspace n'a pas pu récupérer le fichier ICA.
- Action recommandée : contactez le support Citrix.

WebProxyGetLaunchStatusEndPoint.DSAuthFailure

- Description : un problème d'authentification s'est produit.
- Action recommandée : essayez de vous réauthentifier. Contactez le support Citrix.

WebProxyGetLaunchStatusEndPoint.LaunchFailed

- Description : une erreur interne s'est produite lors du lancement de l'application.
- Action recommandée : contactez le support Citrix.

WebProxyGetLaunchStatusEndPoint.ResourceNotFound

- Description : le lancement a échoué car l'application est introuvable.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops et la configuration des applications.

WebProxyLaunchIcaEndpoint.DSAuthFailure

- Description : un problème d'authentification s'est produit.
- Action recommandée : essayez de vous réauthentifier. Contactez le support Citrix.

WebProxyLaunchIcaEndpoint.LaunchFailed

- Description : une erreur interne s'est produite lors du lancement de l'application.
- Action recommandée : contactez le support Citrix.

WebProxyLaunchIcaEndpoint.ResourceNotFound

- Description : le lancement a échoué car l'application est introuvable.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops et la configuration des applications.

WebProxySessionsLaunchIcaEndpoint.SessionNotFound

- Description : Workspace n'a pas pu se reconnecter à la session HDX existante. Votre session est peut-être interrompue.
- Action recommandée : relancez l'application.

WebProxySessionsLaunchIcaEndpoint.DSAuthFailure

- Description : un problème d'authentification s'est produit.
- Action recommandée : essayez de vous réauthentifier. Contactez le support Citrix.

WebProxySessionsLaunchIcaEndpoint.ReconnectSessionFailed

- Description : Workspace n'a pas pu se reconnecter à la session HDX existante. Votre session est peut-être interrompue.
- Action recommandée : contactez le support Citrix.

WebProxySessionsLaunchIcaEndpoint.Error

- Description : une erreur interne s'est produite lors de la reconnexion à la session.
- Action recommandée : contactez le support Citrix.

WebProxySessionsGetLaunchStatusEndpoint.DSAuthFailure

- Description : un problème d'authentification s'est produit.
- Action recommandée : essayez de vous réauthentifier. Contactez le support Citrix.

WebProxySessionsGetLaunchStatusEndpoint.ReconnectSessionFailed

- Description : Workspace n'a pas pu se reconnecter à la session HDX.
- Action recommandée : contactez le support Citrix.

WebProxySessionsGetLaunchStatusEndpoint.Error

- Description : une erreur interne s'est produite lors de la reconnexion à la session.
- Action recommandée : contactez le support Citrix.

DetermineGateway.Error

- Description : Workspace n'a pas pu déterminer le composant Gateway auquel se connecter.
- Action recommandée : vérifiez la configuration de Gateway. Contactez le support Citrix.

ConnectionRoutingProviderLaunch.Error

- Description : Workspace n'a pas pu déterminer le composant Gateway auquel se connecter.
- Action recommandée : vérifiez la configuration de Gateway. Contactez le support Citrix.

BrokerGetAddressCall.AnonymousPrelaunchNotSupported

- Description : Workspace ne peut pas lancer l'application car la batterie de serveurs ne prend pas en charge les lancements anonymes.
- Action recommandée : contactez le support Citrix.

BrokerGetAddressCall.LeasingError

- Description : Workspace a reçu une erreur de la part du broker Citrix Virtual Apps and Desktops.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops. Contactez le support Citrix.

BrokerGetAddressCall.ServiceConnectionError

- Description : Workspace n'a pu contacter aucun broker Citrix Virtual Apps and Desktops de la batterie de serveurs.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops. Contactez le support Citrix.

BrokerGetAddressCall.BrokerError

- Description : Workspace a reçu une erreur d'un broker Citrix Virtual Apps and Desktops.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops. Contactez le support Citrix.

BrokerGetAddressCall.LicensingError

- Description : Workspace n'a pas pu lancer l'application en raison d'une erreur de licence.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops. Contactez le support Citrix.

BrokerGetAddressCall.Error

- Description : Workspace ne peut pas récupérer les détails du VDA auprès du broker Citrix Virtual Apps and Desktops.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops. Contactez le support Citrix.

GetLaunchReference.NoAccessToken

- Description : Workspace ne parvient pas à se connecter au VDA.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops. Contactez le support Citrix.

GetLaunchReference.BrokerError

- Description : Workspace ne parvient pas à se connecter au VDA.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops. Contactez le support Citrix.

GetLaunchReference.Error

- Description : Workspace ne parvient pas à se connecter au VDA.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops. Contactez le support Citrix.

GenerateIcaFile.InvalidIcaSetting

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

StoreIcaFileAndGetTicket.StoreIcaFileAndCreateTicketFailed

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

StoreIcaFileAndGetTicket.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GetFasVdaLogonTicket.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GenerateSTATicket.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GetVdaAddress.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GetTicket.NoAccessToken

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GetTicket.BrokerError

- Description : le broker Citrix Virtual Apps and Desktops n'a pas pu lancer la session HDX.
- Action recommandée : vérifiez l'ID dans le message d'erreur et vérifiez vos journaux Citrix Virtual Apps and Desktops.

GetTicket.ServiceConnectionError

- Description : Workspace ne peut pas contacter un broker Citrix Virtual Apps and Desktops.
- Action recommandée : contactez le support Citrix.

GetTicket.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GetNetscalerConfigurationByCustomer.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

DiscoverMPSServerCapabilities.Error

- Description : un problème s'est produit lors de l'envoi d'une demande auprès du broker Citrix Virtual Apps and Desktops.
- Action recommandée : vérifiez vos journaux Citrix Virtual Apps and Desktops. Contactez le support Citrix.

GetResourceLocationNetScalerConfig.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GetCustomerResourceLocations.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GetResourceLocationFromResourceProvider.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GetNetScalerGatewayInfo.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GetCustomerEntitlements.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GetResourceLocationForServerFeed.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

GetResourceInformation.Error

- Description : une erreur interne s'est produite lors de l'établissement d'une connexion HDX.
- Action recommandée : contactez le support Citrix.

Citrix Gateway as a Service

CGS-ICASN_ERR_00001

- Description : le lancement de l'application a échoué en raison d'une erreur d'analyse des demandes.
- Action recommandée : contactez le support Citrix.

CGS-ICASN_ERR_00002

- Description : échec de la validation du ticket d'authentification.
- Action recommandée : contactez le support Citrix.

CGS-ICASN_ERR_00003

- Description : échec de la validation du ticket d'authentification.
- Action recommandée : contactez le support Citrix.

CGS-ICASN_ERR_00004

- Description : échec de la validation du ticket d'authentification.
- Action recommandée : contactez le support Citrix.

CGS-ICASN_ERR_00005

- Description : échec de l'établissement de la connexion au Connector.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Si le problème persiste, contactez le support Citrix.

CGS_ICASN_ERR_00006

- Description : la demande de connexion au Connector a expiré.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Vérifiez si des paramètres de proxy bloquent le trafic entre le Connector/VDA et le NGS. Vérifiez la connectivité entre le VDA et le Connector. Si le problème persiste, contactez le support Citrix.

CGS_ICASN_ERR_00007

- Description : l'application Citrix Workspace a fermé la connexion.
- Action recommandée : vérifiez que la connectivité réseau côté client est stable. Si le problème persiste, contactez le support Citrix.

CGS_ICASN_ERR_00008

- Description : le serveur principal a fermé la connexion.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Vérifiez la stabilité du réseau entre le Connector/VDA et le réseau public (NGS). Si le problème persiste, contactez le support Citrix.

CGS_ICASN_ERR_00009

- Description : échec de l'établissement de la connexion entre le VDA et le NGS (Rendezvous).
- Action recommandée : vérifiez l'état d'intégrité du Connector. Le VDA doit être en mesure de contacter le service NGS. Vérifiez la connectivité entre le VDA et le Connector. Si le problème persiste, contactez le support Citrix.

CGS_ICASN_ERR_00010

- Description : basculement EDT vers TCP. Vérifiez les prérequis pour l'EDT.
- Action recommandée : Rendezvous doit être activé et le VDA doit être en mesure de contacter le service NGS via UDP. Si le problème persiste, contactez le support Citrix.

CGS_ICASN_ERR_00011

- Description : échec du service interne du NGS.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00012

- Description : échec du service interne du NGS.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00013

- Description : échec de la validation du GCT.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00014

- Description : échec de la validation du GCT.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00015

- Description : échec du service interne du NGS.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00016

- Description : échec du service interne du NGS.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00017

- Description : échec du service interne du NGS.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00018

- Description : échec de la validation du ticket d'authentification.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00019

- Description : échec de la validation du ticket d'authentification.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00020

- Description : erreur dans la licence interne du CGS.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00021

- Description : basculement de Rendezvous v2 à cause de l'indicateur de fonctionnalités (feature flag) désactivé.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00022

- Description : échec du service interne du NGS.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00023

- Description : délai d'expiration dans l'échange CLXMTP.
- Action recommandée : vérifiez que les connecteurs sont intègres et accessibles par le service NGS. Si le problème persiste, contactez le support Citrix.

CGS_ICASN_ERR_00024

- Description : échec de la validation CLXMTP VSR.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00025

- Description : échec de la validation CLXMTP VSR.
- Action recommandée : contactez le support Citrix.

CGS_ICASN_ERR_00026

- Description : le connecteur n'est pas disponible dans CLXMTP.
- Action recommandée : vérifiez si le connecteur se trouve dans un état d'intégrité normal pour l'emplacement des ressources. Si le problème persiste, contactez le support Citrix.

CGS_ICASN_ERR_00027

- Description : la redirection CLXMTP vers le connecteur a échoué après un nombre maximal de tentatives.

- Action recommandée : vérifiez si le connecteur se trouve dans un état d'intégrité normal pour l'emplacement des ressources. Vérifiez que le service `Citrix ClxMtp Service` est en cours d'exécution sur tous les connecteurs. Contactez le support Citrix.

CGS_ICASN_ERR_00028

- Description : impossible de communiquer avec le contrôleur.
- Action recommandée : contactez le support Citrix.

Success: CGS_ICASN_SUCCESS_00001

- Description : demande de lancement de session reçue.
- Action recommandée : non applicable

Success: CGS_ICASN_SUCCESS_00002

- Description : demande de lancement de session terminée.
- Action recommandée : non applicable

Proxy XAXD

XDPXY_INF_00001

- Description : le broker envoie une demande au VDA pour préparer les connexions entrantes.
- Action recommandée : non applicable

XDPXY_INF_00002

- Description : le VDA confirme la demande de connexion par le broker.
- Action recommandée : non applicable

XDPXY_ERR_00001

- Description : échec de communication avec le VDA.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Pour plus d'informations, consultez Citrix Cloud Connector et CTX224133.
  - Redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.

  - Si un proxy Web existe entre le connecteur et le broker, assurez-vous qu'il est correctement configuré.
  - Si le problème persiste, contactez le support Citrix.

XDPXY_ERR_00002

- Description : XaxdProxy a dépassé le délai d'attente d'une réponse du VDA.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Pour plus d'informations, consultez Citrix Cloud Connector et CTX224133.
  - Redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.
  - Si un proxy Web existe entre le connecteur et le broker, assurez-vous qu'il est correctement configuré.
  - Si le problème persiste, contactez le support Citrix.

XDPXY_ERR_00003

- Description : une erreur ou une exception WCF a été rencontrée lors de la tentative de demande.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Pour plus d'informations, consultez Citrix Cloud Connector et CTX224133.
  - Redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.
  - Si un proxy Web existe entre le connecteur et le broker, assurez-vous qu'il est correctement configuré.
  - Si le problème persiste, contactez le support Citrix.

XDPXY_INF_00003

- Description : la demande de validation pour la connexion ICA ou RDP entrante est appelée par la pile.
- Action recommandée : non applicable

XDPXY_INF_00004

- Description : la validation de la connexion ICA ou RDP entrante est établie.
- Action recommandée : non applicable

XDPXY_ERR_00001

- Description : échec de communication avec le proxy du VDA.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Pour plus d'informations, consultez Citrix Cloud Connector et CTX224133.
  - Redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.
  - Si un proxy Web existe entre le connecteur et le broker, assurez-vous qu'il est correctement configuré.
  - Si le problème persiste, contactez le support Citrix.

XDPXY_ERR_00002

- Description : XaxdProxy a dépassé le délai d'attente d'une réponse du proxy du VDA.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Pour plus d'informations, consultez Citrix Cloud Connector et CTX224133.
  - Redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.
  - Si un proxy Web existe entre le connecteur et le broker, assurez-vous qu'il est correctement configuré.
  - Si le problème persiste, contactez le support Citrix.

XDPXY_ERR_00003

- Description : une exception a été rencontrée lors de la tentative de demande.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Pour plus d'informations, consultez Citrix Cloud Connector et CTX224133.
  - Redémarrez le service Citrix Delivery Agent sur le VDA ou redémarrez le VDA.
  - Si un proxy Web existe entre le connecteur et le broker, assurez-vous qu'il est correctement configuré.
  - Si le problème persiste, contactez le support Citrix.

XDPXY_INF_00005

- Description : une demande de trafic de session HDX directement vers le VDA est effectuée.
- Action recommandée : non applicable

XDPXY_INF_00006

- Description : le VDA établit une connexion directe avec le plan de contrôle Citrix Cloud pour le trafic de session HDX.
- Action recommandée : non applicable

XDPXY_INF_00007

- Description : le client envoie une demande de connexion à un magasin StoreFront local pour une ressource.
- Action recommandée : non applicable

XDPXY_INF_00008

- Description : le magasin StoreFront local accepte les demandes de connexion du client pour la ressource.
- Action recommandée : non applicable

XDPXY_ERR_00004

- Description : XaxdProxy a reçu une réponse d'erreur HTTP lors de la tentative de connexion.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Pour plus d'informations, consultez Citrix Cloud Connector et CTX224133.
  - Vérifiez la stabilité du réseau entre le Connector et le réseau public.
  - Si un proxy Web existe entre le connecteur et le broker, assurez-vous qu'il est correctement configuré.
  - Si le problème persiste, contactez le support Citrix.

XDPXY_ERR_00006

- Description : le format de la demande XML n'est pas valide.
- Action recommandée : contactez le support Citrix.

XDPXY_ERR_00007

- Description : la demande XML comporte des en-têtes et/ou un format d'informations d'identification non valides.
- Action recommandée : déconnectez-vous, reconnectez-vous et recommencez l'action. Si le problème persiste, contactez le support Citrix

XDPXY_INF_00011

- Description : le lancement de la continuité du service est demandé par l'utilisateur via WSA.
- Action recommandée : non applicable

XDPXY_INF_00012

- Description : le lancement de la continuité du service est demandé par l'utilisateur via WSA.
- Action recommandée : non applicable

XDPXY_ERR_00004

- Description : XaxdProxy a rencontré une erreur HTTP lors de la tentative de connexion.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Pour plus d'informations, consultez Citrix Cloud Connector et CTX224133.
  - Si un proxy Web existe entre le connecteur et le broker, assurez-vous qu'il est correctement configuré.
  - Si le problème persiste, contactez le support Citrix.

XDPXY_ERR_00008

- Description : le lancement de la continuité du service a échoué car XaxdProxy a dépassé le délai d'attente d'une réponse.
- Action recommandée : vérifiez l'état d'intégrité du Connector. Pour plus d'informations, consultez Citrix Cloud Connector et CTX224133.
  - Si un proxy Web existe entre le connecteur et le broker, assurez-vous qu'il est correctement configuré.
  - Si le problème persiste, contactez le support Citrix.

XDPXY_ERR_00009

- Description : le lancement de la continuité de service a échoué en raison du blocage et/ou de la révocation de la location.
- Action recommandée : contactez votre administrateur Citrix Cloud en lui fournissant les détails de l'erreur. Pour plus d'informations, consultez la documentation Continuité du service.
  - Si le problème persiste, contactez le support Citrix.

Citrix DaaS pour les fournisseurs de services Citrix

February 13, 2024

Cet article décrit comment **Citrix Service Providers (CSP)** peut configurer Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) pour les clients locataires dans Citrix Cloud. Pour obtenir une vue d'ensemble des fonctionnalités disponibles pour Citrix Partners, reportez-vous à la section Citrix Cloud pour les partenaires.

Exigences

- Vous êtes un partenaire Citrix Service Provider.
- Vous disposez d'un compte Citrix Cloud.
- Vous disposez d'un abonnement à Citrix DaaS.

Limitations et problèmes connus

Limitations

- Les changements de nom de locataire prennent jusqu'à 24 heures pour s'appliquer à toutes les interfaces.
- Lors de la création d'un locataire, l'adresse e-mail doit être unique.
- Le filtrage dans **Gérer > Configuration complète** par étendue (similaire à Surveiller) n'est pas disponible. Pour afficher les ressources attachées à une étendue, sélectionnez **Administrateurs** dans le volet gauche. Sous l'onglet **Étendues**, sélectionnez l'étendue, puis sélectionnez **Modifier l'étendue** dans le volet Action.

Problèmes connus

- Une fois les étendues affectées à une ressource, vous ne pouvez pas utiliser la console de gestion pour les supprimer ou les annuler. Ces tâches sont prises en charge uniquement via PowerShell.
- **Gérer > Configuration complète** n'applique pas les étendues. Il vous incombe de sélectionner l'étendue appropriée lors de la création de catalogues de machines, de groupes de mise à disposition et de groupes d'applications.
- Lorsque plus de 15 étendues sont créées (créées automatiquement et personnalisées), les informations d'accès personnalisé à Citrix Cloud pour un administrateur (**Gestion des identités et des accès > Administrateurs**) ne s'affichent pas correctement. Solution : Limitez les étendues à 15 ou moins.

Ajouter un client

1. Connectez-vous à Citrix Cloud avec vos informations d'identification CSP. Sélectionnez **Clients** dans le menu supérieur gauche.
2. Dans le tableau de bord client, sélectionnez **Inviter ou Ajouter**. Entrez les informations demandées.
3. Si le client n'a pas de compte Citrix Cloud, l'ajout du client crée un compte. L'ajout du client vous ajoute automatiquement en tant qu'administrateur d'accès complet du compte de ce client.
4. Si le client dispose d'un compte Citrix Cloud :

    a) Une URL Citrix Cloud s'affiche, que vous copiez et envoyez au client. Pour plus de détails sur ce processus, consultez la section Inviter un client à se connecter.
    b) Le client doit vous ajouter en tant qu'administrateur d'accès complet à son compte. Voir Ajouter des administrateurs à un compte Citrix Cloud.

Vous pouvez ajouter plus d'administrateurs ultérieurement et contrôler les clients qu'ils peuvent voir dans les consoles **Gérer** et **Surveiller**.

Ajouter Citrix DaaS à un client

1. Connectez-vous à Citrix Cloud avec vos informations d'identification CSP. Sélectionnez **Clients** dans le menu supérieur gauche.
2. Dans le tableau de bord du client, dans le menu des points de suspension du client, sélectionnez **Ajouter un service**.
3. Dans **Sélectionner un service à ajouter**, sélectionnez **Virtual Apps and Desktops**.
4. Sélectionnez **Continue**.

Une fois cette procédure terminée, le client est intégré à votre abonnement Citrix DaaS.

Une fois l'intégration terminée, une nouvelle étendue client est créée automatiquement dans Citrix DaaS. L'étendue est visible dans l'écran **Gérer > Configuration complète** . Cette étendue est unique à ce client. Vous pouvez renommer l'étendue, mais vous ne pouvez pas la supprimer.

Utilisez cette étendue pour personnaliser l'accès pour les autres administrateurs. Par exemple, disons que vous avez dix clients et deux administrateurs. En utilisant l'étendue unique, vous pouvez restreindre l'accès d'un administrateur à seulement trois clients. L'autre administrateur peut accéder à l'un de ces trois clients, plus deux autres clients. Pour plus de détails, voir Contrôler l'accès des administrateurs aux clients.

Configurer un emplacement de ressources

Un emplacement de ressources contient les machines qui fournissent des applications et des bureaux à vos clients, ainsi que les composants d'infrastructure tels que Citrix Cloud Connectors. Pour plus de détails, voir Se connecter à Citrix Cloud.

Configurer des catalogues et des groupes pour fournir des applications et des bureaux

> **Remarque :**
>
> Pour gérer le DaaS d'un client locataire, vous devez passer au compte du client CSP. Pour cela, cliquez sur le nom du client dans le menu en haut à droite, puis sur **Changer de client**.

Un catalogue est un groupe de machines virtuelles identiques. Lorsque vous créez un catalogue, une image est utilisée (avec d'autres paramètres) comme modèle pour créer les machines. Pour de plus amples informations, consultez la section Créer des catalogues de machines.

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 ou les bureaux à la disposition des utilisateurs. Pour de plus amples informations, consultez la section Créer des groupes de mise à disposition.

Les groupes d'applications vous permettent de gérer des collections d'applications. Vous pouvez créer des groupes d'applications pour les applications partagées entre différents groupes de mise à disposition ou utilisées par un sous-ensemble d'utilisateurs dans des groupes de mise à disposition. Pour plus de détails, voir Créer des groupes d'applications.

Lors de la configuration de groupes, assurez-vous que :

- L'étendue du groupe de mise à disposition est un sous-ensemble de l'étendue du catalogue de machines. Par exemple, supposons que l'étendue du catalogue est A et B. L'étendue du groupe de mise à disposition peut être A ou B, ou A et B.
- L'étendue du groupe d'applications est un sous-ensemble de l'étendue du groupe de mise à disposition. Par exemple, supposons que les groupes de mise à disposition associés à un groupe d'applications ont une étendue A et B. L'étendue du groupe d'applications peut être A ou B, ou A et B.

Domaines fédérés

Les domaines fédérés permettent aux utilisateurs d'utiliser les informations d'identification d'un domaine attaché à votre emplacement de ressources CSP pour se connecter à leur espace de travail. Cela vous permet de fournir des espaces de travail dédiés à vos clients auxquels les utilisateurs

peuvent accéder à l'aide d'une adresse URL d'espace de travail personnalisée (par exemple, customer.cloud.com), l'emplacement des ressources se trouvant toujours sur votre compte Citrix Cloud. Vous pouvez fournir des espaces de travail dédiés en plus de l'espace de travail partagé auxquels les clients peuvent accéder à l'aide de l'adresse URL de votre espace de travail CSP (par exemple, csp-partner.cloud.com).

Pour permettre aux clients d'accéder à leur espace de travail dédié, vous les ajoutez aux domaines appropriés que vous gérez. Après avoir configuré l'espace de travail via l'option Configuration de l'espace de travail, les utilisateurs peuvent se connecter à leur espace de travail et accéder aux applications et aux bureaux que vous avez rendus disponibles.

Ajouter un client à un domaine

1. Connectez-vous à Citrix Cloud avec vos informations d'identification CSP. Sélectionnez **Clients** dans le menu supérieur gauche.
2. Dans le tableau de bord du client, sélectionnez **Gestion des identités et des accès** dans le menu supérieur gauche.
3. Sous l'onglet **Domaines**, sélectionnez **Gérer le domaine fédéré** dans le menu des points de suspension du domaine.
4. Sur la carte **Gérer le domaine fédéré**, dans la colonne **Clients disponibles**, sélectionnez un client que vous souhaitez ajouter au domaine. Sélectionnez le signe plus en regard du nom du client. Le client sélectionné apparaît désormais dans la colonne **Clients fédérés**. Répétez cette opération pour ajouter d'autres clients. Lorsque vous avez terminé, sélectionnez **Appliquer**.

Supprimer un client d'un domaine

Lorsque vous supprimez un client d'un domaine que vous gérez, les utilisateurs du client ne peuvent plus accéder à leurs espaces de travail à l'aide des informations d'identification de votre domaine.

1. Dans le menu Citrix Cloud, sélectionnez **Gestion des identités et des accès**, puis sélectionnez **Domaines**.
2. Recherchez le domaine que vous souhaitez gérer et sélectionnez le bouton représentant des points de suspension. Sélectionnez **Gérer le domaine fédéré**.
3. Dans la liste des clients fédérés, recherchez les clients que vous souhaitez supprimer, puis sélectionnez le bouton X. Sélectionnez **Tout supprimer** pour supprimer tous les clients de la liste du domaine. Les clients sélectionnés sont déplacés vers la liste des clients disponibles.
4. Sélectionnez **Appliquer**.
5. Vérifiez les clients que vous avez sélectionnés et sélectionnez **Supprimer les clients**.

Contrôler l'accès des administrateurs aux clients

Vous pouvez contrôler l'accès administrateur des clients à l'aide de l'étendue unique créée lorsque vous avez ajouté Citrix DaaS au client. Vous pouvez configurer l'accès lorsque vous ajoutez un administrateur ou ultérieurement.

Pour en savoir plus sur la restriction d'accès à l'aide de rôles et d'étendues dans Citrix DaaS, reportez-vous à la section Administration déléguée.

Ajouter un administrateur avec accès restreint

1. Connectez-vous à Citrix Cloud avec vos informations d'identification CSP. Sélectionnez **Clients** dans le menu supérieur gauche.
2. Dans le tableau de bord du client, sélectionnez **Gestion des identités et des accès** dans le menu supérieur gauche.
3. Sous l'onglet **Administrateurs**, sélectionnez **Ajouter adm. de**, puis sélectionnez **Identité Citrix**.
4. Tapez l'adresse e-mail de la personne que vous ajoutez en tant qu'administrateur, puis sélectionnez **Inviter**.
5. Configurez les autorisations d'accès appropriées de l'administrateur. Citrix recommande de sélectionner **Accès personnalisé**, sauf si vous souhaitez que l'administrateur puisse gérer Citrix Cloud et tous les services abonnés.
6. Après avoir sélectionné **Accès personnalisé**, sélectionnez une ou plusieurs paires rôle/étendue pour Citrix DaaS, selon vos besoins. Assurez-vous d'activer uniquement les entrées qui contiennent l'étendue unique créée pour le client.
7. Lorsque vous avez terminé de sélectionner des paires rôle/étendue, sélectionnez **Envoyer une invitation**.

Lorsque l'administrateur accepte l'invitation, il dispose de l'accès que vous avez attribué.

Modifier les autorisations d'administration déléguée pour les administrateurs

1. Connectez-vous à Citrix Cloud avec vos informations d'identification CSP. Sélectionnez **Clients** dans le menu supérieur gauche.
2. Dans le tableau de bord du client, sélectionnez **Gestion des identités et des accès** dans le menu supérieur gauche.
3. Sous l'onglet **Administrateurs**, sélectionnez **Modifier l'accès** dans le menu des points de suspension de l'administrateur.
4. Sélectionnez et effacez les paires rôle/étendue pour Citrix DaaS, selon vos besoins. Assurez-vous d'activer uniquement les entrées qui contiennent l'étendue unique créée pour le client.
5. Sélectionnez **Save**.

Afficher les administrateurs des clients ainsi que les rôles et les étendues qui leur sont attribués

1. Connectez-vous à Citrix Cloud avec vos informations d'identification CSP. Sélectionnez **Clients** dans le menu supérieur gauche.
2. Dans le tableau de bord du client, sélectionnez **Mes services > DaaS** dans le menu supérieur gauche.
3. Dans Citrix DaaS, sélectionnez **Gérer > Configuration complète**.
4. Sélectionnez **Administrateurs** dans le volet gauche.

Les informations sont disponibles sur trois onglets :

- L'onglet **Administrateurs** répertorie les administrateurs qui ont été créés, ainsi que leurs rôles et étendues.
- L'onglet **Rôles** répertorie tous les rôles. Pour afficher les détails d'un rôle, sélectionnez le rôle dans le volet central. La partie inférieure du panneau répertorie les types d'objets et les autorisations associées pour le rôle. Sélectionnez l'onglet **Administrateurs** dans le volet inférieur pour afficher une liste des administrateurs détiennent actuellement ce rôle.
- L'onglet **Étendues** répertorie toutes les étendues, y compris celles générées pour les clients des partenaires Citrix.

Configurer les espaces de travail

Le client dispose de son propre espace de travail avec une URL `customer.cloud.com` unique. C'est dans cet espace de travail que les utilisateurs du client accèdent à leurs applications et bureaux publiés.

L'URL de l'espace de travail est affichée à deux endroits :

- Dans le tableau de bord du client, sélectionnez **Configuration de l'espace de travail** dans le menu situé en haut à gauche.
- Sur la page **Accueil** (onglet **Présentation**) de Citrix DaaS, l'URL de l'espace de travail apparaît au bas de la page.

Vous pouvez modifier l'accès et l'authentification à un espace de travail. Vous pouvez également personnaliser l'apparence et les préférences de l'espace de travail. Pour de plus amples informations, consultez les articles suivants :

- Configurer les espaces de travail
- Espaces de travail sécurisés

Surveiller le service d'un client

Le tableau de bord **Surveiller** dans un environnement CSP est essentiellement le même qu'un environnement non-CSP. Voir Surveiller pour plus de détails.

Par défaut, le tableau de bord **Surveiller** affiche des informations sur tous les clients. Pour afficher des informations sur un client, utilisez **Sélectionner un client**.

Gardez à l'esprit que la possibilité de voir les affichages du tableau de bord Surveiller pour un client est contrôlée par l'accès configuré pour l'administrateur. L'accès doit inclure une paire rôle/étendue incluant l'étendue unique du client.

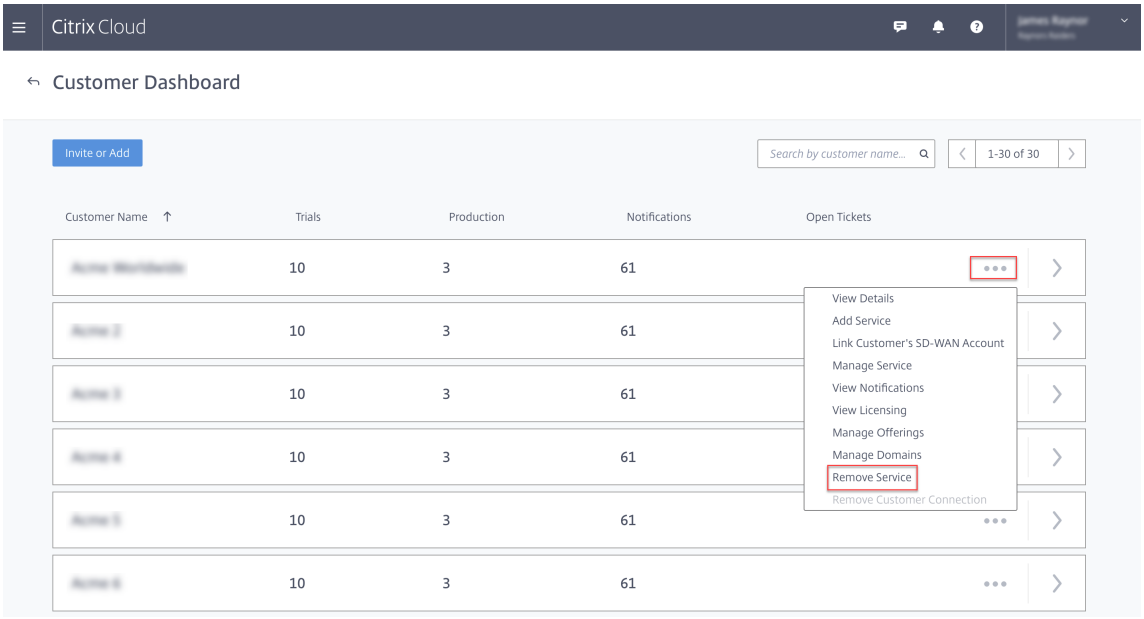
Si vous avez utilisé des rôles intégrés pour configurer l'accès : les rôles intégrés contrôlent si l'administrateur peut voir les écrans **Gérer** et **Surveiller**. Si vous sélectionnez uniquement des paires rôle/étendue client qui n'incluent pas la visibilité de l'onglet **Surveiller**, cet administrateur ne peut pas voir l'onglet **Surveiller** pour les clients sélectionnés. Par exemple, si vous donnez à un administrateur uniquement un accès **Administrateur en lecture seule, ClientABC**, cet administrateur ne peut pas voir l'onglet **Surveiller** du client ABC, car les administrateurs en lecture seule n'ont pas accès aux écrans Surveiller.

Supprimer un service

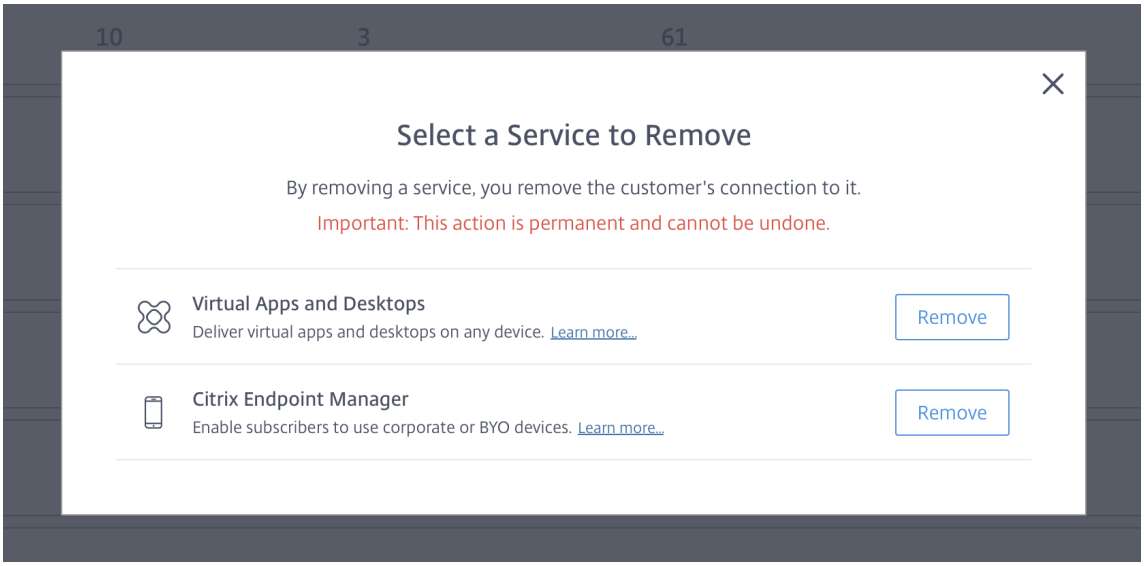
Pré-requis

- Assurez-vous que votre étendue client n'est liée à aucun objet Citrix DaaS. S'ils sont liés, vous ne pouvez pas supprimer le service. Pour dissocier des étendues, accédez à **Citrix Studio > Administrateurs > Étendues** et modifiez l'étendue.
- Pour connaître l'étendue client et la gérer, consultez Créer et gérer des étendues.

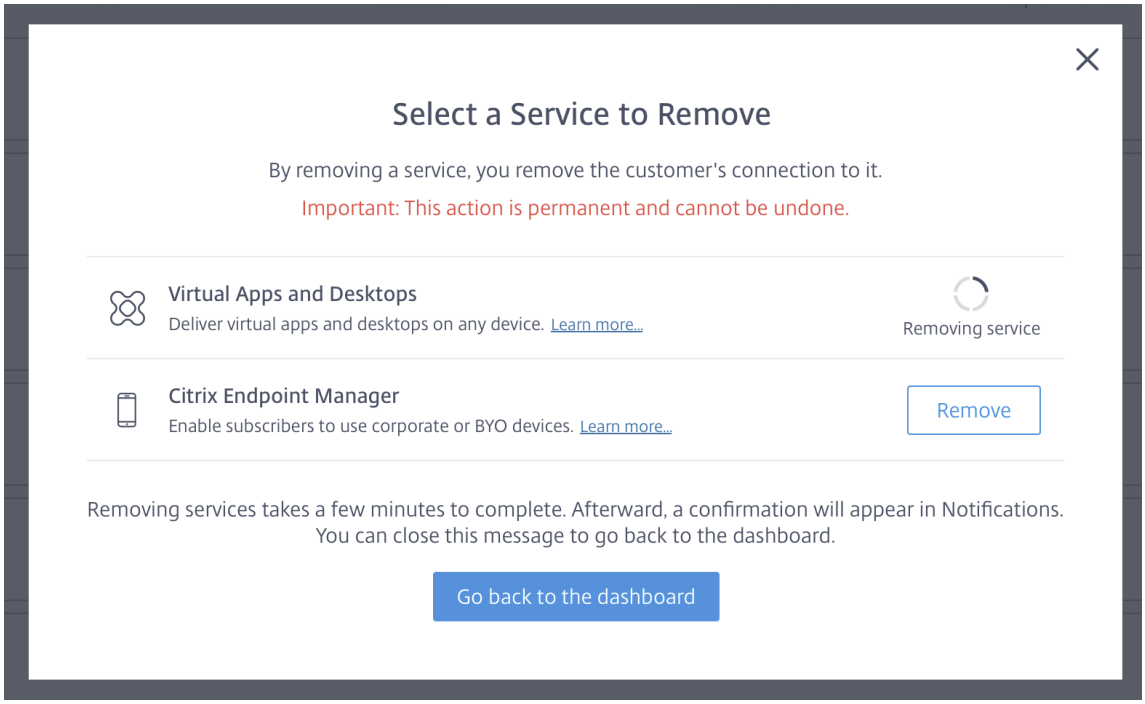
1. Connectez-vous à Citrix Cloud avec vos informations d'identification Citrix Service Provider.
2. Dans le **Tableau de bord client**, cliquez sur le menu représentant des **points de suspension** (…) du client dont vous souhaitez supprimer un service, puis sélectionnez **Supprimer service**.



La page **Sélectionnez un service à supprimer** s'affiche.



3. Cliquez sur **Supprimer** pour supprimer le service.



Citrix Gateway Service

December 7, 2022

Citrix Gateway fournit aux utilisateurs un accès sécurisé aux applications Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).

Citrix Gateway Service permet d'accéder à distance et de manière sécurisée à ces applications, sans avoir à déployer Citrix Gateway dans la DMZ ou à reconfigurer votre pare-feu. Les opérations d'infrastructure liées à l'utilisation de Citrix Gateway sont transférées sur Citrix Cloud.

Pour plus d'informations sur le service Citrix Gateway, consultez la documentation du produit. Cette référence explique comment activer le service Citrix Gateway et contient une section Problèmes connus pour la version que vous utilisez.

Citrix ADC est un Delivery Controller d'application qui analyse le trafic spécifique à l'application pour distribuer, optimiser et sécuriser intelligemment le trafic réseau des couches 4 - 7 (L4-L7) pour les applications Web. L'appliance virtuelle Citrix ADC VPX peut être hébergée sur diverses plates-formes de virtualisation et de cloud. Pour de plus amples informations, consultez la section Déployer une instance de Citrix ADC VPX.

SDK et API

December 18, 2023

SDK Remote PowerShell Citrix DaaS

Le SDK Remote PowerShell automatise les tâches complexes et répétitives. Il fournit le mécanisme qui permet de configurer et gérer l'environnement de Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) sans utiliser les interfaces utilisateur **Gérer**.

- Les détails de l'applet de commande sont fournis dans le SDK Citrix DaaS.
- Les modules pris en charge sont répertoriés dans Prise en charge et limitations. Cette section répertorie également les applets de commande qui sont désactivées dans ce SDK.
- Le SDK Remote PowerShell peut être téléchargé à partir du site Web de Citrix.

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

Différences entre ce SDK et le SDK pour déploiements gérés par le client

Dans un déploiement Citrix Virtual Apps and Desktops installé et géré par les administrateurs du client, ces administrateurs exécutent des scripts et applets de commande dans un site contenant des VDA et des Delivery Controller au sein d'une structure de domaine commune. Par comparaison, Citrix DaaS répartit les VDA et les Controller dans un emplacement de ressources et le plan de contrôle, respectivement. Cette répartition signifie que le SDK PowerShell Citrix Virtual Apps and Desktops d'origine ne fonctionne pas dans un environnement Citrix DaaS. Il ne peut pas traverser la limite sécurisée entre l'emplacement de ressources et le plan de contrôle.

La solution est le kit de développement logiciel distant SDK Remote PowerShell Citrix DaaS. Lors de son exécution dans l'emplacement de ressources, le SDK Remote PowerShell accède au plan de contrôle comme s'il était local. Les mêmes fonctionnalités sont les mêmes qu'avec un seul site Citrix Virtual Apps and Desktops. Seule une faible couche de communication non visible existe, optimisée pour fonctionner soit dans un seul site local, soit dans l'environnement de cloud. Les applets de commande sont identiques et la plupart des scripts existants fonctionnent de la même façon.

L'applet de commande `Get-XdAuthentication` fournit l'autorisation permettant de traverser la limite sécurisée entre l'emplacement de ressources et le plan de contrôle. Par défaut, `Get-XdAuthentication` invite les utilisateurs à entrer des informations d'identification CAS, ce qui doit être effectué une seule fois par session PowerShell. L'utilisateur peut également définir un profil d'authentification à l'aide d'un client sécurisé d'accès aux API, créé dans la console Citrix Cloud. Dans les deux cas, les informations de sécurité sont conservées afin de pouvoir être utilisées dans les

appels ultérieurs du SDK PowerShell. Si cette applet de commande n'est pas explicitement exécutée, elle est appelée par la première applet de commande du SDK PowerShell.

Conditions préalables

Pour utiliser le SDK Citrix DaaS Remote PowerShell, ajoutez les URL suivantes à la liste blanche :

Commercial

- https://accounts.cloud.com
- https://[service].citrixworkspacesapi.net/[customerid]
- https://[customerid].xendesktop.net:443

Japon

- https://accounts.citrixcloud.jp
- https://[service].citrixworkspacesapi.jp/[customerid]
- https://[customerid].apps.citrixworkspacesapi.jp:443

Gouvernement

- https://accounts.cloud.us
- https://[service].citrixworkspacesapi.us/[customerid]
- https://[customerid].xendesktop.us:443

Installer et utiliser le SDK Remote PowerShell

Configuration requise et considérations :

> **Remarque :**
>
> N'installez pas le SDK PowerShell Remote sur une machine Citrix Cloud Connector. Il peut être installé sur n'importe quelle machine appartenant au domaine dans le même emplacement de ressource.
>
> Citrix ne prend pas en charge l'exécution des applets de commande de ce SDK sur des Cloud Connector. Le fonctionnement du SDK n'implique pas les Cloud Connector.
>
> Si vous disposez également d'un déploiement Citrix Virtual Apps and Desktops (en plus du déploiement Citrix DaaS), n'installez pas le kit SDK Remote PowerShell sur une machine Delivery Controller locale.

- Installez **Microsoft Edge WebView2**.

- Assurez-vous que PowerShell 3.0, 4.0 ou 5.0 est disponible sur la machine.
- Le programme d'installation du SDK télécharge et installe .NET Framework 4.8 s'il n'est pas déjà installé (ou une version ultérieure prise en charge).
- Si le SDK Citrix Virtual Apps and Desktops est déjà installé sur la machine, supprimez ce SDK (à partir de Programmes et fonctionnalités de Windows) avant d'installer le SDK Remote PowerShell.
- Dans un environnement automatisé, utilisez le paramètre `-quiet` pour installer le SDK sans intervention de l'utilisateur.

Pour installer et utiliser le SDK Remote PowerShell :

1. Depuis la page de téléchargement, téléchargez le kit de développement logiciel Citrix Virtual Apps and Desktops Remote PowerShell.
2. Installez et exécutez le kit de développement logiciel.

Les journaux d'installation sont créés dans `%TEMP%\CitrixLogs\CitrixPoshSdk`. Ils peuvent aider à résoudre les problèmes d'installation.

Exécutez le kit de développement logiciel sur un ordinateur joint au domaine dans cet emplacement de ressources :

- Ouvrez une invite de commandes PowerShell. Vous n'avez pas besoin de l'exécuter en tant qu'administrateur
- 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`).
- Vous pouvez vous authentifier explicitement à l'aide de l'applet de commande `Get-XdAuthentication`. Ou, exécutez votre première commande du SDK Remote PowerShell qui vous invite à utiliser la même authentification que `Get-XdAuthentication`. Si vous utilisez un proxy, vous devez vous authentifier auprès du proxy pour pouvoir utiliser l'applet de commande `Get-XdAuthentication`. Pour plus d'informations, consultez la section Utiliser le SDK Remote PowerShell avec un proxy.
- Pour contourner l'invite d'authentification, vous pouvez utiliser l'applet de commande `Set-XdCredentials` pour créer un profil d'authentification par défaut, à l'aide d'un client sécurisé créé dans la console Citrix Cloud.
- Continuez à exécuter les applets de commande SDK PowerShell ou les scripts d'automatisation SDK PowerShell. Voyez un exemple.

Pour désinstaller le SDK Remote PowerShell, à partir de la fonctionnalité Windows de suppression ou modification des programmes, sélectionnez **Citrix Virtual Apps and Desktops Remote PowerShell SDK**. Cliquez avec le bouton droit et sélectionnez **Désinstaller**. Suivez les dialogues.

Utiliser le SDK Remote PowerShell avec un proxy Si vous utilisez un proxy, il se peut que vous ne puissiez pas utiliser l'applet de commande `Get-xdAuthentication` car le proxy bloque les

requêtes HTTP émises par l'applet de commande.

Il existe deux manières de s'authentifier auprès du proxy. Vous pouvez utiliser le paramètre `ProxyUseDefault` ou les paramètres `ProxyUsername` et `ProxyPassword` :

- Le paramètre `ProxyUseDefault` active l'authentification auprès du proxy à l'aide des informations d'identification du proxy par défaut. Par exemple :

```
Get-XdAuthentication -ProxyUseDefault
<!--NeedCopy-->
```

- Les paramètres `ProxyUsername` et `ProxyPassword` permettent l'authentification auprès du proxy au sein de la session PowerShell. Par exemple :

```
$secureString = ConvertTo-SecureString -String "password" -
    AsPlainText -Force

Get-XdAuthentication -ProxyUsername user1 -ProxyPassword
    $secureString
<!--NeedCopy-->
```

Exemples d'activités

Les activités courantes incluent la configuration de catalogues de machines, d'applications et d'utilisateurs. Un exemple de script est illustré ci-dessous.

```
    $users = "xd.local\Domain Users"

    $TSVDACatalogName = "TSVDA"

    $TSVDADGName = "TSVDA"

    $TSVDAMachineName = "xd\ds-tsvda2"

    #Create TSVDA Catalog

    $brokerUsers = New-BrokerUser -Name $users

    $catalog = New-BrokerCatalog -Name $TSVDACatalogName -
       AllocationType "Random" -Description $TSVDACatalogName -
       PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
       SessionSupport "MultiSession" -MachinesArePhysical $true

    #Add TSVDA Machine to Catalog

    $BrokeredMachine = New-BrokerMachine -MachineName $TSVDAMachineName
        -CatalogUid $catalog.uid

    #Create new desktops & applications delivery group

```



```
21      $dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
            $TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession
            " -DeliveryType DesktopsAndApps -Description $TSVDADGName
22
23      #Create notepad application
24
25      New-BrokerApplication -ApplicationType HostedOnDesktop -Name "
            Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup $dg
26
27      #Assign users to desktops and applications
28
29      New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
             $dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName
30
31      New-BrokerAccessPolicyRule -Name $TSVDADGName -
            IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers -
            DesktopGroupUid $dg.Uid -AllowedProtocols @("HDX","RDP")
32
33      New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -
            DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description
             $TSVDADGName
34
35      #Add machine to delivery group
36
37      Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
38  <!--NeedCopy-->
```

Prise en charge et limitations

Les systèmes d'exploitation suivants sont pris en charge par le SDK Remote PowerShell :

- Windows 11
- Windows 10
- Windows 10 IoT Enterprise LTSC x32 2019
- Windows 10 IoT Enterprise LTSC x64 2019
- Windows 10 IoT Enterprise 21h1 x64
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Les modules PowerShell Citrix Virtual Apps and Desktops suivants sont pris en charge dans cette version:

- Broker
- Identité Active Directory (AD)
- Création d'une machine
- Configuration

- Journalisation de la configuration
- Hôte
- Administration déléguée
- Analytics

Pour plus d'informations sur les applets de commande, consultez la section Citrix Virtual Apps and Desktops SDK.

Une fois authentifié, l'accès distant reste valide dans la session PowerShell en cours pendant 24 heures. Passé ce délai, vous devez entrer vos informations d'identification.

Le SDK Remote PowerShell doit être exécuté sur un ordinateur dans l'emplacement de ressources.

Les applets de commande suivantes sont désactivées dans les opérations à distance pour maintenir l'intégrité et la sécurité du plan de contrôle Citrix Cloud.

Citrix.ADIdentity.Admin.V2:

- Copy-AcctIdentityPool
- Get-AcctDBConnection
- Get-AcctDBSchema
- Get-AcctDBVersionChangeScript
- Get-AcctInstalledDBVersion
- Remove-AcctServiceMetadata
- Reset-AcctServiceGroupMembership
- Set-AcctDBConnection
- Set-AcctServiceMetadata
- Set-AcctADAccountUserCert
- Test-AcctDBConnection

Citrix.Analytics.Admin.V1:

- Get-AnalyticsDBConnection
- Get-AnalyticsDBSchema
- Get-AnalyticsDBVersionChangeScript
- Get-AnalyticsInstalledDBVersion
- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership
- Set-AnalyticsDBConnection
- Set-AnalyticsServiceMetadata
- Set-AnalyticsSite
- Set-AnalyticsDBConnection

Citrix.DelegatedAdmin.Admin.V1:

- Add-AdminRight
- Get-AdminDBConnection
- Get-AdminDBSchema
- Get-AdminDBVersionChangeScript
- Get-AdminInstalledDBVersion
- Import-AdminRoleConfiguration
- New-AdminAdministrator
- Remove-AdminAdministrator
- Remove-AdminAdministratorMetadata
- Remove-AdminRight
- Remove-AdminServiceMetadata
- Reset-AdminServiceGroupMembership
- Set-AdminAdministrator
- Set-AdminAdministratorMetadata
- Set-AdminDBConnection
- Set-AdminServiceMetadata
- Test-AdminDBConnection

Citrix.Broker.Admin.V2:

- Get-BrokerDBConnection
- Get-BrokerDBSchema
- Get-BrokerDBVersionChangeScript
- Get-BrokerInstalledDBVersion
- Get-BrokerLease
- Get-BrokerController
- New-BrokerMachineConfiguration
- Remove-BrokerControllerMetadata
- Remove-BrokerLease
- Remove-BrokerLeaseMetadata
- Remove-BrokerMachineConfigurationMetadata
- Remove-BrokerMachineConfiguration
- Remove-BrokerSiteMetadata
- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection
- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
- Set-BrokerDBConnection
- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata

- Set-BrokerSiteMetadata
- Test-BrokerDBConnection
- Test-BrokerLicenseServer
- Update-BrokerBrokerLocalLeaseCache

Citrix.Configuration.Admin.V2:

- Export-ConfigFeatureTable
- Get-ConfigDBConnection
- Get-ConfigDBSchema
- Get-ConfigDBVersionChangeScript
- Get-ConfigInstalledDBVersion
- Get-ConfigServiceGroup
- Import-ConfigFeatureTable
- Register-ConfigServiceInstance
- Remove-ConfigRegisteredServiceInstanceMetadata
- Remove-ConfigServiceGroup
- Remove-ConfigServiceGroupMetadata
- Remove-ConfigServiceMetadata
- Remove-ConfigSiteMetadata
- Reset-ConfigServiceGroupMembership
- Set-ConfigDBConnection
- Set-ConfigRegisteredServiceInstance
- Set-ConfigRegisteredServiceInstanceMetadata
- Set-ConfigServiceGroupMetadata
- Set-ConfigServiceMetadata
- Set-ConfigSite
- Set-ConfigSiteMetadata
- Test-ConfigDBConnection
- Unregister-ConfigRegisteredServiceInstance

Citrix.Host.Admin.V2:

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript
- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
- Reset-HypServiceGroupMembership
- Set-HypDBConnection
- Set-HypServiceMetadata
- Test-HypDBConnection

Citrix.ConfigurationLogging.Admin.V1:

- Get-LogDBConnection
- Get-LogDBSchema
- Get-LogDBVersionChangeScript
- Get-LogInstalledDBVersion
- Remove-LogOperation
- Remove-LogServiceMetadata
- Remove-LogSiteMetadata
- Reset-LogDataStore
- Reset-LogServiceGroupMembership
- Set-LogDBConnection
- Set-LogServiceMetadata
- Set-LogSite
- Set-LogSiteMetadata
- Test-LogDBConnection

Citrix.MachineCreation.Admin.V2:

- Get-ProvDBConnection
- Get-ProvDBSchema
- Get-ProvDBVersionChangeScript
- Get-ProvInstalledDBVersion
- Get-ProvServiceConfigurationData
- Remove-ProvServiceConfigurationData
- Remove-ProvServiceMetadata
- Reset-ProvServiceGroupMembership
- Set-ProvDBConnection
- Set-ProvServiceMetadata
- Test-ProvDBConnection

Citrix.EnvTest.Admin.V1:

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript
- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
- Reset-EnvTestServiceGroupMembership
- Set-EnvTestDBConnection
- Set-EnvTestServiceMetadata
- Test-EnvTestDBConnection

Citrix.Monitor.Admin.V1:

- Get-MonitorConfiguration
- Get-MonitorDBConnection
- Get-MonitorDBSchema
- Get-MonitorDBVersionChangeScript
- Get-MonitorDataStore
- Get-MonitorDataStore
- Get-MonitorInstalledDBVersion
- Remove-MonitorServiceMetadata
- Reset-MonitorDataStore
- Reset-MonitorServiceGroupMembership
- Set-MonitorConfiguration
- Set-MonitorDBConnection
- Set-MonitorServiceMetadata
- Test-MonitorDBConnection

Citrix.Storefront.Admin.V1:

- Build-SfCluster
- Get-SfClusters
- Get-SfDBConnection
- Get-SfDBSchema
- Get-SfDBVersionChangeScript
- Get-SfInstalledDBVersion

Module de détection du service Citrix DaaS pour les packages et les serveurs App-V

Citrix DaaS peut fournir les applications contenues dans les packages App-V à vos points de terminaison à l'aide d'une des méthodes suivantes :

- Méthode de gestion d'administration unique (accès aux packages à partir d'un partage réseau)
- Méthode de gestion d'administration double (accès aux packages à partir d'un serveur d'administration Microsoft App-V)

Le processus d'enregistrement des packages App-V, des serveurs de gestion et de publication Microsoft App-V dans la bibliothèque d'applications à l'aide de Citrix DaaS diffère légèrement de l'enregistrement de packages à l'aide d'un déploiement local. Cependant, le processus d'attribution d'applications aux utilisateurs et de lancement sur le poste d'un utilisateur est identique.

La console de gestion Citrix DaaS dans Citrix Cloud ne peut pas afficher les fichiers dans un emplacement de ressources. En outre, elle ne peut pas détecter directement les packages App-V ou les

serveurs Microsoft App-V dans votre infrastructure. Le module de détection fournit des fonctions qui découvrent les informations de package App-V dans votre infrastructure locale et télécharge les informations de package vers votre instance Citrix DaaS. Les informations sur les packages incluent les packages App-V, les serveurs Microsoft App-V et les applications qu'ils contiennent.

Le module de détection utilise le SDK Remote PowerShell de Virtual Apps and Desktops. Il peut découvrir des informations de package à partir d'un partage réseau ou d'un serveur Microsoft App-V Management Server. Vous devez utiliser le module de détection sur une machine dans votre emplacement de ressources.

Conditions préalables à l'utilisation du module de détection :

- Assurez-vous que PowerShell 3.0 ou version ultérieure est disponible sur la machine.
- Assurez-vous que le SDK Remote PowerShell Citrix Virtual Apps and Desktops est installé sur la machine.
- Vérifiez que vous avez accès au partage réseau contenant les packages App-V.
- Vérifiez que vous avez accès au serveur sur lequel les Citrix Cloud Connectors sont installés et que Microsoft App-V Management Server est hébergé.

Ajouter des packages App-V à la bibliothèque d'applications dans Citrix Cloud

La procédure ci-dessous est valide pour ajouter des packages App-V à partir de partages réseau (gestion d'administration unique) et ajouter tous les packages App-V publiés à partir de Microsoft App-V Management Server (gestion d'administration double). Si vous utilisez la méthode de gestion d'administration double, vous devez gérer les packages App-V ajoutés comme vous le faites lors de l'utilisation de la méthode de gestion d'administration unique.

1. Téléchargez le module de détection à partir de la page de téléchargements de Citrix DaaS https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.html. Extrayez le fichier zip `Citrix.Cloud.AppLibrary.Admin.v1.psm1` dans un dossier pratique.

   > **Remarque :**
   >
   > Ce fichier est également fourni sur l'ISO de Citrix Virtual Apps and Desktops dans `Support\Tools\Scripts`. Vous pouvez le copier localement ou le référencer directement depuis le lecteur de CD.

2. Vérifier que le SDK Remote PowerShell de Virtual Apps and Desktops est installé sur la machine
3. Naviguez jusqu'au dossier contenant le module de détection. Dans la fenêtre PowerShell, tapez le chemin d'accès complet du dossier contenant le module de détection, puis appuyez sur **Entrée**.

4. Importez le module de détection avec la commande `Import-Module .\Citrix.Cloud.AppLibrary.Admin.v1.psm1`.
5. Ajoutez les packages App-V à la bibliothèque d'applications dans Citrix Cloud en utilisant l'une des méthodes suivantes.

   - Pour ajouter des packages App-V à partir d'un partage réseau, exécutez l'applet de commande PowerShell : `Import-AppVPackageToCloud`.

     Pa exemple : `Import-AppVPackageToCloud –PackagePath \\AppVSrv\share\Notepad++.appv`

     Pour obtenir de l'aide sur l'applet de commande, tapez `Get-Help Import-AppVPackageToCloud`.

   - Pour ajouter des packages App-V à partir d'un serveur de gestion Microsoft App-V, exécutez l'applet de commande PowerShell : `Import-AppVPackagesFromManagementServerToCloud`

     Pa exemple : `Import-AppVPackagesFromManagementServerToCloud –ManagementSrvFQDN AppVMngSrv.domain.local`

     Pour obtenir de l'aide sur l'applet de commande, tapez `Get-Help Import-AppVPackagesFromManagementServerToCloud`.

     Cette commande importe tous les packages App-V publiés à partir du serveur Microsoft App-V Management Server vers Citrix Cloud.

     Après avoir ajouté les packages App-V à Citrix Cloud, vous devez les gérer comme vous le faites à l'aide de la méthode de gestion d'administration unique.

6. Connectez-vous à Citrix Cloud. Sélectionnez le client cible. Une fois le script exécuté correctement, les packages App-V sont ajoutés à la bibliothèque d'applications dans Citrix Cloud.

Fonctions PowerShell de haut niveau

Le module contient les fonctions de haut niveau suivantes que vous pouvez appeler à partir de votre propre script PowerShell :

- `Import-AppVPackageToCloud -PackagePath <Full UNC path to App-V package>`

  Détecte et charge sur Citrix DaaS toutes les informations nécessaires à la publication d'applications à partir d'un package App-V unique.

- `Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN <FQDN of a Microsoft App-V Management Server>`

Détecte les chemins UNC des packages publiés par le serveur de gestion et appelle **Import-AppVPackageToCloud** pour chacun d'eux à tour de rôle.

Les packages détectés de cette manière sont chargés sur Citrix DaaS à l'aide de la méthode de gestion d'administration unique. Citrix DaaS ne peut pas fournir de packages à l'aide de la méthode de gestion à double administration.

- `Import-AppVDualAdminToCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Détecte les serveurs de gestion et de publication Microsoft App-V et importe le contenu dans la bibliothèque d'applications. Cette applet de commande importe tous les packages gérés à l'aide du serveur de gestion Microsoft App-V et les informations associées. Les serveurs peuvent être ajoutés et supprimés via PowerShell.

  Cette applet de commande ajoute des packages App-V en mode administrateur double. Seuls les packages App-V publiés sur le serveur de gestion Microsoft App-V et qui ont ajouté des groupes AD, sont importés. Si vous apportez des modifications au serveur de gestion Microsoft App-V, réexécutez cette applet de commande pour synchroniser la bibliothèque d'applications avec le serveur de gestion Microsoft App-V.

- `Remove-AppVServerFromCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Supprime les serveurs de gestion et de publication Microsoft App-V ajoutés à la bibliothèque d'applications.

  Cette applet de commande supprime les serveurs de gestion et de publication Microsoft App-V spécifiés, ainsi que tous les packages App-V associés.

Exécutez le module de détection des packages et des serveurs App-V sur un ordinateur joint à un domaine dans cet emplacement de ressources. Suivez les instructions de la procédure d'installation et d'utilisation du SDK Remote PowerShell pour commencer. Continuez à exécuter les applets de commande ou les scripts PowerShell. Voir les exemples suivants.

Exemples d'activités

Importez le module de détection de packages Citrix DaaS App-V.

```
1 import-module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.
     v1.psm1"
2 <!--NeedCopy-->
```

Lisez en boucle le répertoire du magasin de packages App-V et charger chaque paquet.


```
Get-ChildItem -Path "\FileServer.domain.net\App-V Packages" -Filter *.
    appv |
Foreach-Object{

    Import-AppVPackageToCloud -PackagePath $_.FullName
 }

<!--NeedCopy-->
```

Détectez et chargez des packages enregistrés avec un serveur de gestion Microsoft App-V.

```
Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN
    AppVManagementServer.domain.net
<!--NeedCopy-->
```

Détectez les serveurs de gestion et de publication Microsoft App-V et ajouter la configuration à la bibliothèque d'applications. Cela importe également tous les packages gérés par le serveur de gestion Microsoft App-V en mode administrateur double.

```
Import-AppVDualAdminCloud -ManagementSrvUrl http://AppVManagementServer
    .domain.net  – PublishingServerUrl http://AppVManagementServer.domain
    .net:8001
<!--NeedCopy-->
```

Lisez la documentation d'aide de PowerShell incluse dans le module.

```
Get-Help Import-AppVPackageToCloud
<!--NeedCopy-->
```

Limitations

- Vous ne pouvez pas détecter les packages App-V sur votre infrastructure d'emplacement de ressources directement à partir de la console de gestion Citrix DaaS dans Citrix Cloud. Pour plus d'informations sur Citrix Cloud, consultez la documentation Citrix Cloud.
- La console de gestion Citrix DaaS dans Citrix Cloud n'a pas de connexion active au Microsoft App-V Management Server. Les modifications apportées aux packages et à d'autres configurations dans le Microsoft App-V Management Server ne sont pas répercutées dans la console de gestion Citrix DaaS tant que `Import-AppVDualAdminCloud` n'est pas réexécuté.

API Monitor Service OData

En plus d'utiliser les fonctions de surveillance pour afficher les données d'historique, vous pouvez interroger les données à l'aide de l'API de Monitor Service. Utilisez l'API pour :

- Analyser des tendances historiques pour la planification

- Effectuer une résolution des problèmes détaillée des échecs de connexion et de machine
- Extraire des informations afin de les envoyer dans d'autres outils et processus ; par exemple, à l'aide des tables PowerPivot de Microsoft Excel pour afficher les données de différentes manières
- Créer une interface utilisateur personnalisée en plus des données offertes par l'API

Pour de plus amples informations, consultez Monitor Service OData API. Pour accéder à l'API Monitor Service, consultez la section Accéder aux données de Monitor Service à l'aide du point de terminaison OData v4 dans Citrix Cloud.

API Citrix DaaS

Les API Citrix DaaS sont disponibles sur https://developer.cloud.com/citrixworkspace/citrix-daas.

Clause d'exclusion de responsabilité

Ce logiciel/exemple de code est fourni « en l'état », sans aucune déclaration, garantie ou condition. Vous pouvez l'utiliser, le modifier et le distribuer à vos propres risques. CITRIX EXCLUT TOUTE GARANTIE EXPRESSE, TACITE, ÉCRITE, ORALE OU LÉGALE, Y COMPRIS, MAIS SANS S'Y LIMITER, TOUTE GARANTIE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER, DE PROPRIÉTÉ ET D'ABSENCE DE CONTREFAÇON. Nonobstant ce qui précède, vous reconnaissez et acceptez (a) que le logiciel/exemple de code peut présenter des erreurs, des défauts de conception ou d'autres problèmes, susceptibles d'entraîner une perte de données ou des dommages à la propriété ; (b) qu'il peut être impossible de rendre le logiciel/exemple de code entièrement opérationnel ; et (c) que Citrix peut, sans préavis ni responsabilité, cesser de mettre à votre disposition la version actuelle et/ou les versions futures du logiciel/exemple de code. En aucun cas le logiciel/code ne devra être utilisé dans le cadre d'activités à haut risque, telles que, mais sans limitation aucune, les activités de maintien en vie ou d'explosion. CITRIX, SES FILIALES OU SES AGENTS NE POURRONT ÊTRE RESPONSABLES, EN VERTU D'UNE RUPTURE DE CONTRAT OU DE TOUTE AUTRE THÉORIE DE RESPONSABILITÉ, DE TOUT DOMMAGE RÉSULTANT DE L'UTILISATION DU LOGICIEL/EXEMPLE DE CODE, Y COMPRIS MAIS SANS LIMITATION AUCUNE, LES DOMMAGES DIRECTS, SPÉCIAUX, ACCESSOIRES, PUNITIFS, INDIRECTS OU AUTRES, MÊME S'ILS ONT ÉTÉ PRÉVENUS DE L'ÉVENTUALITÉ DE TELS DOMMAGES. Vous acceptez d'assurer l'indemnisation et la défense de Citrix contre toute réclamation résultant de l'utilisation, de la modification ou de la distribution du code.